Lenovo XClarity Administrator REST API Guide

Version 4.1

Note

Before using this information and the product it supports, read the general and legal notices in the XClarity Administrator online documentation.

Second Edition (June 2024)

Contents

Summary of changes in the REST API for v4.1

Lenovo XClarity Administrator v4.1 supports enhancements to the Open REST API.

For information about enhancements to the REST API in other releases, see REST APIs in the XClarity Administrator online documentation in the XClarity Administrator online documentation.

This documentation includes new methods and parameters that apply to the current XClarity Administrator release and later. If you are using an earlier release of XClarity Administrator, you can use the *REST API Reference* PDF for a list of methods and parameters that apply to that specific release. To find PDFs for the release that you need, see PDF files in the XClarity Administrator online documentation.

The following methods were added or updated in this release.

- Virtual appliance management
  - GET /aicc. Added the **is_clean** response attribute to return information about whether initial setup has not been started on the virtual appliance. Added the **hideUnmanagedChassis** response attribute to return whether to hide the chassis that are not explicitly managed.
  - (New) GET /aicc/service/sftp/locks. Returns a list of all SFTP service locks.
  - (New) POST /aicc/service/sftp/locks. Starts (enable) the SFTP service for a specific function and acquire an SFTP service lock by creating a lock ID.
  - (New) GET /aicc/service/sftp/locks/*{id}*. Returns information about a specific SFTP service lock.
  - (New) DELETE /aicc/service/sftp/locks/*{id}*. Releases a specific SFTP service lock by deleting a specific lock ID and, if all locks are deleted, stop (disable) the SFTP service (unless dbgshell account exist on the Lenovo XClarity Administrator instance).
- Firmware updates
  - POST /compliancePolicies. The **exportWithPackages** value was added to the **action** query parameter to compress the specified compliance policy .xml file and the update files used by the policy into a .zip file and downloads the .zip file to the local system. A job is created to export a compliance policy with or without packages.
  - PUT /compliancePolicies. When the **action=import** query is specified, a job is created to import the compliance policy with or without packages.
- Security
  - GET /ldapClientSettings. Added the **groupFilters** response attribute to return the groups search filters to customize the authentication process when configuring XClarity Administrator with an external LDAP server . Added the **userFilters** response attribute to return the users search filters to customize the authentication process when configuring XClarity Administrator with an external LDAP server . Added the **searchLimit** response attribute to return the number of in-search results that can be retrieved in an LDAP search operation using user and group filters. Added the **timeout** response attribute to return the amount of time, in seconds, to complete an LDAP search operation before timing out.
  - PUT /ldapClientSettings. Added the **groupFilter**, **searchFilter**, **searchSizeLimit**, and **timeoutLimit** request attributes to manually configure the LDAP search parameters.

Chapter 1. Lenovo XClarity Administrator REST APIs

Lenovo XClarity Administrator provides a set of easy-to-use APIs that can be used to access XClarity Administrator data and services from applications running outside of the XClarity Administrator framework.

The REST APIs allow for easy integration of XClarity Administrator capabilities into other software, whether the software is running on the same system as the XClarity Administrator server, or on a remote system within the same network. These APIs are based on the REST architecture and are accessed via the HTTPS protocol.

Attention: The content type that you specify in the HTTP header must match the format of data that you specify in the request body. If there is a mismatch, XClarity Administrator returns an error code because it cannot parse the data. For example, when sending JSON format, if you specify `Content-Type:application/x-www-form-urlencoded`, you will receive an error code. The default content type for all requests is "application/json; charset=UTF-8."

The following documentation includes new methods and parameters that apply to the XClarity Administrator *Version 4.1* and later. If you are using an earlier version of XClarity Administrator, you can use the *REST API Reference* PDF for a list of methods and parameters that apply to that specific release. To find PDFs for the release that you need, see PDF files in the XClarity Administrator online documentation.

REST API authorization and authentication

When programming with the Lenovo XClarity Administrator REST APIs, you must authenticate using a user ID and password. The user ID must have the correct authorization to perform the intended task.

You can use Lenovo XClarity Administrator web interface or CLI to configure the authorizations that provide access to Lenovo XClarity Administrator tasks and resources (see Managing user accounts in the Lenovo XClarity Administrator online documentation).

Note: If you encounter a temporary HTTP connection error, attempt to log in to Lenovo XClarity Administrator again.

Important: When running automated scripts, if you want the session to respect the inactivity timeout, add the **X-NOT-USER-INPUT** field with a value of **checkSession** to the request header of each request. Adding this header implies that the session times out based on the inactivity timeout value. If the session times out, the session is not renewed, although active requests for uploading and downloading data are not canceled.

REST API response codes

The Lenovo XClarity Administrator REST APIs use the HTTP protocol for sending and retrieving data. Client code using the REST APIs makes an HTTP request to the Lenovo XClarity Administrator server and processes the HTTP response accordingly. Included with the HTTP response data is the HTTP response code. The response code provides some indication as to the success of the HTTP request and can provide information on how to handle the included response data.

The following table lists some of the most common response codes.

Code	Description	Comments
200	OK	The request completed successfully.
201	Created	One or more new resources were successfully created.

Code	Description	Comments
202	Accepted	The request has been accepted for processing, but the processing has not yet completed. The request might or might not be acted upon, depending on the results of the processing.
203	Found	The URL changed. The response header returns the correct URL in the Location field.
204	No Content	The request completed successfully, but no response content is returned.
206	Partial Content	The part, but not all, of the request completed successfully.
307	Temporary Redirect	The URL changed for this REST API. The response header returns the correct URL in the Location attribute.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
405	Method Not Allowed	A specified resource is invalid. A descriptive error message is returned in the response body.
406	Not Supported	A specified resource is not supported or not available for connection. A descriptive error message is returned in the response body.
408	Request Timeout	The orchestrator server did not receive a required request in a specific amount of time. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
412	Precondition failed	Specified data is invalid because of missing values. A descriptive error message is returned in the response body.
413	Request Entity Too Large	Clients might impose limitations on the length of the request URI, and the request URI is too long to be handled. A descriptive error message is returned in the response body.
423	Locked	The source or target resource is locked. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.
503	Service Unavailable	The server is not ready to handle the request.

Status messages

The status message attributes identify the success or failure of an REST API operation.

Some POST, PUT, PATCH, and DELETE requests include status-message attributes in the response body to describe the success or failure of the request, using the following JSON structure.

Most GET requests that are successful (2xx response code) *do not* include status-message attributes. Some GET requests that fail (response codes other than 2xx) include status-message attributes in the response body to describe the failure of the request, using the following JSON structure.

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned for a failed REST API request.

```
{
    "result": "failed",
   "messages": [{
      "id": "FQXHMSS1002J",
      "text": "The request to change the log level of com.apache to ERROR was not successful.",
      "explanation": "The log level requested could not be changed.",
      "recovery": {
         "text": "Please retry the action.",
         "url": ""
      }
   }]
}
```

Chapter 2. Virtual-appliance management

The following resources are available for managing the Lenovo XClarity Administrator virtual appliance.

/aicc

Use this REST API to retrieve or configure information about the Lenovo XClarity Administrator virtual appliance.

HTTP methods

GET, PUT

GET /aicc

Use the method to retrieve information about the Lenovo XClarity Administrator, such as NTP server settings, date and time settings, services that are currently running, and the build level.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/aicc`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

Attributes		Type	Description
appliance		Object	Information about the current instance of the XClarity Administrator virtual appliance
	build	String	Current build level
	date	String	Current date and time
	name	String	Current appliance name
	runlevel	Integer	Current state of the appliance. This can be one of the following values. • **0**. The appliance is halted. • **3**. The appliance is operating normally. • **6**. The appliance is restarting.
	status	String	Current status of the appliance. The value is always “Normal.”

Attributes	Type	Description
uuid	String	UUID of the appliance
version	String	Current version number
appliance_states	Object	List of all available appliance states
description	String	Appliance-state description
runlevel	Integer	Appliance-state value
date	Object	Information about the current date on the XClarity Administrator
date_time	String	Date and time
parts	Array	Information about the current time
yyyy	Integer	Year
mm	Integer	Month
dd	Integer	Day
hours	Integer	Hour
mins	Integer	Minute
secs	Integer	Second
time_format	String	Time format. This can be one of the following values. • **12**. (default). 12-hour clock • **24**. 24-hour clock
timezone	String	Current time zone
timezone_id	String	Time zone ID
timezones	Object	Information about all available time zones
daylight_saves	Integer	Amount of time to be added to local standard time to get the current time. This can be one of the following values. • **3600000**. If **use_daylight** is true, adds 3600000 milliseconds (one hour). • **0**. f **use_daylight** is false, adds 0 milliseconds.
display_name	String	Time zone name
id	String	Time zone ID
offset	Integer	Coordinated Universal Time (UTC) offset (for example, -5 or +4)
uses_daylight	Boolean	Indicates whether daylight saving time is used. This can be one of the following values. • **true**. Daylight saving time is used. • **false**. Daylight saving time is not used.
utc_offset_raw	Integer	UTC offset (for example, -5 or +4)
utc_offset_w_dst	Integer	UTC offset adjusted for daylight saving time, if applicable (for example, -5 or +4)
uses_daylight	Boolean	Identifies whether daylight saving time is used. This can be one of the following values. • **true**. Daylight saving time is used. • **false**. Daylight saving time is not used.
utc_offset	Integer	UTC offset (for example, -5 or +4)

Attributes	Type	Description
utc_offset_raw	Integer	UTC offset (for example, -5 or +4)
utc_offset_w_dst	Integer	UTC offset adjusted for daylight saving time, if applicable (for example, -5 or +4)
hideUnmanagedChassis	Boolean	Indicates whether to hide chassis that were not explicitly managed by a user. This can be one of the following values. • **true**. Hide chassis that were not explicitly managed. • **false**. (default) Show chassis that were not explicitly managed. This attribute is supported in XClarity Administrator v4.1 and later.
is_clean	Boolean	Indicates whether initial setup has not been started on the virtual appliance. This can be one of the following values. • **true**. Initial setup has not been started. • **false**. Initial setup has been started or completed. This attribute is supported in XClarity Administrator v4.1 and later.
network_interfaces	Array	List of XClarity Administrator network interfaces
id	String	Network ID (such as “eth0” or “eth1”)
ip_addresses	Array	IPv4 and IPv6 addresses for this interface
assign_method	String	Assignment method used for this IP address. This can be one of the following values. • **static** • **dhcp** • **auto**
ip	String	IPv4 or IPv6 address
ip_linklocal	Boolean	Indicates whether this address is an IPv6 link local address. This can be one of the following values. • **true**. This address is an IPv6 link local address. • **false**. This address is not an IPv6 link local address.
prefix_length	Integer	Prefix length (in bits) for this IP address
version	Integer	IP version of this address. This value is either “4” or “6”.
mac_address	String	MAC address
role	Array of strings	Roles that are performed by this interface. This can be one or more of the following values. • **none** • **management** • **osdeployment**
rpf	String	
ntp	Object	Information about the NTP server that is associated with XClarity Administrator.
servers	Array of objects	List of NTP servers
authenticated	Boolean	Indicates whether the XClarity Administrator is authenticated with the NTP server. This can be one of the following values. • **true**. XClarity Administrator is authenticated with the NTP server. • **false**. XClarity Administrator is not authenticated with the NTP server.

Attributes	Type	Description
server	String	IP address or hostname of the NTP server
version	Integer	Version of the NTP server. This can be one of the following values. • **1**. No key authentication is required. • **3**. NTPv3 is used, and key authentication is required. You must specify the authentication key and index for the NTP server for M-MD5 or SHA1 or both using the **v3_key**, **v3_key_type**, and **v3_key_index** parameters.
v3_key	String	Key value specified in `/etc/ntp/keys`
v3_key_index	Integer	Key-index value specified in `/etc/ntp/keys`
v3_key_type	String	Key-type value specified in `/etc/ntp/keys`. This can be one of the following values. • **M**. M-MD5 authentication • **SHA1**. SHA1 authentication
preferredDisplayName	String	Property to use to displayed the device names in the user interface. This can be one of the following values. • **byDefault**. Displays the value that is provided by XClarity Administrator. • **userDefinedName** • **dnsHostname** • **hostname** • **ipv4Address** • **serialNumber** If the selected property is not applicable or is applicable but there is no value available for a device, then **byDefault** is used.
preferredSortGridState	Boolean	Indicates whether to sort the inventory and groups data using the value set for the **preferredDisplayName** attribute. This can be one of the following values. • **true**. Sorts the inventory and groups data alphabetically using the **preferredDisplayName** attribute. • **false**. Sorts alphabetically using **byDefault.**
service_states	Object	List of all available service states
description	String	Service-state description
state	Integer	Service-state value
services	Array	List of the XClarity Administrator services
id	String	Service ID
initd	String	Service name
pid	Integer	Process ID
state	Integer	Current state of the service. This can be one of the following values. • **0**. The service is running. • **1**. The service is stopped but PID file exists. • **2**. The service is stopped but lock file exists. • **3**. The service is not running. • **4**. The current state of the service is unknown.
subscriptions	Array	List of subscriptions
id	Integer	Subscription ID

Attributes		Type	Description
	monitor_uri	String	Network-related resource that is to be monitored by XClarity Administrator. If **monitor_uri** is set to “/aicc” or “”, every /aicc URI is monitored. If **monitor_uri** is set to “”, IP change notifications are received through DHCP.
	submonitor_uri	String	
	uri	String	Resource to which XClarity Administrator writes a POST when XClarity Administrator detects a change in monitored resource. The specified URI must be able to accept POST requests, where the body of the POST matches the JSON PUT to **monitor_uri**.

The following example is returned if the request is successful.


```
{
   "appliance": {
      "build": "686",
      "date": "686",
      "name": "LXCA - 10.240.61.98",
      "runlevel": 3,
      "status": "Normal",
      "uuid": "963602b8-edaf-4183-bf18-e842db92f610",
      "version": "2.99.99"
   },
   "appliance_states": [{
      "description": "Halt the appliance",
      "runlevel": 0
   },
   ...,
   {
      "description": "Reboot the appliance",
      "runlevel": 6
   }],
   "date": {
      "date_time": "August 6, 2018 11:29:41 AM EDT",
      "parts": {
         "yyyy": 2018,
         "mm": 8,
         "dd": 6,
         "hours": 11,
         "mins": 29,
         "secs": 41
      },
      "time_format": "12",
      "timezone": "Eastern Standard Time",
      "timezone_id": "America/New_York",
      "timezones": [{
         "daylight_saves": 0,
         "display_name": "Greenwich Mean Time",
         "id": "Africa/Abidjan",
         "offset": 0,
         "uses_daylight": false,
         "utc_offset_raw": 0,
         "utc_offset_w_dst": 0
      },
      ...,
      {
         "daylight_saves": 0,
```

```
        "display_name": "Mountain Standard Time",
        "id": "MST",
        "offset": -25200000,
        "uses_daylight": false,
        "utc_offset_raw": -25200000,
        "utc_offset_w_dst": -25200000
    }],
    "uses_daylight": true,
    "utc_offset": -18000000,
    "utc_offset_raw": -18000000,
    "utc_offset_w_dst": -14400000
},
"hideUnmanagedChassis": true,
"is_clean": false,
    "id": "eth0",
    "ip_addresses": [{
        "assign_method": "static"
        "ip": "fe80:0:0:0:215:5dff:fe3f:f143%eth0",
        "ip_linklocal": "true",
        "prefix_length": 64,
        "version": 6
    },
    ...,
    {
        "assign_method": "none",
        "ip": "0::0%0",
        "ip_linklocal": "false",
        "prefix_length": 64,
        "version": 6
    }],
    "mac_address": "00:15:5D:3F:F1:43",
    "role": ["management","osdeployment"],
    "rpf": "RFC3704Strict"
}],
"ntp": {
    "servers": [{
        "authenticated": true,
        "server": "time-a.nist.gov",
        "version": 3
        "v3_key": "12345678901234567890123456789Oabcdefabcd",
        "v3_key_index": 3,
        "v3_key_type": "M",
    },
    {
        "authenticated": true,
        "server": "us.pool.ntp.org",
        "version": 3,
        "v3_key": "12345678901234567890123456789Oabcdefabcd"
        "v3_key_index": 1,
        "v3_key_type": "SHA1",
    }]
},
"preferredDisplayName": "byDefault",
"preferredSortGridState": true,
"service_states": [{
    "description": "Service is running",
    "state": 0
},
...,
{
    "description": "Special purpose state used to trigger restart through REST",
```

```
      "state": 191
   }],
   "services": [{
      "id": "core",
      "initd": "xhmc-core",
      "pid": 1962,
      "state": 0
   },
   ...,
   {
      "id": "xcat",
      "initd": "xcatd",
      "pid": 18247,
      "state": 0
   }],
   "subscriptions": [{
      "id": 1,
      "monitor_uri": "/aicc",
       "submonitor_uri": "/ntp",
      "uri": "/ntpNotification"
   },
   {
      "id": 2,
      "monitor_uri": "/aicc/network/interfaces",
      "submonitor_uri": "",
      "uri": "/netchangenotsec"
   }]
}
```


PUT /aicc

Use this method to configure Lenovo XClarity Administrator settings (such as NTP server settings, date and time settings, and services that are currently running), change the virtual appliance name, and restart or shutdown the virtual appliance.

Note: Restarting or shutting down the virtual appliance causes any outstanding jobs to be interrupted and stopped. Before calling **PUT /aicc** to shut down or restart the virtual appliance, use GET /tasks to check for any outstanding jobs.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/aicc`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
appliance	Optional	Object	Information about the current instance of the XClarity Administrator virtual appliance
name	Optional	String	Name of the virtual appliance

Attributes	Re-quired / Optional	Type	Description
runlevel	Optional	Integer	Appliance run level. This can be one of the following values. • **0**. Shut down • **6**. Restart
date	Optional	Object	Information about the current date and time on XClarity Administrator
parts	Optional	Array	Current date and time
yyyy	Optional	Integer	Year
mm	Optional	Integer	Month
dd	Optional	Integer	Day
hours	Optional	Integer	Hour
mins	Optional	Integer	Minute
secs	Optional	Integer	Second
time_format	Optional	String	Time format. This can be one of the following values. • **12**. (default). 12-hour clock • **24**. 24-hour clock
timezone_id	Optional	String	Time zone ID
hideUnmanagedChassis	Optional	Boolean	Indicates whether to hide chassis that were not explicitly managed by a user. This can be one of the following values. • **true**. Hide chassis that were not explicitly managed. • **false**. (default) Show chassis that were not explicitly managed. This attribute is supported in XClarity Administrator v4.1 and later.
ntp	Optional	Object	Information about the NTP server that is associated with XClarity Administrator
servers	Optional	Array of objects	List of NTP servers
server	Required	String	IP address or hostname of the NTP server
sync	Required	Boolean	Indicates whether XClarity Administrator synchronizes with the NTP server specified with the **server** attribute.
version	Optional	Integer	Version of the NTP server. This can be one of the following values. • **1**. No key authentication is required. • **3**. NTPv3 is used, and key authentication is required. You must specify the authentication key and index for the NTP server for M-MD5 or SHA1 or both using the **v3_key**, **v3_key_type**, and **v3_key_index** parameters.

Attributes	Re-quired / Optional	Type	Description
v3_key	Optional	String	Authentication key. This can be one of the following values. • For the M-MD5 key, specify an ASCII string. • For the SHA1 key, specify a 40-character ASCII string, including only 0–9 and a-f. **Note:** The key index and authentication key must match the key ID and password values set on the NTP server. See the documentation for your NTP server for information about setting the key ID and key index.
v3_key_index	Optional	String	Authentication key index **Note:** The key index and authentication key must match the key ID and password values set on the NTP server. See the documentation for your NTP server for information about setting the key ID and password.
v3_key_type	Optional	String	Authentication key-type. This can be one of the following values. • **M**. M-MD5 authentication • **SHA1**. SHA1 authentication
preferredDisplayName	Optional	String	Property to use to displayed the device names in the user interface. This can be one of the following values. • **byDefault**. Displays the value that is provided by XClarity Administrator. • **userDefinedName** • **dnsHostname** • **hostname** • **ipv4Address** • **serialNumber** If the selected property is not applicable or is applicable but there is no value available for a device, then **byDefault** is used.
preferredSortGridState	Optional	Boolean	Indicates whether to sort the inventory and groups data using the value set for the **preferredDisplayName** attribute. This can be one of the following values. • **true**. Sorts the inventory and groups data alphabetically using the **preferredDisplayName** attribute. • **false**. Sorts alphabetically using **byDefault.**
services	Optional	Array	List of the XClarity Administrator services
id	Optional	String	Service ID To obtain the service IDs, use GET /aicc.
state	Optional	Integer	Current state of the service. This can be one of the following values. • **191**. Restart the service.
vaSettings	Optional	Object	Cryptographic and certificate settings for this XClarity Administrator instance.

Attributes	Re-quired / Optional	Type	Description
certificate	Optional	String	Apache server certificate readiness. This can be one of the following values. • **ready** • **not available**. The OS deployment role is not enabled for any XClarity Administrator network interfaces (see Configuring network access in the Lenovo XClarity Administrator online documentation). • **NA**. (default) The certificate is not generated.
cryptographicMode	Optional	String	Cryptographic mode. This can be one of the following values. • **COMP**. (default) This mode is compatible with older firmware versions, browsers, and other network clients that do not implement strict security standards that are required for compliance with NIST SP 800-131A. • **NIST**. This mode is designed to comply with the NIST SP 800-131A standard. • **NA**. For more information about these settings, see Setting the cryptography mode and communication protocols in the Lenovo XClarity Administrator online documentation.
tlsMode	Optional	String	Minimum TLS protocol version to use for client connections. This can be one of the following values. • **tls1.2**. TLS v1.2 and later can be used • **tls1.3**. TLS v1.3 and later can be used • **NA** For more information about these settings, see Setting the cryptography mode and communication protocols in the Lenovo XClarity Administrator online documentation.

The following example sets an NTPv1 server.

```
{
    "ntp": {
        "servers": [{
            "server": "1.1.1.2",
            "version": 1
        }]
    }
}
```

The following example sets an NTPv3 server using both M-MD5 and SHA1 authentication.

```
{
   "ntp": {
      "servers": [{
         "server": "time-a.nist.gov",
         "version": 3
         "v3_key": "12345678901234567890123456789Oabcdefabcd",
         "v3_key_index": 3,
         "v3_key_type": "M",
      },
      {
         "server": "us.pool.ntp.org",
         "version": 3,
         "v3_key": "12345678901234567890123456789Oabcdefabcd"
         "v3_key_index": 1,
         "v3_key_type": "SHA1",
```

```
      }]
   }
}
```

The following example synchronizes XClarity Administrator with the NTP server.

```
{
   "ntp": {
      "servers": [{
         "server": "time-a.nist.gov",
         "sync": "true"
      }]
   }
}
```

The following example sets the clock setting and time zone.

```
{
   "date": {
      "time_format": "24",
      "timezone_id": "America/ New_York"
   }
}
```

The following example sets the date and time.

```
{
   "date": {
      "parts": {
         "yyyy": 2014,
         "dd": 7,
         "mm": 5,
         "hours": 2,
         "mins": 10,
         "secs": 24
      }
   }
}
```

The following example restarts network services.

```
{
   "services": [{
      "id": "network",
      "state": 191
   }]
}
```

The following example shuts down the virtual appliance.

```
{
   "appliance": {
     "runlevel": 0
   }
}
```

The following example restarts the virtual appliance.

```
{
   "appliance": {
      "runlevel": 6
   }
}
```

The following example changes the virtual appliance name.

```
{
   "appliance": {
      "name": "myAppliance"
   }
}
```

The following example displays the device names and sorts tables in the web interface using the IPv6 address of the device.

```
{
   "preferredDisplayName": "ipv6Address",
   "preferredSortGridState": true
}
```

The following example hides chassis that are not explicitly managed.

```
{
   "hideUnmanagedChassis": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/aicc/network/host

Use this REST API to retrieve or configure information about the Lenovo XClarity Administrator host.

HTTP methods

GET, PUT

GET /aicc/network/host

Use the method to retrieve the Lenovo XClarity Administrator host settings.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/aicc/network/host`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
domain_name	String	Domain name of the virtual appliance
dns_servers	Array	IP addresses that is used to resolve DNS queries
ip	String	IP address of the DNS entry
priority	Integer	Relative priority of the DNS entry
hostname	String	Hostname of the virtual appliance
proxy	Array	Information about the proxy server
enabled	Boolean	Indicates whether the proxy server is enabled. This can be one of the following values. • **true**. The proxy server is enabled. • **false**. The proxy server is disabled.
ip	String	IPv4 or IPv6 address of the proxy server
isPasswordSet	Boolean	Indicates whether the password is set for the proxy server. This can be one of the following values. • **true**. The password is set. • **false**. The password is not set.
port	Integer	Port number of the proxy server
userid	String	User ID used to access the proxy server

The following example is returned if the request is successful.

```
{
   "domain_name": "",
   "dns_servers": [{
      "ip": "10.240.0.10",
      "priority": 1
   },
   {
      "ip": "10.240.0.11",
      "priority": 2
   }],
   "hostname": "localhost",
   "proxy": {
      "enabled": false,
      "ip": "",
      "isPasswordSet": false,
      "port": 0,
      "userid": ""
   }
}}
```

PUT /aicc/network/host

Use this method to configure the Lenovo XClarity Administrator host settings.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/aicc/network/host`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
domain_name	Optional	String	Domain name of the virtual appliance
dns_servers	Optional	Array of objects	IP addresses to be used to resolve DNS queries
ip	Required	String	IP address of the DNS entry
priority	Required	Integer	Relative priority of the DNS entry
hostname	Optional	String	Hostname of the virtual appliance
proxy	Optional	Array of objects	Information about the proxy server
enabled	Required	Boolean	Indicates whether the proxy server is enabled. This can be one of the following values. • **true**. The proxy server is enabled. • **false**. The proxy server is disabled.
ip	Required	String	IPv4 or IPv6 address of the proxy server
password	Required	String	Password for the user ID
port	Required	Integer	Port number of the proxy server
userid	Required	String	User ID used to access the proxy server

The following example sets the hostname.

```
{
   "hostname": "my_host"
}
```

The following example sets the domain name.

```
{
   "domain_name": "my_domain"
}
```

The following example configures the DNS servers.

```
{
   "dns_servers": [{
      "ip": "1.1.1.10",
      "priority": 1
```

```
   },
   {
      "ip": "2.2.2.20",
      "priority": 2
   },
      ...
   {
      "ip": "3.3.3.30",
      "priority": 3
   }]
}
```

The following example configures the proxy server.

```
{
   "proxy": {
      "enabled": true,
      "ip": "1.1.1.1",
      "password": "password",
      "port": 11,
      "userid": "userid"
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/aicc/network/hostname

Use this REST API to retrieve the Lenovo XClarity Administrator hostname.

HTTP methods

GET

GET /aicc/network/hostname

Use this method to return the Lenovo XClarity Administrator hostname.

Authentication

Authentication is not required.

Request URL

`GET https://{management_server_IP}/aicc/network/hostname`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
hostname	String	XClarity Administrator hostname

The following example is returned if the request is successful.

```
{
   "hostname": "localhost"
}
```

/aicc/network/interfaces/*{id}*

Use this REST API to retrieve or configure information about the Lenovo XClarity Administrator network interfaces.

HTTP methods

GET, PUT

GET /aicc/network/interfaces/*{id}*

Use the method to retrieve the information about a specific Lenovo XClarity Administrator network interface.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/aicc/network/interfaces/{id}`

where *{id}* is the network interface ID, such as `eth0` or `eth1`.

Query parameters

None

Request body

None

Response codes

Code	Description
200	OK
404	Not found

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	String	Network interface ID (such as “eth0” or “eth1”)
ip_addresses	Array of objects	Information about the IP addresses
assign_method	String	Assignment method used for this IP address. This can be one of the following values. • **static** • **dhcp** • **auto**
ip	String	IPv4 or IPv6 address
ip_linklocal	String	Identifies whether this address is an IPv6 link local address. This can be one of the following values. • **true**. This address is an IPv6 link local address • **false**. This address is not an IPv6 link local address
prefix_length	Integer	Prefix length (in bits) for this IP address
version	Integer	Type of IP address. This can be one of the following values. • **4**. IPv4 addresses • **6**. IPv6 addresses
mac_address	String	MAC address
role	Array of strings	Roles that are performed by this network interface. This can be one or more of the following values. • **none** • **management** • **osdeployment** **Note:** The first network interface (for example, eth0), is always set to **management**. If a second network interface (for example, eth1) is added, you can use it for OS deployment.
rpf	String	*Reverse path forwarding* settings on the network interface. This can be one of the following values. • **Disabled**. Reverse path forwarding is disabled. • **RFC3704Strict**. Checks the source address of the incoming packet against the Forwarding Information Base (FIB). If packet is received on the interface that would be use to forward the traffic to the source of the packet, then the packets are allowed to pass through. Otherwise, the packages are discarded. • **RFC3704Loose**. Checks the source address of the incoming packet against the Forwarding Information Base (FIB). If the source address is reachable from any interface on that route, the packets are allowed to pass through. Otherwise, the packages are discarded.

The following example is returned if the request is successful.

```
[{
    "id": "eth0",
    "ip_addresses": [{
        "assign_method": "static",
        "ip": "fe80:0:0:0:5054:ff:fe03:4da9%2",
        "ip_linklocal": "true",
        "prefix_length": 64,
        "version": 6
    },
    {
        "assign_method": "static",
        "ip": "10.243.2.189",
        "ip_linklocal": "false",
        "prefix_length": 20,
        "version": 4
    },
    {
        "assign_method": "dhcp",
        "ip": "0::0%0",
        "ip_linklocal": "false",
        "prefix_length": 64,
        "version": 6
    }],
    "mac_address": "52:54:00:03:4D:A9",
    "role": ["management"],
    "rpf": "RFC3704Strict"
}]
```


PUT /aicc/network/interfaces/*{id}*

Use this method to configure the settings for a specific network interface.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/aicc/network/interfaces/{id}`

where *{id}* is the network interface ID, such as eth0 or eth1.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
id	Required	String	Network interface ID (such as “eth0” or “eth1”)
ip_address	Required	Array	Information about the IP addresses
assign_method	Required	String	Assignment method used for this IP address. This can be one of the following values. • **static** • **dhcp** • **auto**

Attributes	Re-quired / Optional	Type	Description
ip	Required	String	IPv4 or IPv6 address
prefix_length	Required	Integer	Prefix length (in bits) for this IP address
version	Required	Integer	IP version of this address. This can be one of the following values. • **4** • **6**
role	Required	Array of strings	Roles that are performed by this network interface. This can be one or more of the following values. • **none** • **management** • **osdeployment** **Note:** The first network interface (for example, eth0), is always set to **management**. If a second network interface (for example, eth1) is added, you can use it for OS deployment.

The following example sets DHCP IPv6 address and static IPv4 address for the eth0 interface using PUT /aicc/network/interfaces/eth0.

```
{
   "id": "eth0",
   "ip_addresses": [{
      "assign_method": "dhcp",
      "version": 6
   },
   {
      "assign_method": "static",
      "ip": "1.1.1.1",
      "prefix_length": 24,
      "version": 4
   }],
   "role": ["management"]
}
```

The following example sets an IPv6 address using auto configuration for the eth1 interface using PUT /aicc/network/interfaces/eth1.

```
{
    "id": "eth1",
    "ip_addresses": [{
        "assign_method": "auto",
        "version": 6
    }]
   "role": ["osdeployment"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMNM00007I",
      "text": "The network specified configuration has been set successfully.",
      "recovery": {
         "text": "",
         "url": ""
      },
      "explanation": "The user has set a new network configuration."
   }]
}
```

/aicc/network/ipdisable

Use this REST API to retrieve or modify the IP address enablement state.

HTTP methods

GET, PUT

GET /aicc/network/ipdisable

Use the method to retrieve the enablement state of IPv4 and IPv6 addresses.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/aicc/network/ipdisable`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
ip_status		Array of objects	Information about the enablement state for IPv4 and IPv6 addresses
	ip_version	Integer	Type of IP address. This can be one of the following values. • **4**. IPv4 addresses • **6**. IPv6 addresses
	ip_disable	Integer	Indicates whether the IP addresses are enabled or disabled. This can be one of the following values. • **0**. Enable the specified addresses. • **1**. Disable the specified addresses.

The following example is returned if the request is successful.

```
{
   "ip_status": [{
      "ip_disable": 0,
      "ip_version": 4
   },
   {
      "ip_disable": 0,
      "ip_version": 6
   }]
}
```

PUT /aicc/network/ipdisable

Use this method to enable or disable IPv4 or IPv6 addresses. You must enable or disable the IP addresses one at a time.

Authentication

Authentication with username and password is required.

Request URL

```
PUT https://{management_server_IP}/aicc/network/ipdisable
```

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
ip_version	Required	Integer	Type of IP address. This can be one of the following values. • **4**. IPv4 addresses • **6**. IPv6 addresses
ip_disable	Required	Integer	Indicates whether the IP addresses are enabled or disabled. This can be one of the following values. • **0**. Enable the specified addresses. • **1**. Disable the specified addresses.

The following example enables IPv4 addresses:

```
{
   "ip_version" : 4,
   "ip_disable" : 0
}
```

The following example disables IPv4 addresses:

```
{
   "ip_version" : 4,
   "ip_disable" : 1
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/aicc/network/routes

Use this REST API to retrieve or configure information about Lenovo XClarity Administrator routes.

HTTP methods

GET, PUT

GET /aicc/network/routes

Use the method to retrieve information about all Lenovo XClarity Administrator routes.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/aicc/network/routes`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
routes		Array	Information about network routes
	destination	String	Destination IPv4 or IPv6 address for this route. This attribute is not returned for default routes.
	dev	String	Device that is used to connect to the device that is specified by **nexthop** (either “eth0” or “eth1”). This attribute is not returned for default routes.
	ip_version	Integer	IP version of this route. This value is either “4” or “6”
	nexthop	String	IP address of the router that is used to forward packets to the address that is specified by **destination**
	prefix_len	Integer	Number of bits in the network mask, or the prefix that is to be applied to the device that is specified by **destination** to get the subnet. This can be one of the following values. • **0**. Default route. • **32**. If the value of **ip_version** is 4, this indicates a host route. • **128**. If the value of **ip_version** if 6, this indicates a host route. All other values are network routes.

The following example is returned if the request is successful.


```
{
   "routes": [{
      "dev": "eth0",
      "destination": "100.10.10.10",
      "ip_version": 4,
      "nexthop": "192.168.56.1",
      "prefix_len": 32
   },
   {
      "dev": "eth0",
      "destination": "10.10.10.0",
      "ip_version": 4,
      "nexthop": "192.168.56.1",
      "prefix_len": 24
   },
   {
      "ip_version": 4,
      "nexthop": "10.0.3.2",
      "prefix_len": 0
   },
   {
      "dev": "eth1",
      "destination": "2001:db7:1::",
      "ip_version": 6,
      "nexthop": "2002:97b:c2bb:83d:5054:ff:fe2c:eefe",
      "prefix_len": 64
   },
   {
      "dev": "eth1",
      "destination": "2002:97b:face:83d:5054:ff:fe2c:eefe",
      "ip_version": 6,
      "nexthop": "2002:97b:c2bb:83d:5054:ff:fe2c:eefe",
      "prefix_len": 128
   }]
}
```


PUT /aicc/network/routes

Use this method to configure the Lenovo XClarity Administrator route settings.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/aicc/network/routes`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
routes	Required	Array	Information about network routes
destination	Optional	String	Destination IPv4 or IPv6 address for this route

Attributes	Re-quired / Optional	Type	Description
dev	Required	String	Interface to be used to connect to the device that is specified by **nexthop** (either “eth0” or “eth1”)
ip_version	Required	Integer	IP version of this route. This value is either “4” or “6.”
nexthop	Required	String	IP address of the router to be used to forward packets to the address that is specified by **destination**
prefix_len	Optional	Integer	Number of bits in the network mask, or the prefix that is to be applied to the device that is specified by **destination** to get the subnet. This can be one of the following values. • **0**. Default route. • **32**. If the value of **ip_version** is 4, this indicates a host route. • **128**. If the value of **ip_version** if 6, this indicates a host route. All other values are network routes.

The following example sets the IPv4 default route.

```
{
   "routes": [{
      "ip_version": 4,
      "nexthop": "192.168.56.1",
      "prefix_len": 0
   }]
}
```

The following example sets an IPv4 route.

```
{
   "routes": [{
      "destination": "100.10.10.10",
      "dev": "eth0",
      "ip_version": 4,
      "nexthop": "192.168.56.1",
      "prefix_len": 32
   }]
}
```

The following example sets the default IPv6 route.

```
{
   "routes": [{
      "ip_version": 6,
      "nexthop": "2002:97b:c2bb:83d:5054:ff:fe2c:eefe",
      "prefix_len": 0
   }]
}
```

The following example sets an IPv6 route.

```
{
   "routes": [{
      "destination": "2002:97b:c2bb:83d::",
      "dev": "eth1",
      "ip_version": 6,
      "nexthop": "2002:97b:c2bb:83d:5054:ff:fe2c:eefe",
      "prefix_len": 64
   }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/aicc/service/sftp/locks

Use this REST API to return a list of all SFTP service locks or start (enable) the SFTP service for a specific function and create a lock ID.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

GET, POST

GET /aicc/service/sftp/locks

Use this method to return a list of all SFTP service locks. The SFTP service is disabled by default.

Note: This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/aicc/service/sftp/locks`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
204	No Content	The request completed successfully, but no response content is returned.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	String	Lock ID. The ID is a 32 character string containing numbers and letters.
component	String	Predefined Lenovo XClarity Administrator component ID. This can be one of the following values. • **CN**. Console • **CP**. Server configuration patterns • **CR**. Virtual appliance • **DI**. Discovery and Inventory • **DM**. Data management • **DS**. Debug Shell • **EM**. Events and monitoring • **FC**. Operating-system deployment • **JM**. Jobs management • **MF**. Metric data collection and forwarders • **MI**. Data migration • **NM**. Network management • **RC**. Remote Control • **SE**. Security • **SP**. Switch ports • **SS**. Service and support • **ST**. Storage management • **TS**. ThinkServer and Thinksystem management • **UP**. Updates • **UI**. User Interface
creationTimestamp	String	Timestamp when the lock was created This timestamp is specified using ISO-8601 format (for example, 2019-05-02T19:28:14.000Z). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
expirationTimeOut	Integer	Number of seconds after which the lock expires When the lock expires, the lock ID is deleted and if there are no other locks, the SFTP service is stopped (disabled).

The following example is returned if the request is successful.

```
[{
   "id": "AB3L4N5L6N9D8FVLSDLSOS223JSNLSE3",
   "component": "UP",
   "creationTimestamp": "2022-09-09T01:46:08Z",
   "expirationTimeOut": 1200
},
{
   "id": "FE3L4N5L6N9D8FVLSDLSOS223JSNLSE3",
   "component": "UP",
   "creationTimestamp": "2022-09-09T01:46:12Z",
```

```
   "expirationTimeOut": 1200
}]
```

POST /aicc/service/sftp/locks

Use this method to start (enable) the SFTP service for a specific function and acquire an SFTP service lock by creating a lock ID.

Notes:

- You must be a member of a user group to which the predefined **Supervisor** role is assigned.
- This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/aicc/service/sftp/locks`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
component	Required	String	Predefined Lenovo XClarity Administrator component ID. This can be one of the following values. • **CN**. Console • **CP**. Server configuration patterns • **CR**. Virtual appliance • **DI**. Discovery and Inventory • **DM**. Data management • **DS**. Debug Shell • **EM**. Events and monitoring • **FC**. Operating-system deployment • **JM**. Jobs management • **MF**. Metric data collection and forwarders • **MI**. Data migration • **NM**. Network management • **RC**. Remote Control • **SE**. Security • **SP**. Switch ports • **SS**. Service and support • **ST**. Storage management • **TS**. ThinkServer and Thinksystem management • **UP**. Updates • **UI**. User Interface
expirationTimeOut	Required	Integer	Amount of time, in seconds, after which the lock expires When the lock expires, the lock ID is deleted and if there are no other locks, the SFTP service is stopped (disabled).

The following example starts the SFTP service for the updates function and deletes the lock ID after 20 minutes.

```
{
   "component": "UP",
   "expirationTimeOut": 1200
}
```

Response codes

Code	Description	Comments
201	Created	One or more new resources were successfully created.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

If the SFTP service is successfully locked, the lock ID is returned in the location field in response header, for example:

```
location:/aicc/service/sftp/locks/FE3L4N5L6N9D8FVLSDLSOS223JSNLSE3
```

Response body

Attributes	Type	Description
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      }
```

```
    }]
}
```

/aicc/service/sftp/locks/*{id}*

Use this REST API to return information about a specific SFTP service lock or release a specific SFTP service lock.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

GET, DELETE

GET /aicc/service/sftp/locks/*{id}*

Use this method to return information about a specific SFTP service lock.

Note: This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/aicc/service/sftp/locks/{id}`

where *{id}* is the ID of the SFTP service lock. To obtain the lock ID, use GET /aicc/service/sftp/locks.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	String	Lock ID. The ID is a 32 character string containing numbers and letters.
component	String	Predefined Lenovo XClarity Administrator component ID. This can be one of the following values. • **CN**. Console • **CP**. Server configuration patterns • **CR**. Virtual appliance • **DI**. Discovery and Inventory • **DM**. Data management • **DS**. Debug Shell • **EM**. Events and monitoring • **FC**. Operating-system deployment • **JM**. Jobs management • **MF**. Metric data collection and forwarders • **MI**. Data migration • **NM**. Network management • **RC**. Remote Control • **SE**. Security • **SP**. Switch ports • **SS**. Service and support • **ST**. Storage management • **TS**. ThinkServer and Thinksystem management • **UP**. Updates • **UI**. User Interface
creationTimestamp	String	Timestamp when the lock was created This timestamp is specified using ISO-8601 format (for example, 2019-05-02T19:28:14.000Z). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
expirationTimeOut	Integer	Number of seconds after which the lock expires When the lock expires, the lock ID is deleted and if there are no other locks, the SFTP service is stopped (disabled).

The following example is returned if the request is successful.

```
{
   "id": "AB3L4N5L6N9D8FVLSDLSOS223JSNLSE3",
   "component": "UP",
   "creationTimestamp": "2022-09-09T01:46:08Z",
   "expirationTimeOut": 1200
}
```

DELETE /aicc/service/sftp/locks/*{id}*

Use this method to release a specific SFTP service lock by deleting a specific lock ID and, if all locks are deleted, stop (disable) the SFTP service (unless dbgshell account exist on the Lenovo XClarity Administrator instance).

Notes:

- You must be a member of a user group to which the predefined **Supervisor** role is assigned.
- This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
DELETE https://{management_server_IP}/aicc/service/sftp/locks/{id}
```

where *{id}* is the ID of the SFTP service lock. To obtain the lock ID, use GET /aicc/service/sftp/locks.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "text": "The request completed successfully.",
```

```
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      }
   }]
}
```

/aicc/subscriptions

Use this REST API to retrieve or add a Lenovo XClarity Administrator subscriptions. When you add a subscription, you will receive notifications for all network related changes.

HTTP methods

GET, POST

GET /aicc/subscriptions

Use the method to retrieve information about all Lenovo XClarity Administrator subscriptions.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/aicc/subscriptions`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	Integer	Subscription ID
monitor_uri	String	Network-related resource that is to be monitored by XClarity Administrator If **monitor_uri** is set to “/aicc” or “”, every /aicc URI is monitored. If **monitor_uri** is set to “”, IP change notifications are received through DHCP.

Attributes	Type	Description
submonitor_uri	String	Subresource to be monitored by XClarity Administrator. You will receive notifications for only this resource
uri	String	Resource to which XClarity Administrator writes a POST when XClarity Administrator detects a change in monitored resource The specified URI must be able to accept POST requests, where the body of the POST matches the JSON PUT to **monitor_uri**.

The following example is returned if the request is successful.

```
[{
   "id": 1,
   "monitor_uri": "/aicc/network/interfaces",
   "submonitor_uri": "",
   "uri": "/osdeployment/rest/internal/event/aicc"
},
{
   "id": 2,
   "monitor_uri": "/aicc",
   "submonitor_uri": "/ntp",
   "uri": "/ntpNotification"
},
{
   "id": 3,
   "monitor_uri": "/aicc/network/interfaces",
   "submonitor_uri": "",
   "uri": "/netchangenotsec"
}]
```

POST /aicc/subscriptions

Use the method to add a subscription to Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/aicc/subscriptions`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
monitor_uri=*{URI}*	Optional	String	Network-related resource that is to be monitored by XClarity Administrator If **monitor_uri** is set to “/aicc” or “”, every /aicc URI is monitored. If **monitor_uri** is set to “”, IP change notifications are received through DHCP.
submonitor_uri=*{URI}*	Optional	String	Subresource to be monitored by XClarity Administrator. You will receive notifications for only this resource. This can be one of the following values. • address • DDNSenabled • DNSenabled • dnsHostnames • domainName • embeddedHypervisorPresence • gateway • globalIPv6enabled • hostConfig • hostMacAddresses • hostname • id • ipInterfaces • ipv4Addresses • IPv4assignments • IPv4DHCPmode • IPv4enabled • ipv4ServiceAddress • ipv6Addresses • IPv6assignments • IPv6DHCPenabled • IPv6enabled • ipv6ServiceAddress • IPv6statelessEnabled • IPv6staticEnabled • IPversionPriority • isConnectionTrusted • isRemotePresenceEnabled • label • macAddresses • mgmtProcIPaddress • name • prefix • priIPv4userDNSserver • priIPv6userDNSserver • scope • secIPv4userDNSserver • secIPv6userDNSserver • serviceHostName • secIPv6userDNSserver • secIPv4userDNSserver • source • subnet • type • terIPv4userDNSserver

Attributes	Re-quired / Optional	Type	Description
			• terIPv6userDNSserver
uri=*{URI}*	Required	String	Resource to which XClarity Administrator writes a POST when XClarity Administrator detects a change in monitored resource The specified URI must be able to accept POST requests, where the body of the POST matches the JSON PUT to **monitor_uri**.

The following example adds a subscription that monitors all network-related changes.

```
{
    "monitor_uri": "/aicc",
    "uri": "/testsubscriber"
}
```

The following example adds a subscription that monitors all NTP-related network changes.

```
{
   "monitor_uri": "/aicc",
   "submonitor_uri": "/ntp",
   "uri": "/ntpNotification"
}
```

Response codes

Code	Description	Comments
201	Created	One or more new resources were successfully created.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	Integer	Subscription ID
monitor_uri	String	Network-related resource that is to be monitored by XClarity Administrator If **monitor_uri** is set to “/aicc” or “”, every /aicc URI is monitored. If **monitor_uri** is set to “”, IP change notifications are received through DHCP.
submonitor_uri	String	Subresource to be monitored by XClarity Administrator. You will receive notifications for only this resource
uri	String	Resource to which XClarity Administrator writes a POST when XClarity Administrator detects a change in monitored resource The specified URI must be able to accept POST requests, where the body of the POST matches the JSON PUT to **monitor_uri**.

The following example is returned when a subscription is created that monitors all network-related changes.

```
{
   "id": 2,
   "monitor_uri": "/aicc",
   "submonitor_uri": "",
   "uri": "/ntpNotification"
}
```

The following example is returned when a subscription is created that monitors all NTP-related network changes.

```
{
   "id": 6,
   "monitor_uri": "/aicc",
   "submonitor_uri": "/ntp",
   "uri": "/ntpNotification"
}
```

/aicc/subscriptions/*{id}*

Use this REST API to retrieve information about or delete a specific Lenovo XClarity Administrator subscription.

HTTP methods

GET, DELETE

DELETE /aicc/subscriptions/*{id}*

Use the method to a specific Lenovo XClarity Administrator subscription.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/aicc/subscriptions/{id}`

where *{id}* is the subscription ID. To obtain the subscription ID, use the GET /aicc/subscriptions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

GET /aicc/subscriptions/*{id}*

Use this method to return information about a specific Lenovo XClarity Administrator subscriptions.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/aicc/subscriptions/{id}`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	Integer	Subscription ID
monitor_uri	String	Network-related resource that is to be monitored by XClarity Administrator If **monitor_uri** is set to “/aicc” or “”, every /aicc URI is monitored. If **monitor_uri** is set to “”, IP change notifications are received through DHCP.
submonitor_uri	String	Subresource to be monitored by XClarity Administrator. You will receive notifications for only this resource
uri	String	Resource to which XClarity Administrator writes a POST when XClarity Administrator detects a change in monitored resource The specified URI must be able to accept POST requests, where the body of the POST matches the JSON PUT to **monitor_uri**.

The following example is returned if the request is successful.

```
{
   "id": 2,
   "monitor_uri": "/aicc",
   "submonitor_uri": "/ntp",
   "uri": "/ntpNotification"
```

```
}
```

/FQDNConfigRequest

Use this REST API to modify the management server's fully-qualified domain name (FQDN) and DNS configuration on managed devices with IMM2, XCC, and CMM or validates communication between the management server and managed devices using the set values.

Important: You must be a member of a user group to which the predefined **Supervisor** role is assigned.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

POST

POST /FQDNConfigRequest

Use this method to modify the management server's fully-qualified domain name (FQDN) and DNS configuration on managed devices with IMM2, XCC, and CMM or validates communication between the management server and managed devices using the set values.

This method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Important: You must be a member of a user group to which the predefined **Supervisor** role is assigned.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/FQDNConfigRequest`

Query parameters

Parameter	Required / Optional	Description
validationOnly=*{Boolean}*	Optional	Indicates whether to validate communication or push FQDN and DNS configuration to managed devices. This can be one of the following values. • **true**. Validates and returns a list of UUIDs for applicable managed devices to modify the management server's FQDN and DNS configuration. • **false**. (default) Modifies the management server's FQDN and DNS configuration on managed devices

The following example validates communication with managed devices.

```
POST https://192.0.2.0/FQDNConfigRequest?validationOnly=true
```

The following example modifies the management server's FQDN and DNS configuration on managed devices.

```
POST https://192.0.2.0/FQDNConfigRequest
```

Request body

If **validationOnly=false**, specify the following attributes in the request body. Otherwise, there is no request body.

Attributes	Required / Optional	Type	Description
dns_action	Required	String	Indicates the action to use to modify DNS entries on managed devices. This can be one of the following values. • **NONE**. No action is taken. • **ADD**. Appends entries if different than existing. This is applicable only if **fqdnEnabled** is set to **true**. • **UPDATE**. Replace existing with given entries. This is applicable only if **fqdnEnabled** is set to **true**. • **DELETE**. Removes DNS entries that matches with the given entries. This is applicable only if **fqdnEnabled** is set to **false**. • **DELETE_ALL**. Removes all DNS entries. This is applicable only if **fqdnEnabled** is set to **false**.
dns_servers	Required	Array of objects	Information about IP addresses that are used to resolve DNS queries
ip	Required	String	IP address of the DNS entry
priority	Required	Integer	Relative priority of the DNS entry into available slots This is applicable only if **fqdnEnabled** is set to **true**.
fqdn	Required	String	Fully qualified domain name of the management server
fqdnEnabled	Required	Boolean	Indicates whether to use the management servers' FQDN to communicate with managed devices. • **true** • **False**.
uuids	Required	Array of strings	List of UUIDs of managed devices for which FQDN and DNS configuration to be modified

The following example adds the management server's FQDN and DNS configuration to three specific managed devices.

```
{
   "dns_action": "ADD",
   "dns_servers": [{
      "ip": "192.0.2.10",
      "priority": 1
   },
   {
      "ip": "192.0.2.11",
      "priority": 2
   }],
   "fqdn": "labs.company.com",
   "fqdnEnabled": true,
   "uuids": [ "20220629175643902E1606DE5E262002", "14DEE51A0682433FB1D5B4A6B5DB282F",
              "20220629175643902E1606DE5E262002" ]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The following attribute is returned if the request is successful and **validationOnly=true**. Otherwise, no response is returned.

Attributes	Type	Description
uuids	Array of strings	List of UUIDs of managed devices for which FQDN and DNS configuration was updated

The following example is returned if the request is successful.

```
{
   "uuids": [ "20220629175643902E1606DE5E262002", "14DEE51A0682433FB1D5B4A6B5DB282F",
              "20220629175643902E1606DE5E262002" ]
}
```

Chapter 3. Discovery and management

The following resources are available for performing discovery, manage, and unmanage functions.

/csvRequest

Use this REST API to manage devices using a bulk-import CSV file.

HTTP methods

POST

POST /csvRequest

Use this method to manage devices using a bulk-import CSV file.

Notes:

- The bulk import file must be in a comma-delimited CSV format.
- When managing switches using bulk import, HTTPS is enabled on the switch, and NTP clients on the switch are configured to use the NTP settings from the management server. To change these setting, use POST /manageRequest.

For information about downloading a template (Excel or CSV format) and completing the bulk import file, see Managing systems in the Lenovo XClarity Administrator online documentation.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/csvRequest
```

Query parameters

Parameters	Required / Optional	Description
validationOnly=*{Boolean}*	Optional	Indicates whether to only validate the bulk-import (CSV) file. This can be one of the following values. • **true**. Validates the contents of the bulk-import CSV file, but does not manage the devices. • **false**. (default) Manages devices that are defined in the bulk-import CSV file.

The following example validates the bulk-import CSV file.

```
POST https://192.0.2.0/csvRequest?validationOnly=true
```

The following example manages devices that are defined in the bulk-import CSV file.

```
POST https://192.0.2.0/csvRequest
```

Request body

Use the “multipart/form-data” media type to import the CSV file. Use the attributes in the following table as the multipart name in the body. For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage.

Request example

HTTP Header

```
Content-Type: multipart/form-data; boundary=AaB03x
```

Request body

```
--AaB03x
    Content-Disposition: form-data; name="uploadedfile"; filename="bulk_manage.csv"
    Content-Type: application/octet-stream
--AaB03x--
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
201	Created	One or more new resources were successfully created.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

If this POST method results in a job getting started, the response header includes a URI in the form /augusta/discovery/jobs/*{job_id}* (for example, `/augusta/discovery/jobs/12`) that represents the job that is monitored by the management server. You can use GET /csvRequest/jobs/*{job_id}* to determine the status of the job.

If a job was not successfully started, refer to the response code and response body for details.

Note: A successful response indicates that the request was successfully transmitted and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Response body

Table 1. Validate in the bulk-import file

The following is response body is returned when **validateOnly=true**. A JSON object is returned for each row in the bulk-import file.

Table 1. Validate in the bulk-import file (continued)

Attributes	Type	Description
currentIP	String	IP address or hostname for the device
currentUserName	String	User name for authenticating to the device, if applicable
displayName	String	Device display name
failedValidationMessages	Array of strings	Input errors for the device
roleGroups	Array of strings	List of role groups that are permitted to view and manage the device. To get a list of available role groups, use GET /roleGroups. You can specify only role groups to which the current user belongs. If you do not specify the **roleGroups** attribute, the default roles groups are assigned. You can obtain the list of default role group using GET /resourceAccessControl. If you specify **roleGroup** with an empty or null value, role groups are not assigned. **Note:** If you add devices to a managed chassis, the new devices will belong to the same role groups as the chassis.
managedAuthentication	Boolean	Indicates whether to use local authentication instead of XClarity Administrator managed authentication. For more information about managed and local authentication, see Managing the authentication server in the Lenovo XClarity Administrator online documentation. This can be one of the following values. • **true**. Use XClarity Administrator managed authentication. • **false**. Use local authentication.
rowNumber	Integer	Row in the CSV file in which the device input is specified
serialNumber	String	Device serial number
storedCredentialsID	String	Stored credential ID that is associated with the device, if applicable. To find the stored credential ID, use GET /storedCredentials.
type	String	Device type. This can be one of the following values. • **Chassis**. • **Filler** • **Rack** • **Server** • **Storage** • **Switch**

The following example is returned when **validateOnly=true**.

```
[{
   "currentIP": "10.243.3.37",
   "currentUsername": "USERID",
   "displayName": null,
   "failedValidationMessages": [],
   "roleGroups": ["LXC-SUPERVISOR","LXC-HW-ADMIN",]
   "rowNumber": 2,
   "serialNumber": null,
   "storedCredentialsId": null,
   "type": "flexchassis",
   "managedAuthEnabled": null
},
...,
```

```
{
   "currentIP": "",
   "currentUserName": "JOHN",
   "displayName": "Server1"
   "failedValidationMessages": ["Missing IP address or hostname","Invalid device type"],
   "roleGroups": "",
   "managedAuthentication": false,
   "rowNumber": 1,
   "serialNumber": "",
   "storedCredentialsID": null,
   "type": "Server"
}]
```

Table 2. Manage devices in the bulk-import file

The following is response body is returned when **validateOnly=false**.

Attributes	Type	Description
result	String	Results of this operation. This can be one of the following values. • **success** • **warning** • **failure**
statusCode	String	Response code
statusDescription	String	Response description
messages	Array of objects	Information about zero or more messages
id	String	Message identifier of a returned message
explanation	String	Additional information to clarify the reason for the message
recovery	String	User actions that can be taken to recover from the event
recoveryUrl	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned when **validateOnly=false**.

```
{
   "result": "failure"
   "statusCode": 400,
   "statusDescription": "There was an error parsing the input to the bulk import request.",
   "messages": [{
      "id": "FQXDM0558G",
      "explanation": "Field \"ManagedAuthEnabled\" is not allowed when field \"Type\" has
                      value \"flexchassis\".",
      "recovery": "Correct the default values that are specified in the bulk import dialog and
                   the  data on line 5 of the CSV file, and try again.",
      "recoveryUrl": "",
      "text": "A field was specified that is not compatible with the value of another field."
   },
   {
      "id": "FQXDM0557G",
      "explanation": "Field \"StoredCredentialsId\" is not allowed when field \"NewPassword\"
                      is specified.",
      "recovery": "Correct the default values entered in the bulk import dialog and/or the data
                   on line 6 of the CSV file and try again.",
      "recoveryUrl": "",
```

```
      "text": "Incompatible fields were specified."
   }]
}
```

/csvRequest/jobs/*{job_id}*

Use this REST API to monitor the status of a management request management request using a bulk-import CSV file.

HTTP methods

GET

GET /csvRequest/jobs/*{job_id}*

Use this method to monitor the status of a management request using a bulk-import CSV file.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/csvRequest/jobs/{job_id}`

where *{job_id}* is the job ID that was returned by the POST /csvRequest method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
progress	Double	Percentage complete of the bulk management job. This can be one of the following values. • **0.0**. Created. • **50.0**. In progress. • **100.0**. Complete.
results	Array of objects	Results of the bulk management jobs
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID
messageAttributes	String	This can be one of the following values. • device IP if not null • device serial number if not null • device UUID
progress	Long	Percentage complete of the management job. If the job is complete, “JOB_DONE” is returned
result	String	Result of the request. This can be one of the following values. • **INCOMPLETE**. The request is not complete. • **SUCCESS**. The request was successful. • **FAILED**. The request failed.
resultLongDescription	String	Detailed description of the result
resultShortDescription	String	Summarized description of the result
status	Object	Status details about the list of management steps
description	Array of objects	List of message descriptions
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID for the set of management steps
percentage	Long	Percentage complete of the set of management steps
state	String	State of the set of management steps. The can be one of the following values. • **Error** • **Running** • **Running_Complete**
substatus	Array of objects	Results of each of the task in the management job
completed	Boolean	Indicates whether the task completed. This can be one of the following values. • **true**. The step has completed. • **false**. The task has not completed.
id	String	Name of the management step
longDescription	String	Long message description

Attributes	Type	Description
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID of the management step
progress	Integer	Progress of the management step
shortDescription	String	Short message description
started	Boolean	Indicates if the management step has started. This can be one of the following values. • **true**. The step has started. • **false**. The step has not started.
status	Object	Status details about the individual management step
percentage	Integer	Percentage complete of the management step
state	String	State of the management step. This can be one of the following values. • **ERROR** • **PENDING** • **RUNNING** • **RUNNING_COMPLETE**
substatus	Array of objects	Results of each of the subtask in the management job
userAction	String	Any user action that is required
taskid	Integer	Task ID
time_spent	Long	Duration of the task in milliseconds
uuid	String	UUID
status		Status of the management job. This can be one of the following values. • **0**. Created. • **50**. Incomplete. • **100**. Done. • **101**. Done_Warnimg.

The following example is returned if the request is successful.


```
{
   "progress": 17.647058823529413,
   "results": [{
      "messageBundle": "com.lenovo.lxca.discovery.bundle.rest.messages",
      "messageID": "0509_LONG",
      "messageParameters": "10.243.3.55"
      "progress": 17.647058823529413,
      "result": "INCOMPLETE",
      "resultLongDescription": "Management job is incomplete",
      "resultShortDescription": "Incomplete",
      "status": {
         "description": [{
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1014_LONG"
         }],
         "percentage": 17.647058823529413,
         "state": "Running",
```

```
"substatus": [{
   "completed": true,
   "id": "STARTING",
   "longDescription": "Starting device management job",
   "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
   "messageID": "1000_SHORT",
   "progress": 100,
   "shortDescription": "Starting",
   "started": true,
   "status": {
      "percentage": 100,
      "state": "Complete"
   },
   "userAction": ""
},
{
   "completed": true,
   "id": "NETWORK_CHOICE",
   "longDescription": "Choosing best network path to manage the device",
   "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
   "messageID": "1001_SHORT",
   "progress": 100,
   "shortDescription": "Network choice",
   "started": true,
   "status": {
      "percentage": 100,
      "state": "Complete"
   },
   "userAction": ""
},
{
   "completed": true,
   "id": "DESCRIPTOR",
   "longDescription": "Creating hardware descriptor",
   "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
   "messageID": "1002_SHORT",
   "progress": 100,
   "shortDescription": "Descriptor",
   "started": true,
   "status": {
      "percentage": 100,
      "state": "Complete"
   },
   "userAction": ""
},
{
   "completed": true,
   "id": "LOGIN",
   "longDescription": "Logging in to device",
   "messageID": "1003_SHORT",
   "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
   "progress": 100,
   "shortDescription": "Login",
   "started": true,
   "status": {
      "percentage": 100,
      "state": "Complete"
   },
   "userAction": ""
},
{
```

```
      "completed": true,
      "id": "DUPLICATE_CHECK",
      "longDescription": "Checking for duplicates of device management",
      "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
      "messageID": "1004_SHORT",
      "progress": 100,
      "shortDescription": "Duplicate check",
      "started": true,
      "status": {
         "percentage": 100,
         "state": "Complete"
      },
      "userAction": ""
   },
   {
      "completed": false,
      "id": "INVENTORY",
      "longDescription": "Collecting device inventory",
      "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
      "messageID": "1005_SHORT",
      "progress": 0,
      "shortDescription": "Inventory",
      "started": true,
      "status": {
         "percentage": 0,
         "state": "Running",
         "substatus": [{
            "completed": false,
            "id": "INV_CHASSIS",
            "longDescription": "Collecting chassis inventory",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1006_SHORT",
            "progress": 0,
            "shortDescription": "Chassis inventory",
            "started": true,
            "status": {
               "percentage": 0,
               "state": "Running"
            },
            "userAction": ""
         },
         {
            "completed": false,
            "id": "INV_NODES",
            "longDescription": "Collecting node inventory",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1007_SHORT",
            "progress": 0,
            "shortDescription": "Node inventory",
            "started": true,
            "status": {
               "percentage": 0,
               "state": "Running"
            },
            "userAction": ""
         },
         {
            "completed": false,
            "id": "INV_IOMS",
            "longDescription": "Collection I/O module inventory",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
```

```
            "messageID": "1008_SHORT",
            "progress": 0,
            "shortDescription": "I/O module inventory",
            "started": true,
            "status": {
               "percentage": 0,
               "state": "Running"
            },
            "userAction": ""
         }]
      },
      "userAction": ""
   },
   {
      "completed": false,
      "id": "INTEROP_CHECK",
      "longDescription": "Verifying device interoperability",
      "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
      "messageID": "1009_SHORT",
      "progress": 0,
      "shortDescription": "Interoperability check",
      "started": false,
      "status": {
         "percentage": 0,
         "state": "Pending"
      },
      "userAction": ""
   },
   {
      "completed": false,
      "id": "CONFIGURATION",
      "longDescription": "Configuring device for management",
      "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
      "messageID": "1010_SHORT",
      "progress": 0,
      "shortDescription": "Configuration",
      "started": false,
      "status": {
         "percentage": 0,
         "state": "Pending",
         "substatus": [{
            "completed": false,
            "id": "CFG_NTP",
            "progress": 0,
            "longDescription": "Configuring NTP",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1011_SHORT",
            "started": false,
            "status": {
               "percentage": 0,
               "state": "Pending"
            },
            "shortDescription": "NTP",
            "userAction": ""
         },
         {
            "completed": false,
            "id": "CFG_DNS_UPD",
            "longDescription": "Updating DNS servers ip addresses on CMM as part of the manage chassis
                                process.",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
```

```
            "messageID": "1067_SHORT",
            "progress": 0,
            "shortDescription": "Updating DNS servers ip addresses on CMM",
            "started": false,
            "status": {
               "percentage": 0,
               "state": "Pending"
            },
            "userAction": ""
         },
         {
            "completed": false,
            "id": "CFG_SECURITY",
            "longDescription": "Configuring security",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1012_SHORT",
            "progress": 0,
            "shortDescription": "Security",
            "started": false,
            "status": {
               "percentage": 0,
               "state": "Pending"
            },
            "userAction": ""
         },
         {
            "completed": false,
            "id": "CFG_CMGMT",
            "longDescription": "Putting device under centralized management",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1013_SHORT",
            "progress": 0,
            "shortDescription": "Centralized management",
            "started": false,
            "status": {
               "percentage": 0,
               "state": "Pending"
            },
            "userAction": ""
         }]
      },
      "userAction": ""
   },
   {
      "completed": false,
      "id": "CFG_CABINET",
      "longDescription": "Configuring Hardware location",
      "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
      "messageID": "1097_SHORT",
      "progress": 0,
      "status": {
         "percentage": 0,
         "state": "Pending"
      },
      "shortDescription": "Configuring Hardware location",
      "started": false,
      "userAction": ""
   }]
},
"taskid": 371,
"time_spent": 117527,
```

```
      "uuid": "48331a223bf34fba90732b379b837b9c"
   }],
   "status": "INCOMPLETE"
}
```

/discovery

Use this REST API to retrieve a list of devices discovered by SLP discovery.

HTTP methods

GET

GET /discovery

Use this method to return a list of devices discovered by SLP discovery.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/discovery`

Query parameters

Parameters	Required / Optional	Description
refresh=*{Boolean}*	Optional	Starts the SLP broadcast job to discover and update the list of discovered devices. This can be one of the following values. • **true**. Rediscovers and updates the list of discovered devices. • **false**. (Default) Returns list of devices that were already discovered.

The following example returns a list of discovered devices.

```
GET https://192.0.2.0/discovery
```

The following example discovers new devices and then returns an updated list of discovered devices.

```
GET https://192.0.2.0/discovery?refresh=true
```

Request body

None

Response codes

None

Response body

The attributes in the response body vary depending on the type of device that is discovered.

Attributes	Type	Description
chassisList	Array of objects	Information about each chassis that was discovered
cmmDisplayName	String	Chassis name that is provided by the CMM

Attributes	Type	Description
cmms	Array of objects	Information about the CMMs in the chassis
cmmDisplayName	String	Name of the CMM
firmware	Array of objects	Information about the CMM firmware
build	String	Firmware build
date	String	Firmware date
name	String	Firmware name
type	String	Firmware type
name	String	Hostname of the CMM
serialNumber	String	Serial number of the CMM
slots	Array of integers	Bay in the chassis where the CMM is installed
type	String	Resource type. This value is always **CMM**.
uuid	String	UUID of the CMM
displayName	String	Chassis name that is defined by the user
fruNumber	String	FRU part number for the chassis
hostname	String	Hostname of the chassis
ipAddresses	Array of strings	All IPv4 and IPv6 addresses for the chassis
machineType	String	Chassis machine type
managementPorts	Array of objects	List of management ports in the chassis
enabled	Boolean	Indicates whether the port enabled. This can be one of the following values. • **true**. The port is enabled. • **false**. The port is disabled.
port	Integer	Port number
protocol	String	Protocol that is running on the port (for example, http, https, or snmpv3)
model	String	Chassis model
name	String	Chassis name
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.

Attributes	Type	Description
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports managed authentication. • **false**. This device does not support managed authentication
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device
publicAccess	String	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
storedCredentials	Object	Information about the stored credential that is associated with this device, if applicable
description	String	Description of the stored credential
id	String	ID of the stored credential
userName	String	Name of the stored credential
uri	String	Chassis URI
serialNumber	String	Serial number for the chassis
status	Array	Current status of the chassis
message	String	Message
name	String	Name
type	String	Resource type. This value is always **Chassis**.
uuid	String	UUID for the chassis
discoveryInProgress	Boolean	Identifies whether the devices are being discovered
lastUpdateElapsedTime	Double	Amount of time since the last update
nodeList	Array	List of all rack and tower servers that were discovered
displayName	String	Name of the rack or tower server
enclosureFormFactor	String	(IMM, IMM2, XCC, or XCC2 only) Form factor of the chassis. This can be one of the following values. • **dense-computing** • **edge-computing** • **rack-tower**
firmware	Array of objects	List of firmware on the rack or tower server
build	String	Build level
date	String	Date
version	String	Build version
fruNumber	String	FRU number
hostname	String	Hostname of the rack or tower server
ipAddresses	Array of Strings	All IPv4 and IPv6 addresses for the rack or tower server

Attributes	Type	Description
machineType	String	Machine type of the rack or tower server
managementProcessor	String	Type of management controller. This can be one of the following values. • **integrated-management-module** • **integrated-management-module2** • **lenovo-xclarity-controller** • **chassis-management-module**
managementPorts	Array of objects	List of management ports in the rack or tower server
enabled	Boolean	Indicates if the port is enabled. One of the following values can be returned: • **true**. The port is enabled. • **false**. The port is not enabled.
port	Integer	Port number
protocol	String	Protocol running on the port (for example, http, https, or snmpv3)
model	String	Model of the rack or tower server
name	String	Name of the rack or tower server
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports the ability to choose managed authentication. • **false**. This device does not support the ability to choose managed authentication.
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device
publicAccess	String	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
storedCredentials	Object	Information about the stored credential that is associated with this device, if applicable
description	String	Description of the stored credential
id	String	ID of the stored credential
userName	String	Name of the stored credential
uri	String	Server URI
serialNumber	String	Serial number for the rack or tower server.
status	Object	Current status.

Attributes	Type	Description
manageable	Boolean	Indicates whether the rack or tower server is manageable. This can be one of the following values. • **true**. The port is enabled. • **false**. The port is not enabled.
message	String	Message
name	String	Name
subType	String	
type	String	Resource type. This can be one of the following values. • **Rack-Tower Server**. Converged, NeXtScale, System x or ThinkSystem server • **Lenovo ThinkServer**. ThinkServer server
uuid	String	UUID of the rack and tower server
rackswitchList	Array of objects	List of all top-of-rack switches that were discovered
displayName	String	Name of the top-of-rack switch
hostname	String	Hostname of the top-of-rack switch
ipAddresses	Array of Strings	All IPv4 and IPv6 addresses for the top-of-rack switch
machineType	String	machine type of the top-of-rack switch
managementPorts	Array of objects	This array is always empty.
model	String	Model of the top-of-rack switch
name	String	Name of the top-of-rack switch
os	String	Operating system. This can be one of the following values. • **CNOS** • **ENOS**
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This is always **false** for top-of-rack switches, meaning that local authentication is used.
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This is always **false** for top-of-rack switches, meaning that local authentication is used.
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device
publicAccess	String	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
storedCredentials	Object	Information about the stored credential that is associated with this device, if applicable
description	String	Description of the stored credential

Attributes	Type	Description
id	String	ID of the stored credential
userName	String	Name of the stored credential
uri	String	Switch URI
serialNumber	String	Serial number for the top-of-rack switch.
status	Object	Current status.
manageable	Boolean	Indicates whether the top-of-rack switch is manageable. This can be one of the following values • **true**. The switch is manageable. • **false**. The switch is not manageable.
message	String	Message
name	String	Name
type	String	Resource type. This value is always **Rackswitch**.
uuid	String	UUID of the top-of-rack switch
storageList	Array of objects	Information about each storage device that was discovered
displayName	String	Name of the storage device
hostname	String	Hostname of the storage device
ipAddresses	Array of strings	All IPv4 and IPv6 addresses for the storage device
firmware	Array of objects	List of firmware on the storage device
build	String	Build level.
date	String	Date
version	String	Build version
fruNumber	String	FRU number
machineType	String	Machine type of the storage device
managementPorts	Array of objects	List of management ports in the storage device
enabled	Boolean	Indicates if the port is enabled. This can be one of the following values. • **true**. The port is enabled. • **false**. The port is not enabled.
port	Integer	Port number
protocol	String	Protocol running on the port (for example, http, https, or snmpv3)
model	String	Model of the storage device.
name	String	Name of the storage device.
serialNumber	String	Serial number for the storage device
status	Object	Current status

Attributes	Type	Description
manageable	Boolean	Indicates whether the storage device is manageable. This can be one of the following values. • **true**. The storage device is manageable. • **false**. The storage device is not manageable.
name	String	Name
type	String	Resource type. This value is always **Lenovo Storage**.
uuid	String	UUID of the storage device
wwnn	String	WWNN of the storage device
xhmcList	Array	Information about each XClarity Administrator management server that was discovered.
hostname	String	Hostname of the XClarity Administrator management server
ipAddresses	Array of strings	All IPv4 and IPv6 addresses for the management server
managementPorts	Array of objects	List of management ports in the top-of-rack switch
enabled	Boolean	Indicates if the port is enabled. This can be one of the following values. • **true**. The port is enabled. • **false**. The port is not enabled.
port	Integer	Port number
protocol	String	Protocol running on the port (for example, http, https, or snmpv3)
name	String	Name of the management server
software	Array of objects	Information about the XClarity Administrator version
version	String	Version of XClarity Administrator that is installed
status	Object	Current status
manageable	Boolean	Indicates whether the management server is manageable. This can be one of the following values. • **true**. The management server is manageable. • **false**. The management server is not manageable.
manager-uuid	String	UUID of the management server
type	String	Resource type This value is always **Domain Manager**.
uuid	String	UUID of the management server

The following example is returned if the request is successful.


```
{
   "chassisList": [{
      "cmmDisplayName": "chassis-2",
      "cmms": [{
         "cmmDisplayName": "chassis-2",
         "firmware": [{
            "build": "1AON18B",
            "date": "2017-10-24",
            "name": "CMM Firmware",
            "type": "CMM Firmware"
```

```
      }],
      "name": "chassis-2",
      "serialNumber": "Y011BG78J093",
      "slots": [1],
      "type": "CMM",
      "uuid": "3d316351852111e78e4fbed8acb88dcf"
   }],
   "displayName": "chassis-2",
   "fruNumber": "81Y2893",
   "hostname": "chassis-2",
   "ipAddresses": ["10.240.60.50", "fe80::2e0:ecff:fe43:2c8b", "fe80::2e0:ecff:fe43:2c8c",
                   "fd55:faaf:e1ab:210f:2e0:ecff:fe43:2c8b"],
   "machineType": "7893",
   "managementPorts": [{
      "enabled": false,
      "port": 80,
      "protocol": "http"
   },
   ...,
   {
      "enabled": true,
      "port": 161,
      "protocol": "snmpv3"
   }],
   "model": "92X",
   "name": "chassis-2",
   "securityDescriptor": {
      "managedAuthEnabled": false,
      "managedAuthSupported": false,
      "publicAccess": false,
      "roleGroups": [],
      "uri": "chassis/5422200a92d34460b5c34c86f1d9ca9c"
   },
   "serialNumber": "100B2AA",
   "status": {
      "message": "Unmanaged",
      "name": "UNMANAGED"
   },
   "type": "Chassis",
   "uuid": "5422200a92d34460b5c34c86f1d9ca9c"
}],
"discoveryInProgress": false,
"lastUpdateElapsedTime": 1198900,
"nodeList": [{
   "displayName": "n6",
   "enclosureFormFactor": "rack-tower",
   "firmware": [{
      "build": "TCOO24A",
      "date": "2016/08/29",
      "version": "3.50"
   },
   {
      "build": "TBE126Q",
      "date": "2016/11/18",
      "version": "2.21"
   }],
   "fruNumber": "01KN187     ",
   "hostname": "cximmnode6",
   "ipAddresses": ["10.240.62.156", "fdea:14a7:304b:40::3:6",
                   "fd55:faaf:e1ab:210f:a94:efff:fe38:f5a1", "fe80::a94:efff:fe38:f5a1"],
   "machineType": "8869",
```

```
    "managementProcessor": "integrated-management-module2",
    "managementPorts": [{
       "enabled": true,
       "port": 5988,
       "protocol": "cimxml-http"
    },
    ...,
    {
       "enabled": true,
       "port": 623,
       "protocol": "rmcp"
    }],
    "model": "ACA",
    "name": "n6",
    "securityDescriptor": {
       "managedAuthEnabled": true,
       "managedAuthSupported": true,
       "publicAccess": false,
       "roleGroups": [],
       "uri": "nodes/0d5d0374dd3511e6b1e20894ef38f59c"
    },
    "serialNumber": "J1192GG",
    "server-type": "Rack-Tower Server",
    "status": {
       "manageable": true,
       "message": "Unmanaged",
       "name": "UNMANAGED"
    },
    "subType": "",
    "type": "Rack-Tower Server",
    "uuid": "0d5d0374dd3511e6b1e20894ef38f59c"
}],
"rackswitchList": [{
    "displayName": "lci-medium-10g-sw01",
    "hostname": "lci-medium-10g-sw01",
    "ipAddresses": ["10.240.62.159", "fdea:14a7:304b:40:0:0:4:3"],
    "machineType": "7159",
    "managementPorts": [],
    "model": "HCD (G8272)",
    "name": "lci-medium-10g-sw01",
    "os": "ENOS",
    "securityDescriptor": {
       "managedAuthEnabled": false,
       "managedAuthSupported": false,
       "roleGroups": [],
       "publicAccess": false,
       "uri": "switches/5C2719BC02553v5E885460D41B2E217CF"
    },
    "serialNumber": "Y05JJ11192MY",
    "status": {
       "manageable": true,
       "name": "UNMANAGED"
    },
    "type": "Rackswitch",
    "uuid": "5C2719BC025535E885460D41B2E217CF",
}],
"storageList": [],
"xhmcList": [{
    "hostname": "lci-lxca-ea14a7304b",
    "ipAddresses": ["10.240.62.163", "fdea:14a7:304b:40::1:2", "fe80::20c:29ff:fe23:1742"],
    "managementPorts": [{
```

```
            "enabled": true,
            "port": 443,
            "protocol": "https"
         }],
         "name": "LXCA - 172.20.250.48",
         "software": [{
            "version": "1.0"
         }],
         "status": {
            "manageable": true,
            "manager-uuid": null
         },
         "type": "Domain Manager",
         "uuid": "e75f3b1c87784420ae1ecf7bfd6b3d8e"
      }]
}
```

/discoveryConfigSettings

Use this REST API to retrieve information about and enable or disable the global discovery setting.

HTTP methods

GET, PUT

GET /discoveryConfigSettings

Use this method to return information about the global discovery setting.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/discoveryConfigSettings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
autoDiscoveryEnabled	Boolean	Indicates whether you can automatically discover baseboard management controllers using the SLP discovery method. This can be one of the following values. • **true**. Automatic discovery using SLP is enabled. • **false**. Automatic discovery using SLP is disabled.
registerRequestEnabled	Boolean	Indicates whether XClarity Administrator accepts discovery requests from a baseboard management controller when the management controller uses DNS to find XClarity Administrator instances. • **true**. Management controller can register with XClarity Administrator as a discovered device. • **false**. Management controller cannot register with XClarity Administrator as a discovered device.

The following example is returned if the request is successful.

```
{
   "autoDiscoveryEnabled": true,
   "registerRequestEnabled": true
}
```

PUT /discoveryConfigSettings

Use this method to enable or disable automatically discovering baseboard management controllers using the SLP discovery method.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/discoveryConfigSettings`

Query parameters

None

Request body

You can specify one of the following attributes in the request body.

Attributes	Re-quired / Optional	Type	Description
autoDiscoveryEnabled	Required	Boolean	Indicates whether you can automatically discover baseboard management controllers using the SLP discovery method. This can be one of the following values. • **true**. Enables automatic discovery using SLP. • **false**. Disables automatic discovery using SLP.
registerRequestEnabled	Required	Boolean	Indicates whether XClarity Administrator accepts discovery requests from a baseboard management controller when the management controller uses DNS to find XClarity Administrator instances. • **true**. Management controller can register with XClarity Administrator as a discovered device. • **false**. Management controller cannot register with XClarity Administrator as a discovered device.

The following example disables automatic SLP discovery.

```
{
   "autoDiscoveryEnabled": false
}
```

The following example accepts discovery requests from a baseboard management controller.

```
{
   "registerRequestEnabled": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/discoverRequest

Use this REST API to discover the manageable devices.

HTTP methods

POST

POST /discoverRequest

Use this method to discover manageable devices. The response header includes a URI that is associated with a job that indicates that a task was started.

Attention: This REST API does not support SLP discovery for the Lenovo ThinkSystem DB-series FC SAN switches and NVIDIA Mellanox switches. Use POST /manageRequest?discovery=true instead.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/discoverRequest`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
ipAddresses	Required	Array of strings	List of IP addresses for each device to be discovered

The following example discovers a manageable device.

```
[{
    "ipAddresses":["10.243.2.233"]
}]
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

If this POST method results in a job getting started, the response header includes a URI in the form /discoverRequest/jobs/*{job_id}* (for example, `/discoverRequest/jobs/12`) that represents the job that is monitored by the management server. You can use GET /discoverRequest/jobs/*{job_id}* to determine the status of the job. If a job was not successfully started, refer to the response code and response body for details.

Note: A successful response indicates that the request was successfully transmitted and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Response body

None

/discoverRequest/jobs/*{job_id}*

Use this REST API to monitor the status of a discovery request.

HTTP methods

GET

GET /discoverRequest/jobs/*{job_id}*

Use this method to monitor the status of a discovery request.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/discoverRequest/jobs/{job_id}`

where *{job_id}* is the job ID that was returned by the POST /discoverRequest method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
progress	Double	Percentage complete of the discovery job. This can be one of the following values. • **0.0**. Created. • **> 0.0**. In progress. • **100.0**. Complete.
result	Integer	Result of the job. This can be one of the following values. • **0**. Created. • **50**. In progress. • **100**. Complete.
chassisList	Array of objects	Information about each chassis that was discovered
cmmDisplayName	String	Chassis name that is provided by the CMM
cmms	Array of objects	Information about the CMMs in the chassis
cmmDisplayName	String	Name of the CMM
firmware	Array of objects	Information about the CMM firmware
build	String	Firmware build
date	String	Firmware date
name	String	Firmware name
type	String	Firmware type
name	String	Hostname of the CMM
serialNumber	String	Serial number of the CMM
slots	Array of integers	Bay in the chassis where the CMM is installed
type	String	Resource type. This value is always **CMM**.
uuid	String	UUID of the CMM
displayName	String	Chassis name that is defined by the user
fruNumber	String	FRU part number for the chassis
hostname	String	Hostname of the chassis
ipAddresses	Array of strings	All IPv4 and IPv6 addresses for the chassis
machineType	String	Chassis machine type
managementPorts	Array of objects	List of management ports in the chassis
enabled	Boolean	Indicates whether the port enabled. This can be one of the following values. • **true**. The port is enabled. • **false**. The port is disabled.
port	Integer	Port number

Attributes	Type	Description
protocol	String	Protocol that is running on the port (for example, http, https, or snmpv3)
model	String	Chassis model
name	String	Chassis name
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports managed authentication. • **false**. This device does not support managed authentication.
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device
publicAccess	String	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
storedCredentials	Object	Information about the stored credential that is associated with this device, if applicable
description	String	Description of the stored credential
id	String	ID of the stored credential
uri	String	Chassis URI
serialNumber	String	Serial number for the chassis
status	Array	Current status of the chassis
message	String	Message
name	String	Name
type	String	Resource type. This value is always **Chassis**.
uuid	String	UUID for the chassis
rackswitchList	Array of objects	List of all top-of-rack switches that were discovered
displayName	String	Name of the top-of-rack switch
firmware	Array	A list of firmware on the top-of-rack switch
build	String	Build level
date	String	Date
version	String	Build version
fruNumber	String	FRU number
hostname	String	Hostname of the top-of-rack switch

Attributes	Type	Description
ipAddresses	Array of Strings	All IPv4 and IPv6 addresses for the top-of-rack switch
machineType	String	Machine type of the top-of-rack switch
managementPorts	Array of objects	List of management ports in the top-of-rack switch
enabled	Boolean	Indicates if the port is enabled. This can be one of the following values. • **true**. The port is enabled. • **false**. The port is not enabled.
port	Integer	Port number
protocol	String	Protocol running on the port (for example, http, https, or snmpv3)
model	String	Model of the top-of-rack switch
name	String	Name of the top-of-rack switch
os	String	Operating system. This can be one of the following values. • **CNOS** • **ENOS**
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports the ability to choose managed authentication. • **false**. This device does not support the ability to choose managed authentication.
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device
publicAccess	String	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
storedCredentials	Object	Information about the stored credential that is associated with this device, if applicable
description	String	Description of the stored credential
id	String	ID of the stored credential
uri	String	Server URI
serialNumber	String	Serial number for the top-of-rack switch
status	Object	Current status
manageable	Boolean	Indicates whether the top-of-rack switch is manageable. This can be one of the following values. • **true**. The switch is manageable. • **false**. The switch is not manageable.

Attributes	Type	Description
message	String	Message
name	String	Name
type	String	Resource type. This value is always **Rackswitch**.
uuid	String	UUID of the top-of-rack switch
serverList	Array	List of all rack and tower servers that were discovered
displayName	String	Name of the rack or tower server
enclosureFormFactor		(IMM, IMM2, XCC, or XCC2 only) Form factor of the chassis. This can be one of the following values. • **dense-computing** • **edge-computing** • **rack-tower**
firmware	Array of objects	List of firmware on the rack or tower server
build	String	Build level
date	String	Date
version	String	Build version
fruNumber	String	FRU number
hostname	String	Hostname of the rack or tower server
ipAddresses	Array of Strings	All IPv4 and IPv6 addresses for the rack or tower server
machineType	String	Machine type of the rack or tower server
managementProcessor	String	The type of management controller. This can be one of the following values. • **integrated-management-module** • **integrated-management-module2** • **lenovo-xclarity-controller** • **chassis-management-module**
managementPorts	Array of objects	List of management ports in the rack or tower server
enabled	Boolean	Indicates if the port is enabled. One of the following values can be returned: • **true**. The port is enabled. • **false**. The port is not enabled.
port	Integer	Port number
protocol	String	Protocol running on the port (for example, http, https, or snmpv3)
model	String	Model of the rack or tower server
name	String	Name of the rack or tower server
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.

Attributes	Type	Description
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports the ability to choose managed authentication. • **false**. This device does not support the ability to choose managed authentication.
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device
publicAccess	String	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
storedCredentials	Object	Information about the stored credential that is associated with this device, if applicable
description	String	Description of the stored credential
id	String	ID of the stored credential
uri	String	Server URI
serialNumber	String	Serial number for the rack or tower server
status	Object	Current status
manageable	Boolean	Indicates whether the rack or tower server is manageable. One of the following values can be returned. • **true**. The port is enabled. • **false**. The port is not enabled.
message	String	Message
name	String	Name
subType	String	
type	String	Server type. This can be one of the following values. • **Edge Server**. ThinkSystem SE server • **Rack-Tower Server**. Converged, NeXtScale, System x or ThinkSystem SD, SR, or ST server • **Lenovo ThinkServer**. ThinkServer server
uuid	String	UUID of the rack and tower server
storageList	Array of objects	Information about each storage device that was discovered
displayName	String	Name of the storage device
hostname	String	Hostname of the storage device
ipAddresses	Array of strings	All IPv4 and IPv6 addresses for the storage device
firmware	Array of objects	List of firmware on the storage device
build	String	Build level
date	String	Date

Attributes	Type	Description
version	String	Build version
fruNumber	String	FRU number
machineType	String	Machine type of the storage device
managementPorts	Array of objects	List of management ports in the storage device
enabled	Boolean	Indicates if the port is enabled. One of the following values can be returned. • **true**. The port is enabled. • **false**. The port is not enabled.
port	Integer	Port number
protocol	String	Protocol running on the port (for example, http, https, or snmpv3)
model	String	Model of the storage device
name	String	Name of the storage device
serialNumber	String	Serial number for the storage device
status	Object	Current status
manageable	Boolean	Indicates whether the storage device is manageable. This can be one of the following values. • **true**. The storage device is manageable. • **false**. The storage device is not manageable.
name	String	Name
type	String	Resource type. This can be one of the following values. • **Lenovo Storage** • **IBM Tape**
uuid	String	UUID of the storage device
wwnn	String	WWNN of the storage device
xhmcList	Array	Information about each XClarity Administrator management server that was discovered
hostname	String	Hostname of the XClarity Administrator management server
ipAddresses	Array of strings	All IPv4 and IPv6 addresses for the management server
managementPorts	Array of objects	List of management ports in the top-of-rack switch
enabled	Boolean	Indicates if the port is enabled. This can be one of the following values. • **true**. The port is enabled. • **false**. The port is not enabled.
port	Integer	Port number
protocol	String	Protocol running on the port (for example, http, https, or snmpv3)
name	String	Name of the management server
software	Array of objects	Information about the XClarity Administrator version

Attributes	Type	Description
version	String	Version of XClarity Administrator that is installed
status	Object	Current status
manageable	Boolean	Indicates whether the management server is manageable. This can be one of the following values. • **true**. The management server is manageable. • **false**. The management server is not manageable.
manager-uuid	String	UUID of the management server
type	String	Resource type This value is always **Domain Manager**.
uuid	String	UUID of the management server

The following example is returned if the request is successful for a chassis.


```
{
   "progress": 100,
   "result": 100,
   "chassisList": [{
      "cmmDisplayName": "chassis-2",
      "cmms": [{
         "cmmDisplayName": "chassis-2",
         "firmware": [{
            "build": "1AON18B",
            "date": "2017-10-24",
            "name": "CMM Firmware",
            "type": "CMM Firmware"
         }],
         "name": "chassis-2",
         "serialNumber": "Y011BG78J093",
         "slots": [1],
         "type": "CMM",
         "uuid": "3d316351852111e78e4fbed8acb88dcf"
      }],
      "displayName": "chassis-2",
      "fruNumber": "81Y2893",
      "hostname": "chassis-2",
      "ipAddresses": ["10.240.60.50", "fe80::2e0:ecff:fe43:2c8b", "fe80::2e0:ecff:fe43:2c8c",
                      "fd55:faaf:e1ab:210f:2e0:ecff:fe43:2c8b"],
      "machineType": "7893",
      "managementPorts": [{
         "enabled": false,
         "port": 80,
         "protocol": "http"
      },
      ...,
      {
         "enabled": true,
         "port": 161,
         "protocol": "snmpv3"
      }],
      "model": "92X",
      "name": "chassis-2",
      "securityDescriptor": {
         "managedAuthEnabled": false,
         "managedAuthSupported": false,
         "publicAccess": false,
         "roleGroups": [],
         "uri": "chassis/5422200a92d34460b5c34c86f1d9ca9c"
```

```
      },
      "serialNumber": "100B2AA",
      "status": {
         "message": "Unmanaged",
         "name": "UNMANAGED"
      },
      "type": "Chassis",
      "uuid": "5422200a92d34460b5c34c86f1d9ca9c"
   }],
   "rackswitchList": [],
   "serverList": [],
   "storageList": [],
   "xhmcList": []
}]
```


The following example is returned if the request is successful for a ThinkServer server.


```
[{
   "progress": 100.0,
   "result": 100,
   "chassisList": [],
   "rackswitchList": [],
   "serverList": [{
      "displayName": "n6",
      "enclosureFormFactor": "rack-tower",
      "firmware": [{
         "build": "TCO024A",
         "date": "2016/08/29",
         "version": "3.50"
      },
      {
         "build": "TBE126Q",
         "date": "2016/11/18",
         "version": "2.21"
      }],
      "fruNumber": "01KN187     ",
      "hostname": "cximmnode6",
      "ipAddresses": ["10.240.62.156", "fdea:14a7:304b:40::3:6",
                      "fd55:faaf:e1ab:210f:a94:efff:fe38:f5a1", "fe80::a94:efff:fe38:f5a1"],
      "machineType": "8869",
      "managementProcessor": "integrated-management-module2",
      "managementPorts": [{
         "enabled": true,
         "port": 5988,
         "protocol": "cimxml-http"
      },
      ...,
      {
         "enabled": true,
         "port": 623,
         "protocol": "rmcp"
      }],
      "model": "ACA",
      "name": "n6",
      "securityDescriptor": {
         "managedAuthEnabled": true,
         "managedAuthSupported": true,
         "publicAccess": false,
         "roleGroups": [],
         "uri": "nodes/0d5d0374dd3511e6b1e20894ef38f59c"
      },
      "serialNumber": "J1192GG",
```

```
      "server-type": "Rack-Tower Server",
      "status": {
         "manageable": true,
         "message": "Unmanaged",
         "name": "UNMANAGED"
      },
      "subType": "",
      "type": "Rack-Tower Server",
      "uuid": "0d5d0374dd3511e6b1e20894ef38f59c"
   }],
   "storageList": [],
   "xhmcList": []
}]
```


The following example is returned if the request is successful for a rack switch.


```
[{
   "progress": 100.0,
   "result": 100,
   "chassisList": [],
   "rackswitchList": [{
      "displayName": "lci-medium-10g-sw01",
      "firmware": [{
         "date": null,
         "build": "Level 1.0",
         "version": "1.0"
      }],
      "fruNumber": null,
      "hostname": "lci-medium-10g-sw01",
      "ipAddresses": ["10.240.62.159", "fdea:14a7:304b:40:0:0:4:3"],
      "machineType": "7159",
      "managementPorts": [{
         "enabled": false,
         "port": 443,
         "protocol": "https"
      },
      {
         "enabled": true,
         "port": 80,
         "protocol": "http"
      }],
      "model": "HCD (G8272)",
      "name": "lci-medium-10g-sw01",
      "os": "ENOS",
      "securityDescriptor": {
         "managedAuthEnabled": false,
         "managedAuthSupported": false,
         "roleGroups": [],
         "publicAccess": false,
         "uri": "switches/5C2719BC02553v5E885460D41B2E217CF"
      },
      "serialNumber": "Y05JJ11192MY",
      "status": {
         "manageable": true,
         "name": "UNMANAGED"
      },
      "type": "Rackswitch",
      "uuid": "5C2719BC025535E885460D41B2E217CF",
   }],
   "serverList": [],
   "storageList": [],
   "xhmcList": []
```

```
}]
```

/manageRequest

Use this REST API to manage devices that have been discovered.

The devices must have been discovered using the POST /discoverRequest method.

HTTP methods

POST

POST /manageRequest

Use this method to manage devices. The response header includes a URI that is associated with a job that indicates that a task was started.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/manageRequest`

Query parameters

Parameters	Required / Optional	Description
discovery={Boolean}	Optional	Indicates whether to discover endpoints as part of this management request. This can be one of the following values. • **true**. Discovers endpoints as part of this request. • **false**. (default) Does not discover endpoints as part of this request. The devices must have been previously discovered using the POST /discoverRequest method.

The following example discovers and manages endpoints.

```
POST https://192.0.2.0/manageRequest?discovery=true
```

The following example manages endpoints have endpoints that have been discovered.

```
POST https://192.0.2.0/manageRequest
```

Request body

Table 3. Discover and manage a device

Attributes	Required / Optional	Type	Description
enableHttps	Optional	Boolean	(Rack switches running ENOS only) Indicates whether to enable HTTPS on the switch. This can be one of the following values. • **true**. (default) Enable HTTPS. • **false**. Do not enable HTTPS.
enablePassword	Optional	String	(Rack switches running ENOS only) “Enable” password that is used to enter Privileged Exec Mode on the switch

Table 3. Discover and manage a device (continued)

Attributes	Required / Optional	Type	Description
forceManage	Optional	Boolean	Indicates whether to force management of the device. This can be one of the following values. • **true**. Force management. • **false**. Do not force management. **Notes:** Use this force-management option only if you previously attempted to manage the device and management was not successful due to one of the following error conditions. • If the managing XClarity Administrator failed and cannot be recovered. **Note:** If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option. • If the managing XClarity Administrator was taken down before the devices were unmanaged. • If the devices were not unmanaged successfully. **Attention:** Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.
ipAddresses	Required	Array of strings	List of device IP addresses or fully-qualified domain names
newPassword	Optional	String	(Chassis and servers only) New password to be used for managed authentication
password	Required	String	Current password to access the device
recoveryPassword	Optional	String	Recovery password to be used for the device
replaceNtpConfiguration	Optional	Boolean	(Rack switches only) Indicates whether to replace the NTP configuration and time zone on the switch with settings that are defined for XClarity Administrator. This can be one of the following values. • **true**. (default) Replace the NTP and time zone settings. • **false**. Do not replace the NTP and time zone settings.
securityDescriptor	Required	Object	Information about the authentication enablement and support the associated stored credentials for a managed device

Table 3. Discover and manage a device (continued)

Attributes	Required / Optional	Type	Description
identityManagementSystem	Required if **identity-Management-System-Enabled** is “true”	String	(Servers only) Information about the identity (in the identity-management system) that is associated with this device, if applicable
address	Required	String	IP address or hostname where the user account is stored as defined in CyberArk. This is typically the IP address of the Lenovo XClarity Controller or external LDAP server (if applicable).
appId	Optional	String	Application ID from CyberArk If you specify the **appID**, you must also specify **safe** and **folder**.
folder	Optional	String	Folder from CyberArk If you specify the **appID**, you must also specify **safe** and **folder**. If the onboarded account is not in a folder, specify an empty string.
name	Optional	String	Type of the identity-management system. This value is always **CyberArk**
safe	Optional	String	Safe from CyberArk If you specify the **appID**, you must also specify **safe** and **folder**.
username	Required	String	Name of the user account for the device
identityManagementSyste-mEnabled	Optional	String	Indicates whether to use an identity-management system for authentication. This can be one of the following values. • **true**. An identity-management system is to authenticate this device. • **false**. An identity-management system is not used to authenticate this device. In this case, either manually entered credentials or stored credentials must be used. **Note:** Identity management systems can be used to authenticate only ThinkSystem and ThinkAgile servers.
managedAuthSupported	Required for Think-Server devices	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports the ability to choose managed authentication. • **false**. This device does not support the ability to choose managed authentication.
managedAuthEnabled	Required for devices other than Think-Server	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.

Table 3. Discover and manage a device (continued)

Attributes	Required / Optional	Type	Description
publicAccess	Optional	Boolean	
roleGroups	Optional	Array of strings	List of role groups that are permitted to view and manage the device. To get a list of available role groups, use GET /roleGroups. You can specify only role groups to which the current user belongs. If you do not specify the **roleGroups** attribute, the default roles groups are assigned. You can obtain the list of default role group using GET /resourceAccessControl. If you specify the **roleGroups** attributes= with an empty or null value, role groups are not assigned. **Note:** If you add devices to a managed chassis, the new devices will belong to the same role groups as the chassis.
storedCredentials	Required if **managedAuthEnabled** is set to `true`	Object	Information about the stored credential that is associated with this device, if applicable **Note:** RackSwitch devices support only stored credentials for authenticating to the switches. Manual user credentials are not supported.
description	Optional	String	Description of the stored credential
id	Required	String	ID of the stored credential
userName	Optional	String	Name of the stored credential
type	Required	String	Type of device to be managed. This can be one of the following values. • **Chassis** • **Edge Server**. ThinkSystem SE server • **IBM Tape**. IBM tape library • **Lenovo ThinkServer** • **Lenovo Storage** • **Rackswitch** • **Rack-Tower Server**. ThinkSystem SD, ThinkSystem SR, or ThinkSystem ST, System x, Converged, or NeXtScale server
username	Required	String	User ID to be used to access the device **Note:** RackSwitch devices support only stored credentials (using the **storedCredentials** attribute) for authenticating to the switches. Manual user credentials using the **username** and **password** attributes are not supported and must be empty or null..

The following example discovers and manages a server when managed authentication is enabled and uses CyberArk for authentication. (when **discovery=true**).

```
[{
   "ipAddresses": ["192.0.2.0"],
```

```
   "forceManage": true,
   "password": null,
   "securityDescriptor": {
      "identityManagementSystem": {
         "address" : "192.0.2.0",
         "appId": "LXCA",
         "name" : "CyberArk",
         "safe": "Test",
         "username": "USERID"
      },
      "identityManagementSystemEnabled": true,
      "managedAuthEnabled": true,
      "managedAuthSupported": true,
      "publicAccess": false,
      "storedCredentials":null
   },
   "type": "Rack-Tower Server",
   "username": null
}]
```

The following example discovers and manages a chassis when managed authentication is enabled. (when **discovery=true**).

```
[{
   "ipAddresses": ["10.243.3.192", "fd55:faaf:e1ab:2021:5ef3:fcff:fe25:e4e7"],
   "password": "Passw0rd",
   "recoveryPassword": "CME44ibm",
   "securityDescriptor": {
      "managedAuthEnabled": true
   },
   "type": "Chassis",
   "username": "USERID"
}]
```

The following example discovers and manages a server when managed authentication is enabled using an identity management system (when **discovery=true**).

```
[{
   "ipAddresses": ["10.243.3.192","fd55:faaf:e1ab:2021:5ef3:fcff:fe25:e4e7"],
   "password": "",
   "securityDescriptor": {
       "IMSCredentialsId": "1234",
       "managedAuthEnabled": true
   },
   "type": "Server",
   "username": ""
}]
```

The following example discovers and manages a chassis when managed authentication is disabled using a stored credential (when **discovery=true**).

```
[{
   "ipAddresses": ["10.243.3.192","fd55:faaf:e1ab:2021:5ef3:fcff:fe25:e4e7"],
   "password": "",
   "securityDescriptor": {
      "managedAuthEnabled": false
      "storedCredentials": {
         "id": "2853"
      }
   },
   "type": "Chassis",
   "username": ""
}]
```

Table 4. Manage a discovered device

Attributes	Re-quired / Optional	Type	Description
displayName	Optional	String	(Rack switches only) Name of the device
enableHttps	Optional	Boolean	(Rack switches running ENOS only) Indicates whether to enable HTTPS on the switch. This can be one of the following values. • **true**. (default) Enable HTTPS. • **false**. Do not enable HTTPS.
enclosureFormFactor	Optional	String	(IMM, IMM2, XCC, or XCC2 only) Form factor of the device. This can be one of the following values. • rack-tower • dense-computing
enablePassword	Optional	String	(Rack switches running ENOS only) “Enable” password that is used to enter Privileged Exec Mode on the switch
firmware	Optional	Array of strings	Information about installed firmware
build	Required	String	Build number
date	Required	String	Release date
version	Required	String	Version number
forceManage	Optional	Boolean	Indicates whether to force management of the device. This can be one of the following values. • **true**. Force management. • **false**. Do not force management. **Notes:** Use this force-management option only if you previously attempted to manage the device and management was not successful due to one of the following error conditions. • If the managing XClarity Administrator failed and cannot be recovered. **Note:** If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option. • If the managing XClarity Administrator was taken down before the devices were unmanaged. • If the devices were not unmanaged successfully. **Attention:** Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.
fruNumber	Optional	String	(Rack switches only) FRU number
hostname	Optional	String	(Rack switches only) hostname of the device

Table 4. Manage a discovered device (continued)

Attributes	Required / Optional	Type	Description
ipAddresses	Required	Array of strings	List of device IP addresses or fully-qualified domain names
ipv4Addresses	Optional	Array of strings	(Rack switches only) List of IPv4 IP addresses
ipv6Addresses	Optional	Array of strings	(Rack switches only) List of IPv6 IP addresses
machineType	Required for ThinkSystem servers; otherwise, optional	String	Machine type
managementPorts	Optional for switches; otherwise, required	Array	List of device management ports
enabled	Required	Boolean	Indicates whether the port enabled. This can be one of the following values. • **true**. The port is enabled • **false**. The port is disabled
port	Required	Integer	Port number
protocol	Required	String	Protocol that is running on the port. See the GET /discoverRequest/jobs/*{job_id}* response body for the supported protocols for the device's management ports.
managementProcessor	Required for ThinkSystem devices; otherwise, optional	String	(Chassis and servers only) Type of management controller. This can be one of the following values. • **integrated-management-module** • **integrated-management-module2** • **lenovo-xclarity-controller** • **chassis-management-module**
model	Optional	String	(Rack switches only) Model of the device
name	Optional	String	(Rack switches only) Name of the device
newPassword	Optional	String	(Chassis and servers only) New password to be used for managed authentication
os	Required for CNOS and ENOS switches	String	(Rack switches only) Firmware type. This can be one of the following values. • **CNOS** • **ENOS**

Table 4. Manage a discovered device (continued)

Attributes	Required / Optional	Type	Description
password	Required	String	Current password to access the device
recoveryPassword	Optional	String	Recovery password to be used for the device
replaceNtpConfiguration	Optional	Boolean	(Rack switches only) Indicates whether to replace the NTP configuration and time zone on the switch with settings that are defined for XClarity Administrator. This can be one of the following values. • **true**. (default) Replace the NTP and time zone settings • **false**. Do not replace the NTP and time zone settings.
securityDescriptor	Required	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
identityManagementSystem	Required if **identity-Manage-ment-System-Enabled** is “true”	String	(Servers only) Information about the identity (in the identity-management system) that is associated with this device, if applicable
address	Required	String	IP address where the user account is stored as defined in CyberArk. This is typically the IP address of the Lenovo XClarity Controller or external LDAP server (if applicable).
appId	Optional	String	Application ID from CyberArk If you specify the **appID**, you must also specify **safe** and **folder**. If you do not specify **appID**, Lenovo XClarity Administrator uses the paths that are already defined to identify the onboarded accounts in CyberArk (see GET /identityManagementSystems/cyberark/paths)
folder	Optional	String	Folder from CyberArk If you specify the **appID**, you must also specify **safe** and **folder**. If the onboarded account is not in a folder, specify an empty string.
name	Optional	String	Type of the identity-management system. This value is always **CyberArk**.
safe	Optional	String	Safe from CyberArk If you specify the **appID**, you must also specify **safe** and **folder**.
username	Required	String	Name of the user account for the device
uri	Optional	String	Device URI

Table 4. Manage a discovered device (continued)

Attributes	Required / Optional	Type	Description
identityManagementSystemEnabled	Optional	String	Indicates whether to use an identity-management system for authentication. This can be one of the following values. • **true**. An identity-management system is to authenticate this device. • **false**. An identity-management system is not used to authenticate this device. In this case, either manually entered credentials or stored credentials must be used. **Note:** Identity management systems can be used to authenticate only ThinkSystem and ThinkAgile servers.
managedAuthSupported	Required for ThinkServer devices	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports the ability to choose managed authentication. • **false**. This device does not support the ability to choose managed authentication.
managedAuthEnabled	Required for devices other than ThinkServer	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.
publicAccess	Optional	Boolean	Indicates whether the device can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
roleGroups	Optional	Array of strings	List of role groups that are permitted to view and manage the device. To get a list of available role groups, use GET /roleGroups. You can specify only role groups to which the current user belongs. If you do not specify the **roleGroups** attribute, the default roles groups are assigned. You can obtain the list of default role group using GET /resourceAccessControl. If you specify the **roleGroups** attribute with an empty or null value, role groups are not assigned. **Note:** If you add devices to a managed chassis, the new devices will belong to the same role groups as the chassis.

Table 4. Manage a discovered device (continued)

Attributes	Required / Optional	Type	Description
storedCredentials	Required if **managedAuthEnabled** is set to `true`	Object	Information about the stored credential that is associated with this device, if applicable **Note:** RackSwitch devices support only stored credentials for authenticating to the switches. Manual user credentials are not supported.
description	Optional	String	Description of the stored credential
id	Required	String	ID of the stored credential
userName	Optional	String	Name of the stored credential
serialNumber	Optional	String	(Rack switches only) Serial number for the device
status	Optional	Object	(Rack switches only) Current status
manageable	Optional	String	Indicates whether the top-of-rack switch is manageable. This can be one of the following values. • **true**. The port is manageable. • **false**. The port is not manageable.
message	Optional	String	Message
name	Optional	Boolean	Name
replaceNtpConfiguration	Optional	Boolean	(Rack switches only) Indicates whether to replace the NTP configuration and time zone on the switch with settings that are defined for XClarity Administrator. This can be one of the following values. • **true**. (default) Replace the NTP and time zone settings. • **false**. Do not replace the NTP and time zone settings.
subType	Required for ThinkSystem DB series and NVIDIA Mellanox switches	String	Device subtype. This can be one of the following values. • **Lenovo ThinkSystem DB Series Switches** • **NVIDIA Mellanox Switches**
server-type	Optional	String	(Servers only) Type of server to be managed. This can be one of the following values. • **Edge Server**. ThinkSystem SE server • **ITE**. Flex System server • **Lenovo ThinkServer**. ThinkServer server • **NeXtScale**. NeXtScale server • **Rack-Tower Server**. ThinkSystem SD, ThinkSystem SR, or ThinkSystem ST, System x, Converged, or NeXtScale server • **SCU**. storage device.

Table 4. Manage a discovered device (continued)

Attributes	Required / Optional	Type	Description
type	Required	String	Type of device to be managed. This can be one of the following values. • **Chassis** • **Edge Server**. ThinkSystem SE server • **IBM Tape**. IBM tape library • **Lenovo ThinkServer** • **Lenovo Storage** • **Rackswitch** • **Rack-Tower Server**. ThinkSystem SD, ThinkSystem SR, or ThinkSystem ST, System x, Converged, or NeXtScale server
username	Required	String	User ID to be used to access the device **Note:** RackSwitch devices support only stored credentials (using the **storedCredentials** attribute) for authenticating to the switches. Manual user credentials using the **username** and **password** attributes are not supported and must be empty or null.
uuid	Optional	String	UUID for the device

The following example manages a discovered chassis (when **discovery=false**).

```
[{
    "ipAddresses": ["10.243.3.55"],
    "managementPorts": [{
        "enabled": false,
        "port": 80,
        "protocol": "http"
    }, ..., {
        "enabled": true,
        "port": 161,
        "protocol": "snmpv3"
    }],
    "password": "xxxxxxxx",
    "recoveryPassword": "xxxxxxxx",
    "securityDescriptor" : {
       "managedAuthEnabled":false,
       "storedCredentials": {
          "description":"A valid user"
          "id":" ED895B48D50D4E34B5DAF1F697CA78B3"
          "userName":"user1",
       }
    }
    "type": "Chassis",
    "username": "USERID",
    "uuid": "48331a223bf34fba90732b379b837b9c"
}]
```

The following example discovers and manages a ThinkSystem server using an identity management system (when **discovery=true**).

```
[{
   "displayName": "Cosmo-157",
   "enclosureFormFactor": "rack-tower",
   "firmware": [{
      "build": "CDI352T",
```

```
      "date": "2020-04-25",
      "version": "4.20"
   }, {
      "build": "TEE155I",
      "date": "2020-03-27",
      "version": "2.60"
   }],
   "forceManage": true,
   "fruNumber": "00MX680",
   "hostname": "XCC-7Y02-0123456789",
   "ipAddresses": [
      "192.0.2.0",
      "fd55:faaf:e1ab:2021:a94:efff:fe4f:5769",
      "fe80::a94:efff:fe4f:5769"
   ],
   "machineType": "7Y02",
   "managementPorts": [{
      "enabled": true,
      "port": 5989,
      "protocol": "cimxml-https"
   }, ..., {
      "enabled": true,
      "port": 623,
      "protocol": "rmcp"
   }],
   "managementProcessor": "lenovo-xclarity-controller",
   "model": "RCZ000",
   "name": "Cosmo-157",
   "password": null,
   "recoveryPassword": "",
   "securityDescriptor": {
      "identityManagementSystem": {
         "address" : "192.0.2.0",
         "appId": "LXCA",
         "name" : "CyberArk",
         "safe": "Test",
         "username": "USERID"
      },
      "identityManagementSystemEnabled": true,
      "managedAuthEnabled": true,
      "managedAuthSupported": true,
      "publicAccess": false,
      "storedCredentials":null
   },
   "serialNumber": "123456789",
   "status": {
      "manageable": true
      "message": "Unmanaged",
      "name": "UNMANAGED",,
   },
   "subType": "",
   "server-type": "Rack-Tower Server",
   "type": "Rack-Tower Server",
   "username": null,
   "uuid": "a6df710c8b7d11e78c2786fa5e924c8c"
}]
```


The following example manages a discovered ThinkSystem server (when **discovery=false**).


```
[{
   "enclosureFormFactor": "rack-tower",
   "displayName": "Electron-SIT-2",
```

```
   "firmware": [{
      "date": "2018-05-10",
      "build": "TEI325I",
      "version": "1.80"
   }, {
      "date": "2018-04-24",
      "build": "TEE123G",
      "version": "1.40"
   }],
   "forceManage": true,
   "fruNumber": "01GT946",
   "hostname": "Electron-SIT-2",
   "ipAddresses": ["10.240.211.155","2002:97b:c2bb:830:10:240:211:155",
                   "fe80::a94:efff:fe41:be01"],
   "machineType": "7X19",
   "managementPorts": [{
      "protocol": "cimxml-https",
      "port": 5989,
      "enabled": true
   }, ..., {
      "protocol": "rmcp",
      "port": 623,
      "enabled": true
   }],
   "managementProcessor": "lenovo-xclarity-controller",
   "model": "25Z000",
   "name": "Electron-SIT-2",
   "newPassword": null,
   "password": null,
   "recoveryPassword": "",
   "securityDescriptor": {
      "managedAuthEnabled": false,
      "roleGroups": [LXC-ADMIN,LXC-HW-MANAGER],
      "storedCredentials": {
         "description": "test_211.155",
         "id": "2852",
         "userName": "test"
      },
      "uri": "nodes/fbb43c13103511e785f2e4a2ced78753"
   },
   "serialNumber": "ELEC0G604G",
   "server-type": "Rack-Tower Server",
   "status": {
      "name": "UNMANAGED",
      "message": "Unmanaged",
      "manageable": true
   },
   "subType": "",
   "type": "Rack-Tower Server",
   "username": null,
   "uuid": "fbb43c13103511e785f2e4a2ced78753",
}]
```


The following example manages a discovered ThinkServer device (when **discovery=false**).


```
[{
   "displayName": "SN#10.240.197.14",
   "firmware": [{
      "build": "Level 1",
      "date": null,
      "version": "1.1"
   }],
```

```
   "forceManage": true,
   "fruNumber": null,
   "hostname": "10.240.197.14",
   "ipAddresses": ["10.240.197.14"],
   "machineType": "7OFO",
   "managementPorts": [{
      "enabled": true,
      "port": 443,
      "protocol": "https"
   }, {
      "enabled": true,
      "port": 80,
      "protocol": "http"
   }],
   "model": "",
   "name": "SN#10.240.197.14",
   "password": "",
   "securityDescriptor": {
      "managedAuthSupported": false,
      "managedAuthEnabled": false,
      "storedCredentials": {
         "id": "353"
      }
   },
   "serialNumber": " ",
   "status": {
      "name": "UNMANAGED",
      "manageable": true
   },
   "type": "Lenovo ThinkServer",
   "username": "",
   "uuid": "fbb43c13103511e785f2e4a2ced78753"
}]
```

The following example discovers and manages a rack switch running ENOS (when **discovery=true**).

```
[{
   "enableHttps": true,
   "enablePassword": "",
   "ipAddresses": ["10.243.3.192","fd55:faaf:e1ab:2021:5ef3:fcff:fe25:e4e7"],
   "password": "",
   "replaceNtpConfiguration": true
   "securityDescriptor": {
      "managedAuthEnabled": false
      "storedCredentials": {
         "id": "352"
      }
   },
   "type": " Rackswitch ",
   "username": ""
}]
```

The following example manages a discovered rack switch (when **discovery=false**).

```
[{
   "displayName": "Gryphon",
   "enableHttps": true,
   "enablePassword": "",
   "forceManage": true,
   "fruNumber": "XXXXXXX      ",
   "hostname": "IBM2-40f2e9b8163d",
   "ipAddresses": [
      "10.243.6.68",
```

```
      "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:163d",
      "fe80::42f2:e9ff:feb8:163d"
   ],
   "ipv4Addresses": ["10.243.6.68"],
   "ipv6Addresses": [
      "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:163d",
      "fe80::42f2:e9ff:feb8:163d"
   ],
   "machineType": "1234",
   "model": "IBM",
   "name": "Gryphon",
   "os": "ENOS",
   "password": "DEF",
   "securityDescriptor": {
      "managedAuthEnabled": false,
      "roleGroups": [LXC-ADMIN,LXC-HW-MANAGER],
      "storedCredentials": {
         "id": "352"
      },
      "uri": "switches/2376f7c628fb11e1b72b5cf3fc3c1448"
   },
   "recoveryPassword": null,
   "serialNumber": "IBM0152",
   "status": {
      "message": "Unmanaged",
      "name": "UNMANAGED",
      "manageable": true
   },
   "replaceNtpConfiguration": true,
   "type": "Rackswitch",
   "username": "",
   "uuid": "fc3058cadf8b11d48c9b9b1b1b1b1b58"
}]
```


Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

If this POST method results in a job getting started, the response header includes a URI in the form /manageRequest/jobs/*{job_id}* (for example, `/manageRequest/jobs/12`) that represents the job that is monitored by the management server. You can use GET /manageRequest/jobs/*{job_id}* to determine the

status of the job. If a job was not successfully started, refer to the response code and response body for details.

Note: A successful response indicates that the request was successfully transmitted and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Response body

Attributes	Type	Description
jobID		ID of the task (job) that was created to manage the device
statusCode		Return code
statusDescription		Description of the return code
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "jobID":"42",
   "statusCode":201
   "statusDescription":"Bulk job 138 was created successfully.",
   "result":"success",
   "messages":[],
}
```

/manageRequest/jobs/*{job_id}*

Use this REST API to monitor the status of a management request.

HTTP methods

GET

GET /manageRequest/jobs/*{job_id}*

Use this method to monitor the status of a management request.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/manageRequest/jobs/{job_id}`

where *{job_id}* is the job ID that was returned by the POST /manageRequest method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
progress	Double	Percentage complete of the bulk management job. This can be one of the following values. • **0.0**. Created. • **> 0.0**. In progress. • **100.0**. Complete.
result	Integer	Result of the job. This can be one of the following values. • **0**. Created. • **50**. In progress. • **100**. Complete.
results	Array of objects	Result of the bulk management jobs
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID (“0509_LONG”)
messageAttributes	String	Message arguments. This can be one of the following values. • device IP if not null • device serial number if not null • device UUID
progress	Long	Percentage complete of the management job. If the job is complete, “JOB_DONE” is returned.

Attributes	Type	Description
result	String	Result of the request. This can be one of the following values. • **success**. The request was successful. • **failed**. The request failed.
resultLongDescription	String	Long description result
resultShortDescription	String	Short description result
status	Object	Status details about the list of management steps
description	Array of objects	List of message descriptions
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID for the set of management steps
percentage	Long	Percentage complete of the set of management steps
state	String	State of the set of management steps. The can be one of the following values. • **ERROR** • **RUNNING** • **RUNNING_COMPLETE**
substatus	Array of objects	Results of each of the task in the management job
completed	Boolean	Indicates whether the task completed. This can be one of the following values. • **true**. The step has completed. • **false**. The task has not completed.
id	String	Name of the management step
longDescription	String	Long message description
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID of the management step
progress	Long	Progress of the management step
shortDescription	String	Short message description
started	Boolean	Indicates if the management step has started. This can be one of the following values. • **true**. The step has started. • **false**. The step has not started.
status	Object	Status details about the individual management step
description	Array of objects	List of message descriptions
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID for the set of unmanagement steps

Attributes	Type	Description
percentage	Long	Percentage complete of the management step
state	String	State of the management step. This can be one of the following values. • **ERROR** • **PENDING** • **RUNNING** • **RUNNING_COMPLETE**
userAction	String	User action that is required
summary	Object	Information about the job summary This summary consists of the following types of information: • **Description**. Describes issues that occurred. • **Actions**. Describes whether the job completed successfully, and if not, lists the steps that the user can perform to resolve the issue. You must provide enough information so that the user can resolve the issue without help from the Lenovo Support. • **Severity**. Describes severity of the job. The job summary is optional for a job that completes successfully; however, it is good practice to set the summary, even when the severity is informational.
actionArgs	Array of strings	List of action arguments for the message
actionBundleKey	String	Bundle in which the user action is declared
actionBundleName	String	Bundle in which the translated user action is located
actionText	String	User action to use if there is no translation
descriptionArgs	Array of strings	List of arguments for the message
descriptionBundleKey		Bundle in which the message description is declared
descriptionBundleName	String	Bundle in which the translated message description is located
descriptionText	String	Message description to use if there is no translation
severity	String	Severity of the subtask. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).
taskid	Integer	Task ID
time_spent	Long	Duration of the task in milliseconds
uuid	String	UUID associated with the management
status		Status of the management job. This can be one of the following values. • **0**. Created. • **50**. Incomplete. • **100**. Done. • **101**. Done_Warnimg.

The following example is returned if the request is successful.


```
{
   "progress": 100,
   "result": 100,
   "results": [{
      "messageBundle": "com.lenovo.lxca.discovery.bundle.rest.messages",
      "messageID": "0509_LONG",
      "messageParameters": "10.243.9.106",
      "progress": 100,
      "result": "SUCCESS",
      "resultLongDescription": "The management job has completed successfully",
      "resultShortDescription": "Success",
      "status": {
         "description": [{
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1028_LONG"
         }],
         "percentage": 100,
         "state": "Complete"
         "substatus": [{
            "completed": true,
            "id": "STARTING",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1000_SHORT",
            "longDescription": "Starting endpoint management job",
            "progress": 100,
            "shortDescription": "Starting",
            "started": true,
            "status": {
               "description": [{
                  "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
                  "messageID": "1028_LONG"
               }],
               "percentage": 100,
               "state": "Complete"
            },
            "userAction": ""
         },
         ...,
         {
            "completed": true,
            "id": "CONFIGURATION",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1010_SHORT",
            "longDescription": "Configuring endpoint for management",
            "progress": 100,
            "shortDescription": "Configuration",
            "started": true,
            "status": {
               "substatus": [{
                  "completed": true,
                  "id": "CFG_NTP",
                  "longDescription": "Configuring NTP",
                  "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
                  "messageID": "1011_SHORT",
                  "progress": 100,
                  "shortDescription": "NTP",
                  "started": true,
                  "status": {
                     "description": [{
                        "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
```

```
                  "messageID": "1028_LONG"
               }],
               "percentage": 100,
               "state": "Complete"
            },
            "userAction": "[{\"format\":[\"paragraph\"],\"text\":\"The problem might be caused by
                           the device momentary loosing connection to the management server during
                        the management process. Either attempt to manage the device again, or
                        manually set the management NTP server and time zone information using
                        the management-controller interface.\"},
                        {\"format\":[\"paragraph\"],\"text\":\"The management-controller firmware
                        for the device might not support the management NTP server settings or
                        the time zone that is currently set in the management server. Update the
                        management-controller firmware to the latest version, and then either
                        attempt to manage the device again, or manually set the management NTP
                        server and time zone information using the management-controller
                        interface.\"}]",
         }
         {
            "completed": true,
            "id": "CFG_SECURITY",
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1012_SHORT",
            "longDescription": "Configuring security",
            "progress": 100,
            "shortDescription": "Security",
            "started": true,
            "status": {
               "description": [{
                  "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
                  "messageID": "1028_LONG"
               }],
               "percentage": 100,
               "state": "Complete"
            },
            "userAction": ""
         }],
         "description": [{
            "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "messageID": "1028_LONG"
         }],
         "percentage": 100,
         "state": "Complete"
      },
      "userAction": ""
   }],
   "summary": {
      "actionArgs": [],
      "actionBundleKey": "",
      "actionBundleName": ""
      "actionText": "",
      "descriptionArgs": [],
      "descriptionBundleKey": "1028_LONG",
      "descriptionBundleName": "com.lenovo.lxca.discovery.bundle.tasks.messages",
      "descriptionText": "The management job has completed successfully",
      "severity": "Informational",
   }
},
"taskid": 99,
"time_spent": 43456,
"uuid": "89b98fbf943f11e6bb84ff1e2236596d"
```

```
    }],
    "status": "DONE"
}
```

/unmanageOffline

Use this REST API to retrieve information about and configure settings for automatically unmanaging devices that are offline for specific amount of time.

HTTP methods

GET, PUT

GET /unmanageOffline

Use this method to return settings for automatically unmanaging devices that are offline for specific amount of time.

Note: Automatic unmanagement of offline devices is supported for Flex System chassis, switches, Lenovo Flex System servers, Lenovo System x servers, ThinkAgile, and ThinkSystem servers.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/unmanageOffline`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
offlinePeriod	Integer	Amount of time, in hours, that devices must be offline before they are automatically unmanaged This value can be from 1 – 24 hours. The default is 24 hours.
unmanageOffline	Boolean	Indicates whether Lenovo XClarity Administrator automatically unmanages devices that are offline for the a specific amount of time. This can be one of the following values. • **true**. Enables automatic unmanagement of offline devices.XClarity Administrator checks for offline devices every hour. If a device is offline for at least the amount of time specified by **offlinePeriod**, XClarity Administrator automatically unmanages that device. • **false**. Disables automatic unmanagement of offline devices.

The following example is returned if the request is successful.

```
{
   "offlinePeriod": 24,
   "unmanageOffline": "false"
}
```

PUT /unmanageOffline

Use this method to configure settings for automatically unmanaging devices that are offline for specific amount of time.

Note: Automatic unmanagement of offline devices is supported for Flex System chassis, switches, Lenovo Flex System servers, Lenovo System x servers, ThinkAgile, and ThinkSystem servers.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/unmanageOffline`

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
offlinePeriod	Optional	Integer	Amount of time, in hours, that devices must be offline before they are automatically unmanaged This value can be from 1 – 24 hours. The default is 24 hours.
unmanageOffline	Required	Boolean	Indicates whether Lenovo XClarity Administrator automatically unmanages devices that are offline for the a specific amount of time. This can be one of the following values. • **true**. Enables automatic unmanagement of offline devices.XClarity Administrator checks for offline devices every hour. If a device is offline for at least the amount of time specified by **offlinePeriod**, XClarity Administrator automatically unmanages that device. • **false**. Disables automatic unmanagement of offline devices.

The following example configure automatic unmanagement settings.

```
{
   "offlinePeriod": 48,
   "unmanageOffline": "true"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/unmanageRequest

Use this REST API to unmanage devices.

HTTP methods

POST

POST /unmanageRequest

Use this method to unmanage one or more target devices. The response header indicates the URI of a job that is associated with a new task that has been started.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/unmanageRequest`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
endpoints	Required	Array	Information about one or more devices to be unmanaged
ipAddresses	Required	Array of strings	IP addresses for the device

Attributes	Required / Optional	Type	Description
type	Required	String	Type of device. This can be one of the following values: • **Chassis** • **Edge Server**. ThinkSystem SE server • **IBM Tape**. IBM tape library • **Lenovo ThinkServer** • **Lenovo Storage** • **Rackswitch** • **Rack-Tower Server**. ThinkSystem SD, ThinkSystem SR, or ThinkSystem ST, System x, Converged, or NeXtScale server
uuid	Required	String	UUID for the device
forceUnmanage	Optional	Boolean	Indicates whether to force the unmanagement of a device. This can be one of the following values. • **true**. Force unmanagment even if the device is not reachable. • **false**. (default) Do not force unmanagement. **Important:** When unmanaging demo hardware, set this attribute to `true`.

Request example

The following is an example of a request that is submitted to unmanage a chassis.

```
{
    "endpoints":[{
        "ipAddresses" : ["10.243.4.144"],
        "type":"Chassis",
        "uuid":"63E29269BB634AB9A610D6F8FCE2B28F"
    }],
    "forceUnmanage":true
}
```

The following is an example of a request that is submitted to unmanage a rack switch.

```
{
   "endpoints":[{
      "ipAddresses":["10.241.139.100"],
      "type":"Rackswitch",
      "uuid":"F6F5A2630C244FDD9DE5376812C55480"
   }],
   "forceUnmanage":false
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

If this POST method results in a job getting started, the response header includes a URI in the form /unmanageRequest/jobs/*{job_id}* (for example, `/unmanageRequest/jobs/12`) that represents the job that is monitored by the management server. You can use GET /unmanageRequest/jobs/*{job_id}* to determine the status of the job. If a job was not successfully started, refer to the response code and response body for details.

Note: A successful response indicates that the request was successfully transmitted and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Response body

None

/unmanageRequest/jobs/*{job_id}*

Use this REST API to monitor the status of an unmanagement request.

HTTP methods

GET

GET /unmanageRequest/jobs/*{job_id}*

Use this method to monitor the status of an unmanagement request that was made using the POST /unmanageRequest method.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/unmanageRequest/jobs/{job_id}`

where *{job_id}* is the job ID that was returned by the POST /unmanageRequest method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
progress	Double	Percentage complete of the bulk management job. This can be one of the following values. • **0.0**. Created. • **> 0.0**. In progress. • **100.0**. Complete.
result	Integer	Result of the job. This can be one of the following values. • **0**. Created. • **50**. In progress. • **100**. Complete.
results	Array of objects	Results of the bulk unmanagement jobs
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID (“0509_LONG”)
messageAttributes	String	This can be one of the following values. • deviceIP if not null • deviceserial number if not null • deviceUUID
progress	Long	Percentage complete of the unmanagement job. If the job is complete, “JOB_DONE” is returned.
result	String	Result of the request. This can be one of the following values. • **success**. The request was successful. • **failed**. The request failed.
resultLongDescription	String	Long description result
resultShortDescription	String	Short description resul.
status	Object	Status details about the list of management steps
description	Array of objects	List of message descriptions
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID for the set of unmanagement steps
percentage	Long	Percentage complete of the set of unmanagement steps

Attributes	Type	Description
state	String	State of the set of unmanagement steps. The can be one of the following values. • **RUNNING** • **RUNNING_COMPLETE** • **ERROR**
substatus	Array of objects	Results of each of the task in the unmanagement job
completed	Boolean	Indicates whether the unmanagement step completed. This can be one of the following values. • **true**. The step has completed. • **false**. The step has not completed.
id	String	Name of the unmanagement step
longDescription	String	Long message description
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID of the unmanagement step
progress	Long	Progress of the unmanagement step
shortDescription	String	Short message description
started	Boolean	Indicates whether the unmanagement step has started. This can be one of the following values. • **true**. The step has started. • **false**. The step has not started.
status	Object	Status details about the individual management step
description	Array of objects	List of message descriptions
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.discovery.bundle.tasks.messages.”
messageID	String	Message ID for the set of unmanagement steps
percentage	Long	Percentage complete of the unmanagement step
state	String	State of the unmanagement step. This can be one of the following values. • **ERROR** • **PENDING** • **RUNNING** • **RUNNING_COMPLETE**
userAction	String	Any user action that is required.

Attributes	Type	Description
summary	Object	Information about the job summary This summary consists of the following types of information. • **Description**. Describes issues that occurred. • **Actions**. Describes whether the job completed successfully, and if not, lists the steps that the user can perform to resolve the issue. You must provide enough information so that the user can resolve the issue without help from the Lenovo Support. • **Severity**. Describes severity of the job. The job summary is optional for a job that completes successfully; however, it is good practice to set the summary, even when the severity is informational.
actionArgs	Array of strings	List of action arguments for the message
actionBundleKey	String	Bundle in which the user action is declared
actionBundleName	String	Bundle in which the translated user action is located
actionText	String	User action to use if there is no translation
descriptionArgs	Array of strings	List of arguments for the message
descriptionBundleKey	String	Bundle in which the message description is declared
descriptionBundleName	String	Bundle in which the translated message description is located
descriptionText	String	Message description to use if there is no translation
severity	String	Severity of the subtask. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).
time_spent	Long	Duration of the task in milliseconds.
taskid	Integer	Task ID
uuid	String	UUID associated with the unmanagement.
status		Status of the management job. This can be one of the following values. • **0**. Created. • **50**. Incomplete. • **100**. Done. • **101**. Done_Warnimg.

The following example is returned if the request is successful.


```
{
    "progress": 100.0,
    "results": [{
        "messageBundle": "com.lenovo.lxca.discovery.bundle.rest.messages",
        "messageID": "0509_LONG",
        "messageParameters": "10.240.72.172",
        "progress": 100.0,
        "result": "SUCCESS",
```

```
        "resultLongDescription": "The unmanagement job has completed successfully",
        "resultShortDescription": "Success",
        "status": {
            "description": [{
                "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
                "messageID": "1028_LONG"
            }],
            "percentage": 100.0,
            "state": "Complete",
            "substatus": [{
                "completed": true,
                "id": "STARTING",
                "longDescription": "Starting device unmanagement job",
                "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
                "messageID": "1000_SHORT",
                "progress": 100.0,
                "shortDescription": "Starting",
                "started": true,
                "status": {
                    "percentage": 100.0,
                    "state": "Complete"
                },
                "userAction": ""
            },
            ...
            {
                "completed": true
                "id": "CFG_CABINET",
                "longDescription": "Configuring Hardware location",
                "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
                "messageID": "1097_SHORT",
                "progress": 100.0,
                "shortDescription": "Configuring Hardware location",
                "started": true,
                "status": {
                    "percentage": 100.0,
                    "state": "Complete"
                },
                "userAction": "",
            }]
        },
         "summary": {
            "actionArgs": [],
            "actionBundleKey": "",
            "actionBundleName": ""
            "actionText": "",
            "descriptionArgs": [],
            "descriptionBundleKey": "1028_LONG",
            "descriptionBundleName": "com.lenovo.lxca.discovery.bundle.tasks.messages",
            "descriptionText": "The unmanagement job has completed successfully",
            "severity": "Informational",
         }
        "time_spent": 234216,
        "taskid": 18725,
        "uuid": "46920c143355486f97c19a34abc7d746"
    }],
    "status": "DONE"
}
```

/ipDuplication

Use this REST API to check whether the specified IP addresses are duplicate in the same subnet.

HTTP methods

GET

GET /ipDuplication

Use this method to check whether the specified IP addresses are duplicate in the same subnet.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/ipDuplication`

Query parameters

Parameters	Required / Optional	Description
IPs=*{IP_addresses}*	Required	List of IP addresses to check for duplication

The following example checks whether the two IP addresses are duplicate.

```
GET https://192.0.2.0/ipDuplication?IPs=10.243.9.18,10.243.3.171
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
duplicateIn	String	Identifies the environment in which the IP address is duplicate. This can be one of the following values. • **network**. A duplicate IP address was found in the same network. • **managed**. A managed device uses the same IP address. • **in_managed**. A device that is currently in the management process uses the same IP address.
IP	String	IP address
available	Boolean	Indicates whether the IP address is not duplicates and can be used. This can be one of the following values. • **true**. The IP address is not duplicate and can be use. • **false**. The IP address is duplicate and cannot be use.

The following example is returned if the request is successful.

```
[
   {
      "duplicateIn": "network",
      "IP": "10.243.3.170",
      "available": false
   },
   …,
   {
      "IP": "10.243.3.171",
      "available": true
   }
]
```

/ipSettings

Use this REST API to retrieve information about whether Lenovo XClarity Administrator checks for duplicate IP addresses in the same subnet and to enable or disable checking for duplicate IP addresses.

HTTP methods

GET, PUT

GET /ipSettings

Use this method to return information about whether Lenovo XClarity Administrator checks for duplicate IP addresses in the same subnet.

To retrieve a list of duplicate IP addresses in the same subnet, use GET /ipDuplication.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/ipSettings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
duplicateIpCheck	Boolean	Indicates whether checking for duplicate IP addresses in the same subnet is enabled or disabled. This can be one of the following values. • **true**. Checks for duplicate IP addresses. When enabled, XClarity Administrator raises an alert if you attempt to change the IP address of XClarity Administrator or manage a device that has the same IP address as another device that is under management or another device found in the same subnet. • **false**. Does not check for duplicate IP addresses.

The following example is returned if the request is successful.

```
{
   "duplicateIpCheck": true
}
```

PUT /ipSettings

Use this method to enable or disable checking for duplicate IP addresses in the same subnet.

Authentication

Authentication with username and password is required.

Request URL

```
PUT https://{management_server_IP}/ipSettings
```

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
duplicateIpCheck	Optional	Boolean	Indicates whether checking for duplicate IP addresses in the same subnet is enabled or disabled. This can be one of the following values. • **true**. Checks for duplicate IP addresses. When enabled, XClarity Administrator raises an alert if you attempt to change the IP address of XClarity Administrator or manage a device that has the same IP address as another device that is under management or another device found in the same subnet. • **false**. Does not check for duplicate IP addresses.

The following example enables checking for duplicate IP addresses in the same subnet.

```
{
   "duplicateIpCheck": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

Chapter 4. Inventory

The following resources are available for performing inventory functions.

/cabinet/view

Use this REST API to retrieve or modify the numbering order preference for devices in racks (cabinets).

HTTP methods

GET, PUT

GET /cabinet/view

Use this method to return the numbering order preference for devices in racks (cabinets).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/cabinet/view`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
topToBottomView	Boolean	Indicates the rack numbering order preference. This can be one of the following values. • **true**. Devices numbers are ordered from the top to the bottom (for example, 1 – 52). • **false**. Devices numbers are ordered from bottom to the top (for example, 52 – 1).

The following example is returned if the request is successful.

```
{
   "topToBottomView": true
}
```

PUT /cabinet/view

Use this method to modify the numbering order preference for devices in racks (cabinets).

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/cabinet/view`

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
topToBottomView	Required	Boolean	Indicates the rack numbering order preference. This can be one of the following values. • **true**. Devices numbers are ordered from the top to the bottom (for example, 1 – 52). • **false**. Devices numbers are ordered from bottom to the top (for example, 52 – 1).

The following example sets the device-order preference to top to bottom.

```
{
   "topToBottomView": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/canisters

Use this REST API to retrieve properties and metrics for all Flex System storage controllers (canisters). Each controller represents one of the storage controllers in a Flex System storage device.

HTTP methods

GET

GET /canisters

Use this method to return properties for all Flex System storage controllers (canisters).

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/canisters
```

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

The following example returns **ipv4Addresses** and **ipv6Addresses** properties in addition to the base properties.

```
GET https://192.0.2.0/canisters?includeAttributes=ipv4Addresses,ipv6Addresses
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
canisterList	Array	List of all storage- controllers
See GET /canisters/*{uuid}*	Object	Detailed information about the individual storage controller

The following example is returned if the request is successful.


```
{    "canisterList": [{
    "cabinetName": "lxcm-test",
    "chassisList": [],
    "complexList": [],
    "height": 52,
    "location": "",
    "nodeList": [{
        "complexNodeCount": -1,
        "itemInventory": {
            "activationKeys": [],
            "accessState": "Online",
            "addinCardSlots": 0,
            "arch": "x86_64",
            "backedBy": "real",
            "bladeState": 0,
            "bootMode": {
                "currentValue": "unspecified",
                "possibleValues": ["uefi","bios"]
            },
            "bootOrder": {
                "bootOrderList": [{
                    "bootType": "SingleUse",
                    "currentBootOrderDevices": ["default"],
                    "possibleBootOrderDevices": ["setup","network","hd","cd","default"]
                }],
                "uri": "nodes/5CF902D17961E511843E3C18A001C6A0/bootOrder"
            },
            "cmmDisplayName": "",
            "cmmHealthState": "Critical",
            "complexID": -1,
            "contact": "",
            "description": "chassis  RD650",
            "domainName": "labs.lenovo.com",
            "driveBays": 2,
            "drives": [{
                "bay": 2,
                "capacity": 250,
                "interfaceType": "SATA",
                "mediaType": "HDD",
                "raidPresence": "Non-RAID  drive",
                "speed": "3.0  Gb/s",
                "state": "active"
            },
            {
                "bay": 1,
                "capacity": 250,
                "interfaceType": "SATA",
                "mediaType": "HDD",
                "raidPresence": "Non-RAID  drive",
                "speed": "3.0  Gb/s",
                "state": "active"
            }],
```

```
"embeddedHypervisorPresence": false,
"encapsulation": {},
"errorFields": [],
"excludedHealthState": "Critical",
"expansionCards": [],
"expansionCardSlots": 0,
"expansionProducts": [],
"expansionProductType": "",
"fans": [],
"firmware": [{
    "build": "",
    "date": "",
    "name": "PSU 2",
    "role": "",
    "status": "ACTIVE",
    "type": "PSU 2",
    "version": "0.0.0"
},
...,
{
    "build": "",
    "date": "",
    "name": "System Manager (BMC)",
    "role": "",
    "status": "ACTIVE",
    "type": "System Manager (BMC)",
    "version": "1.42.78800"
}],
"flashStorage": [],
"FRU": "",
"fruSerialNumber": "8SSB20A05917R2SH56G004J",
"FQDN": "",
"hasOS": false,
"height": 2,
"hostMacAddresses": "",
"hostname": "RD650",
"ipInterfaces": [],
"ipv4Addresses": ["10.243.2.201"],
"ipv6Addresses": [],
"isConnectionTrusted": "true",
"isITME": false,
"isRemotePresenceEnabled": true,
"isScalable": false,
"lanOverUsb": "disabled",
"leds": [{
    "color": "Red",
    "conditions": "Fault",
    "location": "MotherBoard",
    "name": "LED FAN FAULT 5",
    "state": "Off"
},
...},
{
    "color": "Red",
    "conditions": "Fault",
    "location": "MotherBoard",
    "name": "LED FAN FAULT 6",
    "state": "Off"
}],
"location": {
    "lowestRackUnit": 51,
```

```
    "location": "",
    "rack": "lxcm-test",
    "room": ""
},
"logicalID": -1,
"macAddress": "00:8C:FA:E7:FE:4A,00:8C:FA:E7:FE:4B",
"machineType": "70D0",
"manufacturerId": "",
"manufacturer": "LENOVO",
"memoryModules": [{
    "capacity": 8,
    "displayName": "DIMM 1",
    "model": "",
    "manufacturer": "Samsung",
    "partNumber": "M393A1G40DB0-CPB",
    "serialNumber": "411e26be",
    "slot": 1,
    "speed": 1600,
    "speedMBs": 0,
    "type": "RDIMM",
    "voltage": "1.2V"
}],
"memorySlots": 0,
"mgmtProcIPaddress": "10.243.2.201",
"mgmtProcType": "UNKNOWN",
"model": "0026UX",
"name": "RD650",
"nist": {
    "currentValue": "Nist_800_131A_Strict",
    "possibleValues": ["Nist_800_131A_Strict","unsupported","Nist_800_131A_Custom",
                       "Compatibility"]
},
"overallHealthState": "Critical",
"partNumber": "",
"powerStatus": 8,
"productName": "RD650",
"parent": {
    "uri": "cabinet/83094B8D-4709-4254-8E28-2C571816FE81",
    "uuid": "83094B8D-4709-4254-8E28-2C571816FE81"
},
"partitionID": -1,
"pciCapabilities": [],
"pciDevices": [],
"ports": [],
"posID": "",
"powerAllocation": {
    "maximumAllocatedPower": 0,
    "minimumAllocatedPower": 0
},
"powerCappingPolicy": {
    "cappingACorDCMode": "UNKNOWN",
    "cappingPolicy": "UNKNOWN",
    "currentPowerCap": 0,
    "maxPowerCap": -1,
    "maximumPowerCappingHotPlugLevel": -1,
    "minimumHardCapLevel": -1,
    "minPowerCap": -1,
    "minimumPowerCappingHotPlugLevel": -1,
    "powerCappingAllocUnit": "watts"
},
"powerSupplies": [{
```

```
    "dataHandle": 0,
    "description": "Power Supply 1",
    "firmware": [],
    "hardwareRevision": "01",
    "healthState": "GOOD",
    "inputVoltageIsAC": false,
    "inputVoltageMax": 0
    "inputVoltageMin": 0,
    "leds": [{
        "color": "Amber",
        "location": "FRU",
        "name": "FAULT",
        "state": "Off"
    },
    ...,
    {
        "color": "Green",
        "location": "FRU",
        "name": "OUT",
        "state": "On"
    }],
    "manufactureDate": "2014-01-11",
    "manufacturerId": "LITEON",
    "model": "PS-2551-6L-LF",
    "name": "005V",
    "parent": {},
    "powerAllocation": {
        "totalInputPower": 0,
        "totalOutputPower": 0
    },
    "serialNumber": "005V",
    "slots": [0],
    "type": "PowerSupply",
    "uri": "powerSupply/null",
}],
"primary": false,
"processors": [{
    "cores": 6,
    "displayName": "",
    "family": "Intel Nehalem Family",
    "manufacturer": "GenuineIntel",
    "productVersion": "Haswell Server Model",
    "slot": 1,
    "socket": "",
    "speed": 1.6
}],
"processorSlots": 0,
"productId": "",
"raidSettings": [],
"secureBootMode": {
    "currentValue": "",
    "possibleValues": []
},
"securityDescriptor": {
    "managedAuthEnabled": false,
    "managedAuthSupported": false,
    "publicAccess": false,
    "roleGroups": [],
    "storedCredentials": {
        "description": "",
        "id": "557",
```

```
                "userName": "lenovo"
            },
            "uri": "nodes/5cf902d17961e511843e3c18a001c6a0"
        },
        "serialNumber": "MJ03210K",
        "slots": [1],
        "status": {
            "message": "managed",
            "name": "MANAGED"
        },
        "subSlots": [],
        "subType": "ThinkServer",
        "tlsVersion": {
            "possibleValues": ["unsupported",
            "TLS_12",
            "TLS_11",
            "TLS_10"],
            "currentValue": "Unknown"
        },
        "thinkServerFru": [{
            "description": "BackPlane1 FRU",
            "deviceName": "12GBP 12xL",
            "manufatucturer": "LENOVO",
            "manufatucturerDate": "Apr 28, 2015",
            "partNumber": "SSF0A47713",
            "serial": "8SSSF0A47713V1SH54W0077",
        }],
        "type": "Lenovo ThinkServer",
        "userDefinedName": "RD650",
        "userDescription": "",
        "uri": "nodes/5CF902D17961E511843E3C18A001C6A0",
        "uuid": "5CF902D17961E511843E3C18A001C6A0",
        "vnicMode": "disabled",
        "vpdID": ""
    },
    "itemHeight": 2,
    "itemLocation": "",
    "itemLocationRack": "lxcm-test",
    "itemLocationRoom": "",
    "itemLowerUnit": 51,
    "itemName": "SERVER-5CF902D17961E511843E3C18A001C6A0",
    "itemParentUUID": "83094B8D-4709-4254-8E28-2C571816FE81",
    "itemSubType": "ThinkServer",
    "itemType": "SERVER",
    "itemUUID": "5CF902D17961E511843E3C18A001C6A0",
    "nodeCount": -1,
    "physicalID": -1
}],
"placeholderList": [],
"room": "",
"storageList": [{
    "itemName": "S3200",
    "itemUUID": "500C0FF0280E8B3C",
    "itemParentUUID": "208000C0FF280E8B",
    "itemLocationRoom": "",
    "itemLocationRack": "lxcm-test",
    "itemLocation": "",
    "itemLowerUnit": 49,
    "itemType": "STORAGE",
    "itemHeight": 2,
    "itemSubType": "Enclosure",
```

```
"itemInventory": {
    "accessState": "Online",
    "canisterSlots": 2,
    "cmmHealthState": "Critical",
    "contact": "Alan Hawkins5",
    "description": "mineminemine",
    "diskGroups": 3,
    "driveBays": 12,
    "enclosures": [{
        "canisters": [{
            "cmmDisplayName": "controller_b",
            "controllerId": "B",
            "controllerRedundancyMode": "Active-Active ULP",
            "controllerRedundancyStatus": "Redundant",
            "disks": 11,
            "diskBusType": "SAS",
            "diskChannels": 2,
            "expansionPorts": [{
                "healthReason": "No drive enclosure is connected to this expansion port. This is
                                 normal if this is the last (or only) enclosure in the cabling
                                 sequence of the system.",
                "health": "N/A",
                "healthRecommendation": "- No action is required.",
                "name": "Out Port",
                "status": "Disconnected"
            }],
            "energyMetrics": {
                "diskControllerTemperature": [],
                "inletAirTemperature": [],
                "memoryTemperature": []
            },
            "failedOverToThisController": "No",
            "failOverReason": "Not applicable",
            "firmware": {
                "backplaneType": "7",
                "buildDate": "Thu Jun 29 09:26:26 MDT 2017",
                "bundleVersion": "GL221R020-14",
                "capiVersion": "3.19",
                "cpldCodeVersion": "56",
                "diskInterfaceHardwareVersion": "3",
                "expanderControllerCodeVersion": "3206",
                "hardwareVersion": "5.2",
                "hostInterfaceHardwareVersion": "2",
                "hostInterfaceModuleModel": "6",
                "hostInterfaceModuleVersion": "11",
                "managementControllerCodeVersion": "GLM221R037-02",
                "managementControllerLoaderCodeVersion": "6.27.25440",
                "scBootMemoryReferenceCodeVersion": "1.2.1.10",
                "storageControllerCodeBaselevel": "GLS221R13-01",
                "storageControllerCodeVersion": "GLS221R13-01",
                "storageControllerCpuType": "Gladden 1300MHz",
                "storageControllerLoaderCodeVersion": "27.016",
            },
            "hardwareVersion": "5.2",
            "health": "Normal",
            "healthReason": "",
            "healthRecommendation": "",
            "hostPorts": 4,
            "networkPorts": {
                "addressingMode": "Manual",
                "gateway": "10.243.0.1",
```

```
            "health": "OK",
            "healthReason": "",
            "healthRecommendation": "",
            "ipAddress": "10.243.9.149",
            "ipVersion": 4,
            "macAddress": "00:c0:ff:28:04:01",
            "name": "mgmtport_b",
            "networkMask": "255.255.224.0"
        },
        "phyIsolation": "Enabled",
        "ports": [{
            "action": "- If this host port is intentionally unused, no action is required.\n
                       - Otherwise, use an appropriate interface cable to connect this host
                         port to a switch or host.\n
                       - If a cable is connected, check the cable and the switch or host for
                         problems.",
            "actualSpeed": "",
            "configSpeed": "Auto",
            "health": "N/A",
            "media": "FC(-)",
            "port": "B3",
            "reason": "There is no active connection to this host port.",
            "status": "Disconnected",
            "targetId": "277000c0ff280e8b",
            "topology": "PTP"
        },
        ...]
        "position": "Bottom",
        "powerState": "On",
        "systemCacheMemory": 6144,
        "serialNumber": "11S00WC050Y010DH677182",
        "revision": "0",
        "status": "Operational",
    }
    ...],
    "drives": [{
        "model": "ST2000NM0034     X",
        "vendorName": "LENOVO-X",
        "status": "Up",
        "location": "0.7",
        "serialNumber": "Z4H04RK70000R543K1TB",
        "healthReason": "The disk may contain invalid metadata.",
        "health": "Degraded",
        "type": "SAS MDL",
        "healthRecommendation": "- If the associated disk group is offline or quarantined, contact
                                  technical support. Otherwise, clear the disk's metadata to reuse
                                  the disk.",
        "size": "2000.3GB"
    },
    ...],
    "enclosureInfo": {
        "diskCount": 11,
        "driveBays": 12,
        "enclosureId": 0,
        "health": "Degraded",
        "midplaneSerialNumber": "11S00WC065Y010DH67C0RF",
        "model": "S3200",
        "vendorName": "Lenovo",
        "status": "Up",
        "wwn": "500C0FF0280E8B3C"
    },
```

```
    "energyMetrics": {
        "enclosurePower": []
    },
    "frus": [{
        "description": "SPS Memory Card",
        "fruLocation": "LOWER IOM MEMORY CARD SLOT",
        "fruStatus": "OK",
        "partNumber": "40-00000053",
        "serialNumber": "",
        "shortName": "Memory Card"
    },
    ...],
    "location": {
        "rack": "lxcm-test",
        "room": "",
        "location": "",
        "lowestRackUnit": 49
    },
    "powerSupplies": [{
        "health": "OK",
        "healthReason": "",
        "healthRecommendation": "",
        "model": "00WC067",
        "position": "Right",
        "status": "Up",
        "vendorName": ""
    },
    {
        "health": "OK",
        "healthReason": "",
        "healthRecommendation": "",
        "model": "00WC067",
        "position": "Left",
        "status": "Up",
        "vendorName": ""
    }],
    "slots": ["0","1","2","3","4","5","6","7","8","9","10"]
}],
"enclosureCount": 1,
"excludedHealthState": "Critical",
"healthReason": "A subcomponent of this component is unhealthy.",
"ipv4Addresses": ["10.243.9.148","10.243.9.149"],
"isConnectionTrusted": "true",
"location": {
    "rack": "lxcm-test",
    "room": "",
    "location": "",
    "lowestRackUnit": 49
},
"machineType": "6411",
"mgmtProcIPaddress": "10.243.9.148",
"model": "S3200",
"name": "S3200",
"otherMcStatus": "Operational",
"overallHealthState": "Critical",
"parent": {
    "uri": ""
    "uuid": ""
},
"pfu": "Idle",
"productBrand": "Storage",
```

```
            "productName": "S3200",
            "scsiProductId": "S3200",
            "scsiVendorId": "Lenovo",
            "securityDescriptor": {
                "managedAuthEnabled": false,
                "managedAuthSupported": false,
                "publicAccess": false,
                "roleGroups": [],
                "uri": "storage/208000c0ff280e8b"
            },
            "serialNumber": "280E8B",
            "supportedLocales": "English (English), Arabic (العربية), Portuguese (português), Spanish (español),
                                 French (français), German (Deutsch), Italian (italiano), Japanese (日本語),
                                 Korean (한국어), Dutch (Nederlands), Russian (русский),
                                 Chinese-Simplified (简体中文), Chinese-Traditional (繁體中文)",
            "systemLocation": ",,lxcm-test",
            "type": "Lenovo Storage",
            "uri": "storage/208000C0FF280E8B",
            "userDefinedName": "S3200",
            "userDescription": "mineminemine",
            "uuid": "208000C0FF280E8B",
            "vendorName": "Lenovo",
            "virtualPools": 2,
            "wwnn": "208000C0FF280E8B"
        }
    }],
    "switchList": [],
    "UUID": "83094B8D-4709-4254-8E28-2C571816FE81"
}]}
```

/canisters/*{uuid}*

Use this REST API to retrieve or update properties for a specific Flex System storage controller (canister). Each controller represents one of the controllers in a Flex System storage device.

HTTP methods

GET, PUT

GET /canisters/*{uuid}*

Use this method to return properties for a specific Flex System storage controller (canister).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/canisters/{uuid}`

where *{uuid}* is the UUID of the storage controller to be retrieved. To obtain the storage-controller UUID, use the GET /canisters method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

The following example returns **ipv4Addresses** and **ipv6Addresses** properties in addition to the base properties.

```
GET https://192.0.2.0/canisters/6ED2CB368C594C66C2BB066D5A306138?
includeAttributes=ipv4Addresses,ipv6Addresses
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
activationKeys	Array	List of installed Feature On Demand (FOD) keys
backedBy	String	This can be one of the following values. • **real**. The inventory describes real hardware. • **demo**. The inventory describes demo (mock) hardware. • **proxy**. A proxy is temporarily serving to provide the inventory.

Attributes	Type	Description
bladeState	Integer	The blade state. This can be one of the following values. • **0**. Initializing • **1**. Active • **2**. Discovering • **3**. Provisioning • **4**. Provision passed • **5**. Provision failed • **6**. Provisioning failed with isolate • **7**. Pre initialization • **8**. SDR load • **9**. POST initialization • **10**. Communications error • **11**. Init failed • **12**. Kernel mode • **13**. Maintenance mode • **14**. Fire hose dump mode • **15**. Flashing • **16**. No power • **17**. Unknown • **255**. Not Applicable
cmmDisplayName	String	Display name provided by the CMM
cmmHealthState	String	Health summary that corresponds to the highest event severity of all the devices. This can be one of the following values: • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
contact	String	Contact name
dataHandle	Long	Time stamp of the last status update
description	String	Description provided by the CMM
domainName	String	Domain name
driveBays	Integer	Total number of drive bays
drives	Array	Information about the drives
bay	Integer	Drive bay location
capacity	Integer	Drive capacity, in GB
errorFields	Array of objects where each object has *<string, error-Code}*	Error codes. This can be one of the following values. • **FETCH_SUCCESS** • **FETCH_FAILED** • **NO_CONNECTOR** • **FATAL_EXCEPTION** • **NETWORK_FAIL**
firmware	Array	Information about the firmware
build	String	Firmware build

Attributes	Type	Description
date	String	Firmware date
name	String	Firmware name
role	String	Firmware role
status	String	Firmware status
type	String	Firmware type
version	String	Firmware version
FRU	String	FRU part number
fruSerialNumber	String	FRU serial number
hostname	String	Hostname
ipInterfaces	Array	Information about the storage-controller IP addresses
IPv4assignments	Array	Information about IPv4 assignments
address	String	IPv4 address
gateway	String	IPv4 gateway
id	Integer	IPv4 assignment ID
subnet	String	IPv4 subnet mask
type	String	The type of the IPv4 assignment. This can be one of the following values. • **INUSE** • **CONFIGURED** • **ALIAS** • **UNKNOWN**
IPv4DHCPmode	String	IPv4 address DHCP mode. This can be one of the following values. • **STATIC_ONLY** • **DHCP_ONLY** • **DHCP_THEN_STATIC** • **UNKNOWN**
IPv4enabled	Boolean	Identifies whether IPv4 is enabled. This can be one of the following values. • **true**. IPv4 is enabled • **false**. IPv4 is disabled
IPv6assignments	Array	Information about IPv6 assignments
address	String	IPv6 address
gateway	String	IPv6 gateway
id	Integer	IPv6 assignment ID
prefix	Integer	IPv6 prefix
scope	String	Scope of the IPv6 assignment. This can be one of the following values. • **Global** • **LinkLocal** • **Unknown**

Attributes	Type	Description
source	String	Source of the IPv6 assignment. This can be one of the following values. • **DHCP** • **Statelesss** • **Static** • **Other** • **Unknown**
type	String	Type of the IPv6 assignment. This can be one of the following values. • **INUSE** • **CONFIGURED** • **ALIAS** • **UNKNOWN**
IPv6enabled	Boolean	Identifies whether IPv6 is enabled. This can be one of the following values. • **true**. IPv6 is enabled • **false**. IPv6 is disabled
IPv6DHCPenabled	Boolean	Identifies whether IPv6 DHCP is enabled. This can be one of the following values. • **true**. IPv6 DHCP is enabled • **false**. IPv6 DHCP is disabled
IPv6statelessEnabled	Boolean	Identifies whether IPv6 stateless is enabled. This can be one of the following values. • **true**. IPv6 stateless is enabled • **false**. IPv6 stateless is disabled
IPv6staticEnabled	Boolean	Identifies whether IPv6 static is enabled. This can be one of the following values. • **true**. IPv6 static is enabled • **false**. IPv6 static is disabled
name	String	Interface name (such as eth0)
label	String	Label
ipv4Addresses	Array of strings	The list of IPv4 addresses
ipv4ServiceAddress	String	IPv4 service address
ipv6Addresses	Array of strings	List of IPV6 addresses
ipv6ServiceAddress	String	IPv6 service address
lanOverUsb	String	Identifies whether the LAN over USB is enabled or disabled. This can be one of the following values. • **enabled** • **disabled**
leds	Array	Information about storage-controller LEDs
color	String	LED color. This can be one of the following values. • **Red** • **Amber** • **Yellow** • **Green** • **Blue** • **Unknown**

Attributes	Type	Description
location	String	LED location. This can be one of the following values. • **Front panel** • **Lightpath Card** • **Planar** • **FRU** • **Rear Panel** • **Unknown**
name	String	LED name
state	String	LED state. This can be one of the following values. • **Off** • **On** • **Blinking** • **Unknown**
location	Array	Storage-controller location details
location	String	Location description
lowestRackUnit	Integer	Lowest rack unit
rack	String	Rack
room	String	Room
macAddress	String	MAC address
machineType	String	Machine type
manufacturer	String	Manufacturer
uri	String	Parent URI
uuid	String	Parent UUID
manufacturerID	String	Manufacturer ID
memoryModules	Array	Information about the memory modules
capacity	Long	Capacity
displayName	String	Display name
manufacturer	String	Manufacturer
model	String	Model
partNumber	String	Part number
serialNumber	String	Serial number
slot	Integer	Slot
speed	Long	Speed
type	String	Type
model	String	Storage-controller model
memorySlots	Integer	Total number of memory slots

Attributes	Type	Description
name	String	Name that is displayed in the user interface for this device The value of this attribute is determined by **preferredDisplayName** attribute in the GET /aicc method. For example, if the **preferredDisplayName** attribute is set to “hostname,” then the value for this **name** attribute is the same as the **hostname** attribute in the GET /aicc method.
parent	Array	Parent information for the target device
uri	String	Parent URI
uuid	String	Parent UUID
partNumber	String	Part number
powerStatus	Integer	Power status. This can be one of the following values. • **0**. Unknown • **5**. Off • **8**. On • **17**. Standby
processors	Array	Processor details
posID	String	Position ID
cores	Integer	Processor cores
family	String	Processor family
manufacturer	String	Processor manufacturer
slot	Integer	Slot number
speed	Long	Processor speed (GHz)
processorSlots	Integer	Total number of processor slots
productId	String	Product ID
productName	String	Product name
serialNumber	String	Serial number
serviceHostName	String	Service hostname
slots	Array of integers	Slots occupied
subSlots	Array of integers	Sub-slots occupied
subType	String	Sub-type
type	String	Resource type. This value is always “ITE.”
uri	String	Storage-controller URI
userDefinedName	String	User-defined name for the device
userDescription	String	User-defined description
uuid	String	UUID

Attributes	Type	Description
vnicMode	String	Indicates whether VNIC mode is enabled. This can be one of the following values. • **enabled**. VNIC mode is enabled. • **disabled**. VNIC mode is disabled.
vpdID	String	VPD ID

The following example is returned if the request is successful.


```
{
    "cabinetName": "lxcm-test",
    "chassisList": [],
    "complexList": [],
    "height": 52,
    "location": "",
    "nodeList": [{
        "complexNodeCount": -1,
        "itemInventory": {
            "activationKeys": [],
            "accessState": "Online",
            "addinCardSlots": 0,
            "arch": "x86_64",
            "backedBy": "real",
            "bladeState": 0,
            "bootMode": {
                "currentValue": "unspecified",
                "possibleValues": ["uefi","bios"]
            },
            "bootOrder": {
                "bootOrderList": [{
                    "bootType": "SingleUse",
                    "currentBootOrderDevices": ["default"],
                    "possibleBootOrderDevices": ["setup","network","hd","cd","default"]
                }],
                "uri": "nodes/5CF902D17961E511843E3C18A001C6A0/bootOrder"
            },
            "cmmDisplayName": "",
            "cmmHealthState": "Critical",
            "complexID": -1,
            "contact": "",
            "description": "chassis RD650",
            "domainName": "labs.lenovo.com",
            "driveBays": 2,
            "drives": [{
                "bay": 2,
                "capacity": 250,
                "interfaceType": "SATA",
                "mediaType": "HDD",
                "raidPresence": "Non-RAID drive",
                "speed": "3.0 Gb/s",
                "state": "active"
            },
            {
                "bay": 1,
                "capacity": 250,
                "interfaceType": "SATA",
                "mediaType": "HDD",
                "raidPresence": "Non-RAID drive",
                "speed": "3.0 Gb/s",
                "state": "active"
```

```
}],
"embeddedHypervisorPresence": false,
"encapsulation": {},
"errorFields": [],
"excludedHealthState": "Critical",
"expansionCards": [],
"expansionCardSlots": 0,
"expansionProducts": [],
"expansionProductType": "",
"fans": [],
"firmware": [{
    "build": "",
    "date": "",
    "name": "PSU 2",
    "role": "",
    "status": "ACTIVE",
    "type": "PSU 2",
    "version": "0.0.0"
},
...,
{
    "build": "",
    "date": "",
    "name": "System Manager (BMC)",
    "role": "",
    "status": "ACTIVE",
    "type": "System Manager (BMC)",
    "version": "1.42.78800"
}],
"flashStorage": [],
"FRU": "",
"fruSerialNumber": "8SSB20A05917R2SH56G004J",
"FQDN": "",
"hasOS": false,
"height": 2,
"hostMacAddresses": "",
"hostname": "RD650",
"ipInterfaces": [],
"ipv4Addresses": ["10.243.2.201"],
"ipv6Addresses": [],
"isConnectionTrusted": "true",
"isITME": false,
"isRemotePresenceEnabled": true,
"isScalable": false,
"lanOverUsb": "disabled",
"leds": [{
    "color": "Red",
    "conditions": "Fault",
    "location": "MotherBoard",
    "name": "LED FAN FAULT 5",
    "state": "Off"
},
...},
{
    "color": "Red",
    "conditions": "Fault",
    "location": "MotherBoard",
    "name": "LED FAN FAULT 6",
    "state": "Off"
}],
"location": {
```

```
    "lowestRackUnit": 51,
    "location": "",
    "rack": "lxcm-test",
    "room": ""
},
"logicalID": -1,
"macAddress": "00:8C:FA:E7:FE:4A,00:8C:FA:E7:FE:4B",
"machineType": "70D0",
"manufacturerId": "",
"manufacturer": "LENOVO",
"memoryModules": [{
    "capacity": 8,
    "displayName": "DIMM 1",
    "model": "",
    "manufacturer": "Samsung",
    "partNumber": "M393A1G40DB0-CPB",
    "serialNumber": "411e26be",
    "slot": 1,
    "speed": 1600,
    "speedMBs": 0,
    "type": "RDIMM",
    "voltage": "1.2V"
}],
"memorySlots": 0,
"mgmtProcIPaddress": "10.243.2.201",
"mgmtProcType": "UNKNOWN",
"model": "0026UX",
"name": "RD650",
"nist": {
    "currentValue": "Nist_800_131A_Strict",
    "possibleValues": ["Nist_800_131A_Strict","unsupported","Nist_800_131A_Custom",
                       "Compatibility"]
},
"overallHealthState": "Critical",
"partNumber": "",
"powerStatus": 8,
"productName": "RD650",
"parent": {
    "uri": "cabinet/83094B8D-4709-4254-8E28-2C571816FE81",
    "uuid": "83094B8D-4709-4254-8E28-2C571816FE81"
},
"partitionID": -1,
"pciCapabilities": [],
"pciDevices": [],
"ports": [],
"posID": "",
"powerAllocation": {
    "maximumAllocatedPower": 0,
    "minimumAllocatedPower": 0
},
"powerCappingPolicy": {
    "cappingACorDCMode": "UNKNOWN",
    "cappingPolicy": "UNKNOWN",
    "currentPowerCap": 0,
    "maxPowerCap": -1,
    "maximumPowerCappingHotPlugLevel": -1,
    "minimumHardCapLevel": -1,
    "minPowerCap": -1,
    "minimumPowerCappingHotPlugLevel": -1,
    "powerCappingAllocUnit": "watts"
},
```

```
"powerSupplies": [{
    "dataHandle": 0,
    "description": "Power Supply 1",
    "firmware": [],
    "hardwareRevision": "01",
    "healthState": "GOOD",
    "inputVoltageIsAC": false,
    "inputVoltageMax": 0
    "inputVoltageMin": 0,
    "leds": [{
        "color": "Amber",
        "location": "FRU",
        "name": "FAULT",
        "state": "Off"
    },
    ...,
    {
        "color": "Green",
        "location": "FRU",
        "name": "OUT",
        "state": "On"
    }],
    "manufactureDate": "2014-01-11",
    "manufacturerId": "LITEON",
    "model": "PS-2551-6L-LF",
    "name": "005V",
    "parent": {},
    "powerAllocation": {
        "totalInputPower": 0,
        "totalOutputPower": 0
    },
    "serialNumber": "005V",
    "slots": [0],
    "type": "PowerSupply",
    "uri": "powerSupply/null",
}],
"primary": false,
"processors": [{
    "cores": 6,
    "displayName": "",
    "family": "Intel Nehalem Family",
    "manufacturer": "GenuineIntel",
    "productVersion": "Haswell Server Model",
    "slot": 1,
    "socket": "",
    "speed": 1.6
}],
"processorSlots": 0,
"productId": "",
"raidSettings": [],
"secureBootMode": {
    "currentValue": "",
    "possibleValues": []
},
"securityDescriptor": {
    "managedAuthEnabled": false,
    "managedAuthSupported": false,
    "publicAccess": false,
    "roleGroups": [],
    "storedCredentials": {
        "description": "",
```

```
                "id": "557",
                "userName": "lenovo"
            },
            "uri": "nodes/5cf902d17961e511843e3c18a001c6a0"
        },
        "serialNumber": "MJ03210K",
        "slots": [1],
        "status": {
            "message": "managed",
            "name": "MANAGED"
        },
        "subSlots": [],
        "subType": "ThinkServer",
        "tlsVersion": {
            "possibleValues": ["unsupported",
            "TLS_12",
            "TLS_11",
            "TLS_10"],
            "currentValue": "Unknown"
        },
        "thinkServerFru": [{
            "description": "BackPlane1 FRU",
            "deviceName": "12GBP 12xL",
            "manufatucturer": "LENOVO",
            "manufatucturerDate": "Apr 28, 2015",
            "partNumber": "SSF0A47713",
            "serial": "8SSSF0A47713V1SH54W0077",
        }],
        "type": "Lenovo ThinkServer",
        "userDefinedName": "RD650",
        "userDescription": "",
        "uri": "nodes/5CF902D17961E511843E3C18A001C6A0",
        "uuid": "5CF902D17961E511843E3C18A001C6A0",
        "vnicMode": "disabled",
        "vpdID": ""
    },
    "itemHeight": 2,
    "itemLocation": "",
    "itemLocationRack": "lxcm-test",
    "itemLocationRoom": "",
    "itemLowerUnit": 51,
    "itemName": "SERVER-5CF902D17961E511843E3C18A001C6A0",
    "itemParentUUID": "83094B8D-4709-4254-8E28-2C571816FE81",
    "itemSubType": "ThinkServer",
    "itemType": "SERVER",
    "itemUUID": "5CF902D17961E511843E3C18A001C6A0",
    "nodeCount": -1,
    "physicalID": -1
}],
"placeholderList": [],
"room": "",
"storageList": [{
    "itemName": "S3200",
    "itemUUID": "500C0FF0280E8B3C",
    "itemParentUUID": "208000C0FF280E8B",
    "itemLocationRoom": "",
    "itemLocationRack": "lxcm-test",
    "itemLocation": "",
    "itemLowerUnit": 49,
    "itemType": "STORAGE",
    "itemHeight": 2,
```

```
"itemSubType": "Enclosure",
"itemInventory": {
    "accessState": "Online",
    "canisterSlots": 2,
    "cmmHealthState": "Critical",
    "contact": "Alan Hawkins5",
    "description": "mineminemine",
    "diskGroups": 3,
    "driveBays": 12,
    "enclosures": [{
        "canisters": [{
            "cmmDisplayName": "controller_b",
            "controllerId": "B",
            "controllerRedundancyMode": "Active-Active ULP",
            "controllerRedundancyStatus": "Redundant",
            "disks": 11,
            "diskBusType": "SAS",
            "diskChannels": 2,
            "expansionPorts": [{
                "healthReason": "No drive enclosure is connected to this expansion port. This is
                                 normal if this is the last (or only) enclosure in the cabling
                                 sequence of the system.",
                "health": "N/A",
                "healthRecommendation": "- No action is required.",
                "name": "Out Port",
                "status": "Disconnected"
            }],
            "energyMetrics": {
                "diskControllerTemperature": [],
                "inletAirTemperature": [],
                "memoryTemperature": []
            },
            "failedOverToThisController": "No",
            "failOverReason": "Not applicable",
            "firmware": {
                "backplaneType": "7",
                "buildDate": "Thu Jun 29 09:26:26 MDT 2017",
                "bundleVersion": "GL221R020-14",
                "capiVersion": "3.19",
                "cpldCodeVersion": "56",
                "diskInterfaceHardwareVersion": "3",
                "expanderControllerCodeVersion": "3206",
                "hardwareVersion": "5.2",
                "hostInterfaceHardwareVersion": "2",
                "hostInterfaceModuleModel": "6",
                "hostInterfaceModuleVersion": "11",
                "managementControllerCodeVersion": "GLM221R037-02",
                "managementControllerLoaderCodeVersion": "6.27.25440",
                "scBootMemoryReferenceCodeVersion": "1.2.1.10",
                "storageControllerCodeBaselevel": "GLS221R13-01",
                "storageControllerCodeVersion": "GLS221R13-01",
                "storageControllerCpuType": "Gladden 1300MHz",
                "storageControllerLoaderCodeVersion": "27.016",
            },
            "hardwareVersion": "5.2",
            "health": "Normal",
            "healthReason": "",
            "healthRecommendation": "",
            "hostPorts": 4,
            "networkPorts": {
                "addressingMode": "Manual",
```

```
            "gateway": "10.243.0.1",
            "health": "OK",
            "healthReason": "",
            "healthRecommendation": "",
            "ipAddress": "10.243.9.149",
            "ipVersion": 4,
            "macAddress": "00:c0:ff:28:04:01",
            "name": "mgmtport_b",
            "networkMask": "255.255.224.0"
        },
        "phyIsolation": "Enabled",
        "ports": [{
            "action": "- If this host port is intentionally unused, no action is required.\n
                       - Otherwise, use an appropriate interface cable to connect this host
                         port to a switch or host.\n
                       - If a cable is connected, check the cable and the switch or host for
                         problems.",
            "actualSpeed": "",
            "configSpeed": "Auto",
            "health": "N/A",
            "media": "FC(-)",
            "port": "B3",
            "reason": "There is no active connection to this host port.",
            "status": "Disconnected",
            "targetId": "277000c0ff280e8b",
            "topology": "PTP"
        },
        ...]
        "position": "Bottom",
        "powerState": "On",
        "systemCacheMemory": 6144,
        "serialNumber": "11S00WC050Y010DH677182",
        "revision": "0",
        "status": "Operational",
    }
    ...],
    "drives": [{
        "model": "ST2000NM0034     X",
        "vendorName": "LENOVO-X",
        "status": "Up",
        "location": "0.7",
        "serialNumber": "Z4H04RK70000R543K1TB",
        "healthReason": "The disk may contain invalid metadata.",
        "health": "Degraded",
        "type": "SAS MDL",
        "healthRecommendation": "- If the associated disk group is offline or quarantined, contact
                                  technical support. Otherwise, clear the disk's metadata to reuse
                                  the disk.",
        "size": "2000.3GB"
    },
    ...],
    "enclosureInfo": {
        "diskCount": 11,
        "driveBays": 12,
        "enclosureId": 0,
        "health": "Degraded",
        "midplaneSerialNumber": "11S00WC065Y010DH67C0RF",
        "model": "S3200",
        "vendorName": "Lenovo",
        "status": "Up",
        "wwn": "500C0FF0280E8B3C"
```

```
    },
    "energyMetrics": {
        "enclosurePower": []
    },
    "frus": [{
        "description": "SPS Memory Card",
        "fruLocation": "LOWER IOM MEMORY CARD SLOT",
        "fruStatus": "OK",
        "partNumber": "40-00000053",
        "serialNumber": "",
        "shortName": "Memory Card"
    },
    ...],
    "location": {
        "rack": "lxcm-test",
        "room": "",
        "location": "",
        "lowestRackUnit": 49
    },
    "powerSupplies": [{
        "health": "OK",
        "healthReason": "",
        "healthRecommendation": "",
        "model": "00WC067",
        "position": "Right",
        "status": "Up",
        "vendorName": ""
    },
    {
        "health": "OK",
        "healthReason": "",
        "healthRecommendation": "",
        "model": "00WC067",
        "position": "Left",
        "status": "Up",
        "vendorName": ""
    }],
    "slots": ["0","1","2","3","4","5","6","7","8","9","10"]
}],
"enclosureCount": 1,
"excludedHealthState": "Critical",
"healthReason": "A subcomponent of this component is unhealthy.",
"ipv4Addresses": ["10.243.9.148","10.243.9.149"],
"isConnectionTrusted": "true",
"location": {
    "rack": "lxcm-test",
    "room": "",
    "location": "",
    "lowestRackUnit": 49
},
"machineType": "6411",
"mgmtProcIPaddress": "10.243.9.148",
"model": "S3200",
"name": "S3200",
"otherMcStatus": "Operational",
"overallHealthState": "Critical",
"parent": {
    "uri": ""
    "uuid": ""
},
"pfu": "Idle",
```

```
            "productBrand": "Storage",
            "productName": "S3200",
            "scsiProductId": "S3200",
            "scsiVendorId": "Lenovo",
            "securityDescriptor": {
                "managedAuthEnabled": false,
                "managedAuthSupported": false,
                "publicAccess": false,
                "roleGroups": [],
                "uri": "storage/208000c0ff280e8b"
            },
            "serialNumber": "280E8B",
            "supportedLocales": "English (English), Arabic (العربية), Portuguese (português), Spanish (español),
                                 French (français), German (Deutsch), Italian (italiano), Japanese (日本語),
                                 Korean (한국어), Dutch (Nederlands), Russian (русский),
                                 Chinese-Simplified (简体中文), Chinese-Traditional (繁體中文)",
            "systemLocation": ",,lxcm-test",
            "type": "Lenovo  Storage",
            "uri": "storage/208000C0FF280E8B",
            "userDefinedName": "S3200",
            "userDescription": "mineminemine",
            "uuid": "208000C0FF280E8B",
            "vendorName": "Lenovo",
            "virtualPools": 2,
            "wwnn": "208000C0FF280E8B"
        }
    }],
    "switchList": [],
    "UUID": "83094B8D-4709-4254-8E28-2C571816FE81"
}
```


PUT /canisters/*{uuid}*

Use this method to modify properties, refresh inventory, or perform a power operation on a specific Flex System storage controller (canister).

The request body differs depending on the action that you want to perform. You can use this PUT method to perform the following management actions.

- Table 5 “Modify storage-controller properties” on page 142
- Table 6 “Modify the power state” on page 144
- Table 7 “Refresh the inventory” on page 144

If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/canisters/{uuid}`

where *{uuid}* is the UUID of the storage controller to be retrieved. To obtain the storage-controller UUID, use the GET /canisters method.

Query parameters

Attributes	Required / Optional	Description
synchronous=*{value}*	Optional	When modifying attributes, indicates when the job ID is returned • **true**. (default) Returns the job ID and job status after the job is complete. • **false**. Returns the job ID immediately. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. **Note:** This query parameter applies only when one or more property parameters are specified in the request body.

The following example returns the job ID and job status immediately.

```
GET https://192.0.2.0/canisters/6ED2CB368C594C66C2BB066D5A306138?synchronous=false
```

Request body

You can specify attributes from one of the following tables in each request.

Table 5. Modify storage-controller properties

Attributes	Required / Optional	Type	Description
contact	Optional	String	Storage-controller contact information
domainName	Optional	String	Storage-controller domain name
hostname	Optional	String	Storage-controller hostname
ipInterfaces	Optional	Array	Information about the storage-controller IP addresses **Note:** If specified, you must also specify the **name** attribute.
IPv4DHCPmode	Optional	String	The IPv4 DHCP mode. This can be one of the following values. • **STATIC_ONLY** • **DHCP_ONLY** • **DHCP_THEN_STATIC** • **UNKNOWN**
IPv4enabled	Optional	Boolean	Identifies whether IPv4 is enabled. This can be one of the following values. • **true**. IPv4 is enabled • **false**. IPv4 is disabled
IPv6DHCPenabled	Optional	Boolean	Identifies whether IPv6 DHCP is enabled. This can be one of the following values. • **true**. IPv6 DHCP is enabled • **false**. IPv6 DHCP is disabled
IPv6enabled	Optional	Boolean	Identifies whether IPv6 is enabled. This can be one of the following values. • **true**. IPv6 is enabled • **false**. IPv6 is disabled

Table 5. Modify storage-controller properties (continued)

Attributes	Re-quired / Optional	Type	Description
IPv6statelessEnabled	Optional	Boolean	Identifies whether IPv6 stateless is enabled. This can be one of the following values. • **true**. IPv6 stateless is enabled • **false**. IPv6 stateless is disabled
IPv6staticEnabled	Optional	Boolean	Identifies whether IPv6 static is enabled. This can be one of the following values. • **true**. IPv6 static is enabled • **false**. IPv6 static is disabled
IPv4assignments	Optional	Array	Information about IPv4 assignments **Note:** If specified, you must also specify the **id** attribute.
address	Optional	String	IPv4 address
gateway	Optional	String	IPv4 gateway
id	Required	Integer	IPv4 assignment ID
subnet	Optional	String	IPv4 subnet mask
IPv6assignments	Optional	Array	Information about IPv6 assignments **Note:** If specified, you must also specify the **id** attribute.
address	Optional	String	IPv6 address
gateway	Optional	String	IPv6 gateway
id	Required	Integer	IPv6 assignment ID
prefix	Optional	Integer	IPv6 prefix
name	Required	String	IP Interface name
location	Optional	Object	Information about the storage-controller location **Important:** Changes made to the location of the storage controller that is using this API method are not reflected in the rack view.
location	Optional	String	Location of the storage-controller
userDescription	Optional	String	Storage-controller description

The following example modifies the hostname, location, and contact information for the target storage controller:

```
{
    "contact": "new contact",
    "hostname":"",
    "location": {"location":"new location"}
}
```

Table 6. Modify the power state

Attributes	Required / Optional	Type	Description
powerState	Optional	String	Performs a power operation on the storage controller. This can be one of the following values. • **powerOn**. Power on the storage controller • **powerOff**. Power off the storage controller immediately • **powerCycleSoft**. Restart the storage controller immediately • **virtualReseat**. Calls the CMM function to simulate removing power from the bay.

The following example restarts the target storage controller:

```
{
    "powerState": "powerCycleSoft"
}
```

Table 7. Refresh the inventory

Attributes	Required / Optional	Type	Description
refreshInventory	Optional	String	Refreshes inventory for the storage controller

The following example refreshes inventory for the target storage controller.

```
{
   "refreshInventory": "true"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response body provides information about the success or failure of the request. The parameters in the response body differ depending on the specified request attributes.

Note: A response body is not returned for some requests.

The following example is returned when the **"refreshInventory": "true"** is specified in the request body to refresh the device inventory.

```
{
   "statusCode": 200,
   "statusDescription": "The request completed successfully.",
   "messages": [{
      "explanation": "refreshInventory request for target 6ED2CB368C594C66C2BB066D5A306138 has
                      completed successfully.",
      "id": "FQXDM0200",
      "recovery": "",
      "recoveryUrl": "",
      "text": "The request completed successfully."
   }]
}
```

/chassis

Use this REST API to retrieve properties for all Flex System chassis and chassis components.

HTTP methods

GET

GET /chassis

Use this method to return the properties for all Flex System chassis and chassis components.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/chassis`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
formatType=*{type}*	Optional	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv** If the format type is not specified, JSON format is returned. **Note:** To retrieve properties for a large number of devices, use POST /chassis.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.
status=*{string}*	Optional	Returns chassis inventory for all managed or unmanaged chassis. This can be one of the following values. If no value is specified, all managed and unmanaged devices are returned. • **managed**. Return information for only managed chassis. • **unmanaged**. Return information for only unmanaged chassis.

The following example returns a CSV file that contains information about all managed chassis.

```
GET https://192.0.2.0/chassis?status=managed&formatType=csv
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The attributes that are returned vary based on whether the chassis are managed or unmanaged.

Attributes	Type	Description
chassisList	Array	List of managed chassis
See GET /chassis/*{uuid_list}*	Object	Detailed information about the individual chassis

The following example is returned if the request is successful and the **formatType=json** query parameter is specified.


```
{
"chassisList": [{
    "accessState": "Online",
    "accountLockoutPeriod": 60,
    "activationKeys": [],
    "backedBy": "real",
    "complex": [{
        "complexID": "1E495E5E",
        "nodeCount": 1,
        "orphanNodes": [{
            "activationKeys": [],
            "addinCards": [],
            "addinCardSlots": 0,
            "accessState": "Online",
            "arch": "x86",
            "backedBy": "real",
            "bladeState": 1,
            "bladeState_health": "GOOD",
            "bladeState_string": "Newport213-14",
            "bmuParamObject": null,
            "bootMode": {
                    "currentValue": "UEFI Mode",
                    "possibleValues": ["UEFI Mode", "Legacy Mode"]
            },
            "bootOrder": {
                "bootOrderList": [{
                    "bootType": "SingleUse",
                    "currentBootOrderDevices": ["None"],
                    "possibleBootOrderDevices": ["None", "PXE Network", "Hard Disk 0", "Diagnostics",
                                                 "CD/DVD Rom", "Boot To F1", "Hypervisor", "Floppy Disk"]
                }, {
                    "bootType": "Permanent",
                    "currentBootOrderDevices": ["CD/DVD Rom", "Hard Disk 0", "PXE Network"],
                    "possibleBootOrderDevices": ["CD/DVD Rom", "Hard Disk 0", "PXE Network", "Floppy Disk",
                                                 "Hard Disk 1", "Hard Disk 2", "Hard Disk 3", "Hard Disk 4",
                                        "USB Storage", "Diagnostics", "iSCSI", "iSCSI Critical",
                                        "Embedded Hypervisor", "Legacy Only", "IMM1", "IMM2", "DSA",
                                        "USB0", "USB1", "USB2", "USB3", "USB4", "SAS", "NIC1", "NIC2",
                                        "NIC3", "NIC4", "VNIC1", "VNIC2", "VNIC3", "VNIC4", "VNIC5",
                                        "VNIC6", "VNIC7", "VNIC8", "VNIC9", "VNIC10", "VNIC11", "VNIC12",
```

```
                                    "Mezzanine1Device1", "Mezzanine1Device2", "Mezzanine1Device3",
                                    "Mezzanine1Device4", "Mezzanine1Device5", "Mezzanine1Device6",
                                    "Mezzanine2Device1", "Mezzanine2Device2", "Mezzanine2Device3",
                                    "Mezzanine2Device4", "Mezzanine2Device5", "Mezzanine2Device6",
                                    "Mezzanine3Device1", "Mezzanine3Device2", "Mezzanine4Device1",
                                    "Mezzanine4Device2"]
    }, {
        "bootType": "WakeOnLAN",
        "currentBootOrderDevices": ["PXE Network", "CD/DVD Rom", "Hard Disk 0"],
        "possibleBootOrderDevices": ["PXE Network", "CD/DVD Rom", "Hard Disk 0", "Floppy Disk",
                                    "Hard Disk 1", "Hard Disk 2", "Hard Disk 3", "Hard Disk 4",
                                    "USB Storage", "Diagnostics", "iSCSI", "iSCSI Critical",
                                    "Embedded Hypervisor", "Legacy Only", "IMM1", "IMM2", "DSA",
                                    "USB0", "USB1", "USB2", "USB3", "USB4", "SAS", "NIC1", "NIC2",
                                    "NIC3", "NIC4", "VNIC1", "VNIC2", "VNIC3", "VNIC4", "VNIC5",
                                    "VNIC6", "VNIC7", "VNIC8", "VNIC9", "VNIC10", "VNIC11", "VNIC12",
                                    "Mezzanine1Device1", "Mezzanine1Device2", "Mezzanine1Device3",
                                    "Mezzanine1Device4", "Mezzanine1Device5", "Mezzanine1Device6",
                                    "Mezzanine2Device1", "Mezzanine2Device2", "Mezzanine2Device3",
                                    "Mezzanine2Device4", "Mezzanine2Device5", "Mezzanine2Device6",
                                    "Mezzanine3Device1", "Mezzanine3Device2", "Mezzanine4Device1",
                                    "Mezzanine4Device2"]
    }],
    "uri": "nodes/F087DAB569F211E39C766CAE8B702C60/bootOrder"
},
"cmmDisplayName": "Node 13",
"cmmHealthState": "Normal",
"complexID": 508124766,
"contact": "test",
"dataHandle": 1701112556513,
"description": "Device data missing",
"dnsHostnames": ["192.0.12.253"],
"domainName": "",
"driveBays": 8,
"drives": [],
"embeddedHypervisorPresence": false,
"encapsulation": {
    "encapsulationMode": "notSupported"
},
"excludedHealthState": "Normal",
"errorFields": [{
    "ReleaseInfoData": "NO_CONNECTOR"
}, {
    "SingleSignOn": "NO_CONNECTOR"
}, {
        "MPFAHealthStatus": "NO_CONNECTOR"
}],
"expansionCards": [],
"expansionCardSlots": 4,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [{
    "deviceId": 0,
    "entityId": 0,
    "name": "front panel board 1",
    "posID": 0,
    "productId": 0,
    "vpdID": 0
}, {
    "deviceId": 0,
    "entityId": 0,
```

```
    "name": "system board 1",
    "posID": 0,
    "productId": 0,
    "vpdID": 0
}],
"firmware": [{
    "build": "1AOO87B",
    "classifications": [],
    "date": "2018-12-14T00:00:00Z",
    "name": "IMM2 Backup Firmware",
    "revision": "7.20",
    "role": "Backup",
    "status": "Inactive",
    "type": "IMM2-Backup",
    "version": "7.20"
},
...,
{
    "classifications": [],
    "build": "1AOO87B",
    "date": "2018-12-14T00:00:00Z",
    "name": "IMM2 Firmware",
    "revision": "7.20",
    "role": "Primary",
    "status": "Active",
    "type": "IMM2",
    "version": "7.20"
}],
"flashStorage": [],
"FRU": "47C2239",
"fruSerialNumber": "YC31BG3B503C"
"FQDN": "192.0.12.253",
"hasOS": false,
"hostMacAddresses": "6C:AE:8B:70:2C:60,6C:AE:8B:70:2C:64,6C:AE:8B:70:2C:68,6C:AE:8B:70:2C:6C",
"hostname": "IMM2-6cae8b6f0b11",
"inventoryState": "INVENTORY_READY",
"ipv4Addresses": ["192.0.12.253", "169.254.95.118"],
"ipInterfaces": [{
    "IPv4assignments": [{
            "id": 0,
            "address": "192.0.12.253",
            "gateway": "192.0.0.1",
            "subnet": "255.255.224.0",
            "type": "INUSE"
        }],
    "IPv4DHCPmode": "DHCP_ONLY",
    "IPv4enabled": true,
    "IPv6assignments": [{
            "id": 0,
            "address": "fe80:0:0:0:6eae:8bff:fe6f:b14",
            "gateway": "fe80:0:0:0:5:73ff:fea0:2c",
            "prefix": 64,
            "scope": "Unknown",
            "source": "Unknown",
            "type": "UNKNOWN"
        }, {
            "id": 0,
            "address": "fd55:faaf:e1ab:2021:6eae:8bff:fe6f:b14",
            "gateway": "fe80:0:0:0:5:73ff:fea0:2c",
            "prefix": 64,
            "scope": "Global",
```

```
                "source": "Stateless",
                "type": "INUSE"
            }],
        "IPv6DHCPenabled": true,
        "IPv6enabled": true,
        "IPv6statelessEnabled": true,
        "IPv6staticEnabled": false,
        "label": "unknown",
        "name": "eth0"
    }, {
        "IPv4assignments": [],
        "IPv4DHCPmode": "STATIC_ONLY",
        "IPv4enabled": true,
        "IPv6assignments": [{
                "id": 0,
                "address": "fe80:0:0:0:6eae:8bff:fe6f:b14",
                "gateway": "fe80:0:0:0:5:73ff:fea0:2c",
                "prefix": 64,
                "scope": "Unknown",
                "source": "Unknown",
                "type": "UNKNOWN"
            }, {
                "id": 0,
                "address": "fd55:faaf:e1ab:2021:6eae:8bff:fe6f:b14",
                "gateway": "fe80:0:0:0:5:73ff:fea0:2c",
                "prefix": 64,
                "scope": "Global",
                "source": "Stateless",
                "type": "CONFIGURED"
            }],
        "IPv6DHCPenabled": true,
        "IPv6enabled": true,
        "IPv6statelessEnabled": false,
        "IPv6staticEnabled": false,
        "label": "unknown",
        "name": "ethernet-over-usb"
    }],
    "ipv6Addresses": ["fd55:faaf:e1ab:2021:6eae:8bff:fe6f:b14", "fe80:0:0:0:6eae:8bff:fe6f:b14"],
    "isConnectionTrusted": "true",
    "isITME": false,
    "isRemotePresenceEnabled": true,
    "lanOverUsb": "enabled",
    "leds": [{
        "color": "Yellow",
        "location": "Planar",
        "name": "DIMM 48",
        "state": "Off"
    },
    ...,
    {
        "color": "Yellow",
        "name": "DIMM 10",
        "location": "Planar",
        "state": "Off"
    }],
    "isScalable": true,
    "lanOverUsbPortForwardingModes": [{
        "externalIPAddress": "",
        "state": "disabled",
        "type": "DSA"
    }],
```

```
"location": {
    "rack": "",
    "location": "test",
    "lowestRackUnit": 0,
    "room": ""
},
"machineType": "7903",
"logicalID": 0,
"m2Presence": false,
"macAddress": "6C:AE:8B:6F:0B:14,6C:AE:8B:6F:0B:16",
"manufacturer": "CITRIX_BLADE",
"manufacturerId": "20301",
"memoryModules": [{
    "capacity": 4,
    "displayName": "DIMM 1",
    "fruPartNumber": "",
    "healthState": "NA",
    "manufacturer": "Samsung",
    "model": "DDR3",
    "operatingMemoryMode": null,
    "partNumber": "M393B5270QB0-YK0",
    "present": false,
    "serialNumber": "01976141",
    "slot": 1,
    "speed": 1600,
    "speedMBs": 0,
    "type": "DDR3"
}],
"memorySlots": 48,
"mgmtProcIPaddress": "192.0.12.253",
"mgmtProcType": "IMM2",
"model": "AC1",
"name": "Newport213-14",
"nist": {
    "currentValue": "Unknown",
    "possibleValues": ["Nist_800_131A_Strict", "unsupported", "Compatibility"]
},
"onboardPciDevices": [{
    "class": "Display controller",
    "firmware": [],
    "fodUniqueID": "",
    "isAddOnCard": false,
    "isAgentless": false,
    "isPLDMUpdateSupported": false,
    "name": "",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "0",
    "pciBusNumber": "9",
    "pciRevision": "0",
    "pciSubID": "0",
    "pciSubVendorID": "0",
    "portInfo": {},
    "posID": "534",
    "vpdID": "102b"
}, {
    "class": "Network controller",
    "firmware": [{
        "build": "0",
        "classifications": [13],
        "date": "",
        "name": "OneConnect 10G/40G Flash Image",
```

```
            "revision": "0",
            "role": "Primary",
            "softwareID": "10DFE812",
            "status": "Active",
            "type": "Software Bundle",
            "version": "192.0.2.26"
        }],
        "fodUniqueID": "N/A",
        "isAddOnCard": false,
        "isAgentless": true,
        "isPLDMUpdateSupported": false,
        "name": "N/A",
        "pciBusNumber": "139",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "2",
        "pciRevision": "10",
        "pciSubID": "e812",
        "pciSubVendorID": "10df",
        "portInfo": {
                    "physicalPorts": [{
                        "logicalPorts": [{
                            "addresses": "6CAE8B702C68",
                            "logicalPortIndex": 1,
                            "portNumber": 1,
                            "portType": "ETHERNET",
                            "vnicMode": false
                        }],
                        "physicalPortIndex": 3,
                        "peerBay": 0,
                        "portNumber": 3,
                        "portType": "ETHERNET",
                        "speed": 0.0,
                        "status": null
                    }]
                },
        "posID": "720",
        "vpdID": "10df"
    }],
    "overallHealthState": "Normal",
    "osInfo": {
                "description": "",
                "hostname": "",
                "storedCredential": ""
            },
    "parent": {
        "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
        "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
    },
    "parentComplexID": "1E495E5E",
    "partitionID": -1,
    "partNumber": "00AN678",
    "pciCapabilities": ["Raid Link", "OOB PCIe"],
    "pciDevices": [{
        "class": "Display controller",
        "firmware": [],
        "fodUniqueID": "",
        "isAddOnCard": false,
        "isAgentless": false,
        "isPLDMUpdateSupported": false,
        "pciDeviceNumber": "0",
        "name": "",
```

```
    "pciBusNumber": "9",
    "pciFunctionNumber": "0",
    "pciRevision": "0",
    "pciSubID": "0",
    "pciSubVendorID": "0",
    "portInfo": {},
    "posID": "534",
    "vpdID": "102b",
},
...,
{
    "class": "Network controller",
    "firmware": [{
        "build": "0",
        "classifications": [13],
        "date": "",
        "name": "OneConnect 10G/40G Flash Image",
        "revision": "0",
        "role": "Primary",
        "softwareID": "10DFE812",
        "status": "Active",
        "type": "Software Bundle",
        "version": "192.0.2.26"
    }],
    "fodUniqueID": "N/A",
    "isAddOnCard": false,
    "isAgentless": true,
    "isPLDMUpdateSupported": false,
    "name": "N/A",
    "pciBusNumber": "139",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "2",
    "pciRevision": "10",
    "pciSubID": "e812",
    "pciSubVendorID": "10df",
    "portInfo": {
        "physicalPorts": [{
            "logicalPorts": [{
                "addresses": "6CAE8B702C68",
                "logicalPortIndex": 1,
                "portNumber": 1,
                "portType": "ETHERNET",
                "vnicMode": false
            }],
            "peerBay": 0,
            "physicalPortIndex": 3,
            "portNumber": 3,
            "portType": "ETHERNET",
            "speed": 0.0,
            "status": null
        }]
    },
    "posID": "720",
    "vpdID": "10df",
}],
"ports": [{
    "ioModuleBay": 1,
    "portNumber": 1
}, {
    "ioModuleBay": 2,
    "portNumber": 2
```

```
}, {
    "ioModuleBay": 0,
    "portNumber": 3
}, {
    "ioModuleBay": 0,
"portNumber": 4
}],
"posID": "30",
"powerAllocation": {
    "maximumAllocatedPower": 299,
    "minimumAllocatedPower": 211
},
"powerStatus": 5,
"powerSupplies": [],
"primary": false,
"processorIntelSpeedSelect": {
    "currentValue": "",
    "possibleValues": []
},
"processors": [{
    "cores": 12,
    "displayName": "Intel(R) Xeon(R) CPU E7-8850 v2 @ 2.30GHz",
    "family": "PENTIUM_R_4",
    "healthState": "NA",
    "manufacturer": "Intel(R) Corporation",
    "maxSpeedMHZ": 2300,
    "partNumber": "Unknown",
    "present": false,
    "productVersion": "Intel(R) Xeon(R) CPU E7-8850 v2 @ 2.30GHz",
    "serialNumber": "Unknown",
    "slot": 1,
    "speed": 2.3,
    "socket": "",
    "tdpWatts": -1,
}],
"processorSlots": 2,
"productId": "448",
"productName": "",
"raidSettings": [],
"secureBootMode": {
    "currentValue": "Disabled",
    "possibleValues": ["Enabled", "Disabled"]
},
"securityDescriptor": {
    "identityManagementSystemEnabled": false,
    "managedAuthEnabled": true,
    "managedAuthSupported": true,
    "publicAccess": false,
    "roleGroups": ["lxc-supervisor", "lxc-recovery"],
    "storedCredentials": {
        "id": "1752",
        "description": "Credentials for lamMM1",
        "userName": "userid"
    },
    "uri": "nodes/f087dab569f211e39c766cae8b702c60",
},
"serialNumber": "23YVLH4",
"slots": [13, 14],
"ssoEnabled": false,
"status": {
    "message": "managed",
```

```
            "name": "MANAGED"
        },
        "subType": "Nantahala",
        "subSlots": [],
        "tlsVersion": {
            "currentValue": "Unknown",
            "possibleValues": ["unsupported", "TLS_12", "TLS_11", "TLS_10"]
        },
        "type": "ITE",
        "uri": "nodes/F087DAB569F211E39C766CAE8B702C60",
        "userDefinedName": "Newport213-14",
        "userDescription": "",
        "uuid": "F087DAB569F211E39C766CAE8B702C60",
        "vnicMode": "disabled",
        "vpdID": "256",
    }],
    "partition": [],
    "partitionCount": 0,
    "slots": [13, 14],
    "uuid": "F087DAB569F211E39C766CAE8B702C60"
}],
"cmmDisplayName": "IamMM1",
"cmmHealthState": "Critical",
"cmms": [...],
"bladeSlots": 14,
"contact": "No Contact Configured",
"dataHandle": 1701192297537,
"description": "Lenovo Flex System Chassis",
"displayName": "IamMM1",
"domainName": "",
"encapsulation": {
    "encapsulationMode": "normal"
},
"energyPolicies": {
    "acousticAttenuationMode": "Off",
    "hotAirRecirculation": {
        "chassisBay": [{
            "isExceeded": "N",
            "sensorName": "Inlet 1 Temp",
            "sensorValue": 20.0,
            "slot": 13,
            "subSlot": -1
        },
        ...,
        {
            "isExceeded": "N",
            "sensorName": "Inlet Temp",
            "sensorValue": 22.0,
            "slot": 10,
            "subSlot": 1
        }],
        "isEnabled": true,
        "maxVariation": 5.0
    },
    "powerCappingPolicy": {
        "cappingACorDCMode": null,
        "cappingPolicy": "OFF",
        "currentPowerCap": 0,
        "maximumPowerCappingHotPlugLevel": null,
        "maxPowerCap": 12525,
        "minimumHardCapLevel": null,
```

```
            "minimumPowerCappingHotPlugLevel": null,
            "minPowerCap": 3049,
            "powerCappingAllocUnit": "watts"
        },
        "powerRedundancyMode": 3
    },
    "errorFields": [],
    "excludedHealthState": "Critical",
    "fans": [{
        "parent": {
            "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
            "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
        },
        "FRU": "81Y2911",
        "description": "Fan Module",
        "excludedHealthState": "Normal",
        "type": "Fan",
        "uuid": "586E241977E541DD884D3289F72BBDE6",
        "productName": "",
        "manufacturer": "IBM",
        "powerState": "Unknown",
        "overallHealthState": "Normal",
        "powerAllocation": {
            "maximumAllocatedPower": 60,
            "minimumAllocatedPower": 60
        },
        "manufactureDate": "3111",
        "model": "",
        "errorFields": [],
        "firmware": [{
            "build": "",
            "classifications": [],
            "date": "",
            "name": "Fan Controller",
            "revision": "226",
            "role": "",
            "status": "",
            "type": "Fan Controller",
            "version": "226",
        }],
        "machineType": "",
        "serialNumber": "",
        "userDescription": "",
        "productId": "339",
        "manufacturerId": "20301",
        "cmmDisplayName": "Fan 05",
        "uri": "fan/586E241977E541DD884D3289F72BBDE6",
        "cmmHealthState": "Normal",
        "posID": "8",
        "slots": [5],
        "hardwareRevision": "4.0",
        "vpdID": "373",
        "dataHandle": 0,
        "name": "Fan 05",
        "leds": [{
            "color": "Amber",
            "location": "FrontPanel",
            "name": "FAULT",
            "state": "Off"
        }],
        "partNumber": "88Y6670",
```

```
    "fruSerialNumber": "YK10GM17S067"
}],
"fanSlots": 10,
"fanMuxes": [{
    "cmmHealthState": "Non-Critical",
    "cmmDisplayName": "Fan Logic 02",
    "dataHandle": 0,
    "description": "Fan Logic Module",
    "excludedHealthState": "Warning",
    "FRU": "81Y2912",
    "fruSerialNumber": "Y031BG16P017",
    "leds": [{
        "color": "Amber",
        "location": "FrontPanel",
        "name": "FAULT",
        "state": "On"
    }],
    "machineType": "",
    "hardwareRevision": "4.0",
    "manufactureDate": "2611",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Fan Logic 02",
    "overallHealthState": "Warning",
    "parent": {
        "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91".
        "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
    },
    "partNumber": "81Y2990",
    "productId": "338",
    "productName": "IBM Fan Pack Multiplexor Card",
    "serialNumber": "",
    "slots": [2],
    "status": "Non-Critical",
    "type": "FanMux",
    "uri": "fanMux/54D1E375A19F11E0ADA7D9E63ABF920B",
    "uuid": "54D1E375A19F11E0ADA7D9E63ABF920B"
}],
"fanMuxSlots": 2,
"FQDN": "",
"height": 10,
"hostname": "MM40F2E9BF07C4",
"isConnectionTrusted": "true",
"lastOfflineTimestamp": -1,
"ledCardSlots": 1,
"leds": [{
    "color": "Blue",
    "location": "FrontPanel",
    "name": "Location",
    "state": "Off"
}, {
    "color": "Amber",
    "location": "FrontPanel",
    "name": "Information",
    "state": "On"
}, {
    "color": "Amber",
    "location": "FrontPanel",
    "name": "FAULT",
    "state": "Off"
```

```
}],
"location": {
    "location": "No Location Configured",
    "lowestRackUnit": 0,
    "rack": "",
    "room": ""
},
"machineType": "8721",
"managedChassis": true,
"managerName": "UNKNOWN",
"managerUuid": "UNKNOWN",
"manufacturer": "IBM",
"manufacturerId": "20301",
"mgmtProcIPaddress": "192.0.3.55",
"mmSlots": 2,
"model": "HC1",
"name": "IamMM1",
"nist": {
    "currentValue": "Compatibility",
    "possibleValues": ["Nist_800_131A_Strict", "unsupported", "Nist_800_131A_Custom", "Compatibility"]
},
"nodes": [...],
"overallHealthState": "Critical",
"parent": {
    "uri": "cabinet/",
    "uuid": ""
},
"partNumber": "88Y6660",
"passThroughModules": [],
"posID": "14",
"powerAllocation": {
    "allocatedOutputPower": 3049,
    "midPlaneCardMaximumAllocatedPower": 38,
    "midPlaneCardMinimumAllocatedPower": 38,
    "remainingOutputPower": 9476,
    "totalInputPower": 13614,
    "totalOutputPower": 12525
},
"powerSupplies": [{
    "cmmDisplayName": "Power Supply 04",
    "cmmHealthState": "Non-Critical",
    "dataHandle": 0,
    "description": "Power Supply",
    "excludedHealthState": "Warning",
    "firmware": [{
        "build": "",
        "classifications": [],
        "date": "",
        "name": "Power Supply Firmware",
        "revision": "6",
        "role": "",
        "softwareID": "",
        "status": "",
        "type": "Power Supply Firmware",
        "version": "6"
    }],
    "FRU": "69Y5806",
    "fruSerialNumber": "ZK128117L00F",
    "hardwareRevision": "76.54",
    "healthState": "NA",
    "inputVoltageIsAC": true,
```

```
    "inputVoltageMax": -1,
    "inputVoltageMin": -1,
    "leds": [{
        "color": "Green",
        "location": "Planar",
        "name": "OUT",
        "state": "Off"
    },
    ...,
    {
        "color": "Green",
        "location": "Planar",
        "name": "IN",
        "state": "Off"
    }],
    "machineType": "",
    "manufactureDate": "2911",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Power Supply 04",
    "overallHealthState": "Warning",
    "parent": {
        "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
        "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
    },
    "partNumber": "69Y5802",
    "posID": "61",
    "powerAllocation": {
        "totalInputPower": 0,
        "totalOutputPower": 0
    },
    "powerState": "Unknown",
    "productId": "304",
    "productName": "IBM 2500 W Power Supply",
    "serialNumber": "",
    "type": "PowerSupply",
    "userDescription": "",
    "uuid": "388FA5B048634E47990B20EE420FA6BD",
    "uri": "powerSupply/388FA5B048634E47990B20EE420FA6BD",
    "slots": [4],
    "vpdID": "128",
}],
"powerSupplySlots": 6,
"productId": "336",
"productName": "IBM Chassis Midplane",
"securityDescriptor": {
    "identityManagementSystemEnabled": false,
    "managedAuthEnabled": true,
    "managedAuthSupported": true,
    "publicAccess": false,
    "storedCredentials": {
        "id": "1752",
        "description": "Credentials for IamMM1",
        "userName": "userid"
    },
    "roleGroups": ["lxc-supervisor", "lxc-recovery"],
    "uri": "chassis/3d1d5931bdf84d30ada976e21f08cb91",
},
"SecurityPolicy": {
    "cmmPolicyLevel": "SECURE",
```

```
        "cmmPolicyState": "ACTIVE"
    },
    "serialNumber": "23PYP15",
    "status": {
        "message": "MANAGED",
        "name": "MANAGED"
    },
    "switches": [...],
    "switchSlots": 4,
    "tlsVersion": {
        "currentValue": "TLS_12_Server",
        "possibleValues": ["TLS_12_Server", "unsupported", "TLS_12_Server_Client", "SSL_30"]
    },
    "type": "Chassis",
    "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
    "userDefinedName": "IamMM1",
    "userDescription": "",
    "uuid": "3D1D5931BDF84D30ADA976E21F08CB91",
    "vpdID": "336"
}]
}
```


POST /chassis

Use this method to return the properties for a large number of specific Flex System chassis and chassis resources.

Note: If you choose **formatType=csv**, this request creates a file in CSV format and returns the filename in the request header. You can use to download the file using GET /chassis/*{file_name}*.csv.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/chassis`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
formatType	Optional	String	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv**
uuids	Required	String	List of device UUIDs, separated by a comma

The following example returns the properties for a two specific Flex System devices.

```
{
   "formatType": "csv",
   "uuids": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

If **formatType=csv** is specified, the response header includes the URI of the downloaded file. If data for a single chassis is requested, the file name includes the chassis UUID. If multiple chassis are requested, the file name is `allChassis_`*{unique_ID}*`.csv`. For example:

```
Status Code: 201 Created
Location: /chassis/EF6D424FAACA4E539771B812AAEE0F73.csv
```

Response body

If the **formatType=csv** request attribute is specified, no response body is returned.

If the **formatType=json** request attribute is specified, the following JSON object is returned. The attributes that are returned vary based on whether the chassis are managed or unmanaged.

Attributes	Type	Description
chassisList	Array	List of managed chassis
See GET /chassis/*{uuid_list}*	Object	Detailed information about the individual chassis

The following example is returned if the request is successful and the **formatType=json** request attribute is specified.


```
{
   "chassisList": [{
      "accessState": "Online",
      "activationKeys": [],
      "backedBy": "real",
      "bladeSlots": 14,
      "cmmDisplayName": "Chassis126",
      "cmmHealthState": "Critical",
      "cmms": [{
         "accessState": "Online",
         "backedBy": "real",
         "description": "CMM",
         "cmmDisplayName": "SN#Y034BG16F03V",
         "cmmHealthState": "Non-Critical",
         "dataHandle": 1508187250973,
         "errorFields": [],
         "domainName": "",
         "dnsHostnames": ["Chassis126.labs.lenovo.com", "fd55:faaf:e1ab:20fc:5ef3:fcff:fe25:dc6d"],
```

```
"excludedHealthState": "Warning",
"hostConfig": [{
   "DDNSenabled": false,
   "DNSenabled": false,
   "IPversionPriority": "IPv6ThenIPv4",
   "priIPv4userDNSserver": "10.240.0.10",
   "priIPv6userDNSserver": "0:0:0:0:0:0:0:0",
   "secIPv4userDNSserver": "10.240.0.11",
   "secIPv6userDNSserver": "0:0:0:0:0:0:0:0",
   "terIPv4userDNSserver": "0.0.0.0",
   "terIPv6userDNSserver": "0:0:0:0:0:0:0:0"
}],
"hostname": "MM5CF3FC25DC6D",
"ipInterfaces": [{
   "IPv4assignments": [{
      "address": "10.240.75.191",
      "gateway": "10.240.72.1",
      "id": 2,
      "subnet": "255.255.252.0",
      "type": "INUSE"
   }],
   "IPv4DHCPmode": "STATIC_ONLY",
   "IPv4enabled": true,
   "IPv6assignments": [{
      "address": "fe80:0:0:0:5ef3:fcff:fe25:dc6d",
      "gateway": "0:0:0:0:0:0:0:0",
      "id": 1,
      "prefix": 64,
      "scope": "LinkLocal",
      "source": "Other",
      "type": "INUSE"
   }],
   "IPv6DHCPenabled": true,
   "IPv6enabled": true,
   "IPv6statelessEnabled": true,
   "IPv6staticEnabled": true,
   "label": "External",
   "name": "eth0"
}],
"ipv4Addresses": ["10.240.75.191"],
"ipv6Addresses": ["fe80:0:0:0:5ef3:fcff:fe25:dc6d", ..., fd55:faaf:e1ab:20fc:5ef3:fcff:fe25:dc6d"],
"firmware": [{
   "build": "2PET39C",
   "date": "2017-09-13T04:00:00Z",
   "status": "",
   "name": "CMM firmware",
   "role": "",
   "type": "CMM firmware",
   "version": "2.5.10"
}],
"FRU": "68Y7032",
"fruSerialNumber": "Y034BG16F03V"
"leds": [{
   "color": "Amber",
   "location": "FrontPanel",
   "name": "FAULT",
   "state": "Off"
}],
"macAddresses": ["5C:F3:FC:25:DC:6D"],
"machineType": "",
"manufacturer": "IBM",
```

```
    "manufacturerId": "20301",
    "mgmtProcIPaddress": "10.240.75.191",
    "model": "",
    "name": "SN#Y034BG16F03V",
    "overallHealthState": "Warning",
    "parent": {
       "uri": "chassis/E053C9508C244F549011B2518DB71236",
       "uuid": "E053C9508C244F549011B2518DB71236"
    },
    "partNumber": "68Y7029",
    "powerAllocation": {
       "maximumAllocatedPower": 20,
       "minimumAllocatedPower": 20
    },
    "productId": "65",
    "role": "primary",
    "serialNumber": "",
    "slots": [1],
    "type": "CMM",
    "uri": "cmm/4BAF3700D9DE211E0B25CF29BFB9E7E8B",
    "userDefinedName": "CMM1"
    "userDescription": "",
    "uuid": "4BAF3700D9DE211E0B25CF29BFB9E7E8B"
}],
"complex": [],
"contact": "http://liss-bugzilla.labs.lenovo.com",
"dataHandle": 1508188241539,
"description": "IBM Flex System Chassis",
"displayName": "Chassis126",
"domainName": "",
"encapsulation": {
   "encapsulationMode": "notSupported"
},
"energyPolicies": {
   "acousticAttenuationMode": "Off",
   "hotAirRecirculation": {
      "chassisBay": [{
         "isExceeded": "N",
         "sensorName": "Chassis Ambient",
         "sensorValue": 24.0,
         "slot": 0,
         "subSlot": -1
      },
      ...,
      {
         "isExceeded": "N",
         "sensorName": "Inlet Temp",
         "sensorValue": 22.5,
         "slot": 8,
         "subSlot": -1
      }],
      "maxVariation": 5.0,
      "isEnabled": true,
   },
   "powerCappingPolicy": {
      "cappingPolicy": "OFF",
      "currentPowerCap": 0,
      "maxPowerCap": 15030,
      "minPowerCap": 3780
   },
   "powerRedundancyMode": 3
```

```
},
"errorFields": [],
"excludedHealthState": "Critical",
"fanMuxes": [{
   "cmmDisplayName": "Fan Logic 01",
   "cmmHealthState": "Normal",
   "dataHandle": 0,
   "description": "fan logic card",
   "FRU": "94Y5805",
   "fruSerialNumber": "Y011BG35M01T",
   "hardwareRevision": "6.1",
   "leds": [{
      "color": "Amber",
      "location": "FrontPanel",
      "name": "FAULT",
      "state": "Off"
   }],
   "machineType": "",
   "manufactureDate": "2113",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "model": "",
   "name": "Fan Logic 01",
   "parent": {
      "uri": "chassis/E053C9508C244F549011B2518DB71236",
      "uuid": "E053C9508C244F549011B2518DB71236"
   },
   "partNumber": "49Y3276",
   "productId": "338",
   "productName": "IBM Flex System Enterprise Chassis Fan Logic Card",
   "serialNumber": "",
   "status": "Normal",
   "slots": [1],
   "type": "FanMux",
   "uri": "fanMux/E5160099C27611E2A256AAA4CEBCC5D7",
   "uuid": "E5160099C27611E2A256AAA4CEBCC5D7"
}],
"fanMuxSlots": 2,
"fans": [{
   "cmmDisplayName": "Fan 01",
   "dataHandle": 0,
   "cmmHealthState": "Normal",
   "description": "IBM Fan Pack",
   "errorFields": [],
   "firmware": [{
      "build": "",
      "date": "",
      "name": "Fan Controller",
      "role": "",
      "status": "",
      "type": "Fan Controller",
      "version": "226"
   }],
   "FRU": "88Y6685",
   "fruSerialNumber": "YK10JPB69L24",
   "hardwareRevision": "4.0",
   "leds": [{
      "color": "Amber",
      "location": "FrontPanel",
      "name": "FAULT",
      "state": "Off"
```

```
    }],
    "machineType": "",
    "manufactureDate": "2611",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Fan 01",
    "parent": {
       "uuid": "E053C9508C244F549011B2518DB71236",
       "uri": "chassis/E053C9508C244F549011B2518DB71236"
    },
    "partNumber": "88Y6691",
    "productId": "342",
    "productName": "80mm Fan Pack for ITE Cooling",
    "posID": "11",
    "powerAllocation": {
       "maximumAllocatedPower": 75,
       "minimumAllocatedPower": 75
    },
    "powerState": "Unknown",
    "serialNumber": "",
    "slots": [1],
    "type": "Fan",
    "uri": "fan/C74F88A19DB311E0AB5AF1DE32F87750",
    "userDescription": "",
    "uuid": "C74F88A19DB311E0AB5AF1DE32F87750",
    "vpdID": "373"
}],
"fanSlots": 10,
"FQDN": null,
"height": 10,
"hostname": "MM5CF3FC25DC6D",
"isConnectionTrusted": "true",
"ledCardSlots": 1,
"leds": [{
    "color": "Blue",
    "location": "FrontPanel",
    "name": "Location",
    "state": "Off"
},
...,
{
    "color": "Amber",
    "location": "FrontPanel",
    "name": "Information",
    "state": "On"
}],
"location": {
    "lowestRackUnit": 1,
    "location": "R1",
    "rack": "C12",
    "room": "8-1W-4"
},
"machineType": "7893",
"managerName": "UNKNOWN",
"managerUuid": "UNKNOWN",
"manufacturer": "IBM",
"manufacturerId": "20301",
"mgmtProcIPaddress": "10.240.75.191",
"mmSlots": 2,
"model": "92X",
```

```
"name": "Chassis126",
"nist": {
   "currentValue": "Compatibility",
   "possibleValues": ["Compatibility", ... "unsupported"]
},
"nodes": [{
   "accessState": "Online",
   "activationKeys": [],
   "addinCards": [],
   "addinCardSlots": 0,
   "arch": "x86",
   "backedBy": "real",
   "bladeState": 1,
   "bladeState_health": "WARNING",
   "bladeState_string": "ite-bt-890",
   "bootMode": {
      "currentValue": "UEFI Only",
      "possibleValues": ["UEFI and Legacy", "UEFI Only", "Legacy Only"],
   },
   "bootOrder": {
      "bootOrderList": [{
         "bootType": "SingleUse",
         "currentBootOrderDevices": ["None"],
         "possibleBootOrderDevices": ["None", ... "Floppy Disk"]
      }],
      "uri": "node/B9A8192D427011E18F04F5F1A3C864E0/bootOrder"
   },
   "cmmDisplayName": "Node 01",
   "cmmHealthState": "Non-Critical",
   "complexID": -1,
   "contact": "Fred",
   "dataHandle": 1508188861461,
   "description": "IBM Flex System x240 with 10Gb",
   "driveBays": 8,
   "domainName": "labs.lenovo.com",
   "dnsHostnames": ["ite-bt-890-imm1.labs.lenovo.com", "fd55:faaf:e1ab:20fc:5ef3:fcff:fe6e:12fd"]
   "drives": [{
      "bay": 1,
      "capacity": -1
   },
   {
      "bay": 2,
      "capacity": -1
   }],
   "embeddedHypervisorPresence": false,
   "encapsulation": {
      "encapsulationMode": "notSupported"
   },
   "errorFields": [{
      "IOCompatibilityData": "FETCH_FAILED"
   }],
   "excludedHealthState": "Minor-Failure",
   "expansionCards": [{
      "bay": 2,
      "firmware": [{
         "revision": "0",
         "classifications": [13],
         "status": "Active",
         "name": "ISP 26xx Multiboot",
         "role": "Primary",
         "softwareID": "10770240",
```

```
      "type": "Software Bundle",
      "build": "0",
      "date": "2017-01-27T00:00:00Z",
      "version": "4.75.04"
   }],
   "FRU": "69Y1945",
   "fruSerialNumber": "Y251NY3A2GTG",
   "isAgentless": true,
   "manufacturer": "IBM",
   "name": "IBM Flex System FC5172 2-port 16Gb FC Adapter",
   "partNumber": "69Y1944",
   "pciBusNumber": "22",
   "pciDeviceNumber": "0",
   "pciFunctionNumber": "0",
   "pciRevision": "2",
   "pciSubID": "240",
   "pciSubVendorID": "1077",
   "productName": "IBM Flex System FC5172 2-port 16Gb FC Adapter",
   "posID": "2031",
   "slotName": "SlotDesig2_Mezzanine 2 Card",
   "slotNumber": "2",
   "slotSupportsHotPlug": "false",
   "vpdID": "1077",
   "uuid": "C940FAA12B4A11E3AED4EFD2C9E10682"
}],
"expansionCardSlots": 2,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [{
   "entityId": 0,
   "deviceId": 0,
   "posID": 0,
   "productId": 0,
   "name": "system board 1",
   "vpdID": 0
},
...
{
   "deviceId": 0,
   "entityId": 0,
   "posID": 0,
   "productId": 0,
   "name": "drive backplane 1",
   "vpdID": 0
}],
"firmware": [{
   "date": "2017-03-27T00:00:00Z",
   "build": "B2E155CUS",
   "name": "UEFI Firmware/BIOS",
   "role": "Primary",
   "status": "Active",
   "type": "UEFI",
   "version": "2.00"
},
...,
{
   "build": "1AOO75I",
   "date": "2016-11-02T00:00:00Z",
   "name": "IMM2 Backup Firmware",
   "role": "Backup",
   "status": "Inactive",
```

```
      "type": "IMM2-Backup",
      "version": "6.00"
   }],
   "flashStorage": [],
   "FQDN": "ite-bt-890-imm1.labs.lenovo.com",
   "FRU": "81Y5128",
   "fruSerialNumber": "Y032BG1C2007",
   "hasOS": false,
   "hostMacAddresses": "5C:F3:FC:6E:44:B8,5C:F3:FC:6E:44:BC",
   "hostname": "IMM2-5cf3fc6e12fd",
   "ipInterfaces": [{
      "IPv4assignments": [{
         "address": "10.240.75.197",
         "gateway": "0.0.0.0",
         "id": 0,
         "subnet": "255.255.252.0",
         "type": "INUSE"
      }],
      "IPv4DHCPmode": "STATIC_ONLY",
      "IPv4enabled": true,
      "IPv6assignments": [{
         "address": "fd55:faaf:e1ab:20fc:5ef3:fcff:fe6e:12fd",
         "gateway": "0:0:0:0:0:0:0:0",
         "id": 0,
         "prefix": 64,
         "scope": "Global",
         "source": "Static",
         "type": "INUSE"
      }],
      "IPv6DHCPenabled": true,
      "IPv6enabled": true,
      "IPv6statelessEnabled": true,
      "IPv6staticEnabled": true,
      "label": "unknown",
      "name": "eth0"
   }],
   "ipv4Addresses": ["10.240.75.197", "169.254.95.118"],
   "ipv6Addresses": ["fd55:faaf:e1ab:20fc:5ef3:fcff:fe6e:12fd", "fe80:0:0:0:5ef3:fcff:fe6e:12fd"],
   "isRemotePresenceEnabled": true,
   "isScalable": false,
   "isITME": false,
   "isConnectionTrusted": "true",
   "lanOverUsb": "enabled",
   "lanOverUsbPortForwardingModes": [{
      "externalIPAddress": "",
      "state": "disabled",
      "type": "DSA"
   }],
   "leds": [{
      "color": "Yellow",
      "location": "FrontPanel",
      "name": "Fault",
      "state": "Off"
   },
   ...,
   {
      "color": "Yellow",
      "location": "Planar",
      "name": "DIMM 24",
      "state": "Off"
   }],
```

```
"location": {
   "location": "R1",
   "lowestRackUnit": 1,
   "rack": "C12",
   "room": "8-1W-4"
},
"m2Presence": false,
"macAddress": "5C:F3:FC:6E:12:FD,5C:F3:FC:6E:12:FE",
"machineType": "8737",
"manufacturer": "IBM",
"manufacturerId": "20301",
"memoryModules": [{
   "capacity": 8,
   "displayName": "DIMM 1",
   "manufacturer": "Samsung",
   "model": "DDR3",
   "partNumber": "M393B1K70CH0-YH9",
   "serialNumber": "8269E8EC",
   "speed": 1333,
   "speedMBs": 0,
   "slot": 1,
   "type": "DDR3"
}],
"memorySlots": 24,
"mgmtProcIPaddress": "10.240.75.197",
"mgmtProcType": "IMM2",
"model": "AC1",
"name": "ite-bt-890",
"nist": {
   "currentValue": "Unknown",
   "possibleValues": ["Compatibility", "Nist_800_131A_Strict", "unsupported"]
},
"onboardPciDevices": [{
   "class": "Display controller",
   "isAgentless": false,
   "isAddOnCard": false,
   "fodUniqueID": "",
   "name": "",
   "pciBusNumber": "4",
   "pciDeviceNumber": "0",
   "pciFunctionNumber": "0",
   "pciRevision": "0",
   "pciSubID": "405",
   "pciSubVendorID": "1014",
   "portInfo": {},
   "posID": "534",
   "vpdID": "102b"
}],
"overallHealthState": "Minor-Failure",
"parent": {
   "uuid": "E053C9508C244F549011B2518DB71236",
   "uri": "chassis/E053C9508C244F549011B2518DB71236"
},
"partNumber": "95Y4635",
"partitionID": -1,
"pciCapabilities": ["Raid Link", "OOB PCIe"],
"pciDevices": [{
   "class": "Display controller",
   "fodUniqueID": "",
   "isAddOnCard": false,
   "isAgentless": false,
```

```
      "name": "",
      "pciBusNumber": "4",
      "pciDeviceNumber": "0",
      "pciFunctionNumber": "0",
      "pciRevision": "0",
      "pciSubVendorID": "1014",
      "pciSubID": "405",
      "portInfo": {},
      "posID": "534",
      "vpdID": "102b"
   }],
   "ports": [{
      "ioModuleBay": 0,
      "portNumber": 1
   },
   ...,
   {
      "ioModuleBay": 0,
      "portNumber": 10
   }],
   "posID": "20",
   "powerAllocation": {
      "maximumAllocatedPower": 118,
      "minimumAllocatedPower": 75
   },
   "powerStatus": 5,
   "powerSupplies": [],
   "productName": "IBM Flex System x240 Compute Node with embedded 10Gb Virtual Fabric",
   "processors": [{
      "cores": 6,
      "displayName": "Genuine Intel(R) CPU  @ 2.00GHz",
      "family": "INTEL_R_XEON_TM",
      "manufacturer": "Intel(R) Corporation",
      "productVersion": "Genuine Intel(R) CPU  @ 2.00GHz",
      "slot": 1,
      "speed": 2.0
   }],
   "processorSlots": 2,
   "productId": "321",
   "raidSettings": [],
   "secureBootMode": {
      "currentValue": "",
      "possibleValues": []
   },
   "serialNumber": "DSY0123",
   "type": "ITE",
   "slots": [1],
   "status": {
      "message": "managed",
      "name": "MANAGED"
   },
   "subSlots": [],
   "subType": "Blacktip",
   "tlsVersion": {
      "currentValue": "Unknown",
      "possibleValues": ["TLS_10", "TLS_11", "TLS_12", "unsupported"]
   },
   "uri": "node/B9A8192D427011E18F04F5F1A3C864E0",
   "userDescription": "",
   "userDefinedName": "Server1",
   "uuid": "B9A8192D427011E18F04F5F1A3C864E0",
```

```
   "vnicMode": "disabled",
   "vpdID": "256",
}]
"passThroughModules": [],
"overallHealthState": "Critical",
"parent": {
   "uri": "cabinet/C58EA698-C223-42DA-93C8-38ED810F58A9",
   "uuid": "C58EA698-C223-42DA-93C8-38ED810F58A9"
},
"partNumber": "88Y6660",
"productId": "336",
"posID": "14",
"powerAllocation": {
   "allocatedOutputPower": 3780,
   "midPlaneCardMaximumAllocatedPower": 38,
   "midPlaneCardMinimumAllocatedPower": 38,
   "remainingOutputPower": 11250,
   "totalInputPower": 16336,
   "totalOutputPower": 15030
},
"powerSupplies": [{
   "cmmDisplayName": "Power Supply 01",
   "cmmHealthState": "Normal",
   "dataHandle": 0,
   "description": "Power Supply",
   "firmware": [{
      "build": "",
      "date": "",
      "name": "Power Supply Firmware",
      "role": "",
      "status": "",
      "type": "Power Supply Firmware",
      "version": "0"
   }],
   "FRU": "69Y5817",
   "fruSerialNumber": "ZK125116E07T",
   "hardwareRevision": "5.0",
   "inputVoltageIsAC": true,
   "inputVoltageMax": 208,
   "inputVoltageMin": 200,
   "leds": [{
      "color": "Green",
      "location": "Planar",
      "name": "IN",
      "state": "On"
   },
   ...,
   {
      "color": "Amber",
      "location": "Planar",
      "name": "FAULT",
      "state": "Off"
   }],
   "machineType": "",
   "manufactureDate": "2411",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "name": "Power Supply 01",
   "model": "",
   "parent": {
      "uri": "chassis/E053C9508C244F549011B2518DB71236",
```

```
      "uuid": "E053C9508C244F549011B2518DB71236"
   },
   "partNumber": "69Y5801",
   "posID": "60",
   "powerAllocation": {
      "totalInputPower": 2505,
      "totalOutputPower": 1252
   },
   "powerState": "Unknown",
   "productId": "303",
   "productName": "IBM 2500 W Power Supply",
   "serialNumber": "",
   "slots": [1],
   "type": "PowerSupply",
   "userDescription": "",
   "uri": "powerSupply/D0A3B8399BFD11E000FD00FD00FD00FD00FD",
   "vpdID": "128",
   "uuid": "D0A3B8399BFD11E000FD00FD00FD00FD00FD"
}],
"powerSupplySlots": 6,
"productName": "IBM Chassis Midplane",
"securityDescriptor": {
   "managedAuthEnabled": true,
   "managedAuthSupported": true,
   "publicAccess": true,
   "roleGroups": ["lxc-admin","lxc-security-admin"],
   "uri": "chassis/E053C9508C244F549011B2518DB71236"
},
"SecurityPolicy": {
   "cmmPolicyLevel": "LEGACY",
   "cmmPolicyState": "ACTIVE"
},
"serialNumber": "100065A",
"status": {
   "message": "MANAGED",
   "name": "MANAGED"
},
"switches": [{
   "accessState": "Online",
   "attachedNodes": [],
   "backedBy": "real",
   "cmmDisplayName": "IO Module 01",
   "cmmHealthState": "Normal",
   "dataHandle": 1508187387271,
   "description": "EN4093 10Gb Ethernet Switch",
   "dnsHostnames": ["SW-Y250VT161664.labs.lenovo.com", "fd55:faaf:e1ab:20fc:a17:f4ff:fe77:1fef"],
   "errorFields": [{
      "IOCompatibilityData": "FETCH_FAILED"
   }],
   "excludedHealthState": "Normal",
   "hostname": "",
   "ipInterfaces": [{
      "IPv4assignments": [{
         "address": "10.240.75.192",
         "gateway": "10.240.72.1",
         "id": 2,
         "subnet": "255.255.252.0",
         "type": "INUSE"
      }],
      "IPv4DHCPmode": "STATIC_ONLY",
      "IPv4enabled": true,
```

```
   "IPv6assignments": [{
      "address": "fd55:faaf:e1ab:20fc:a17:f4ff:fe77:1fef",
      "gateway": "0:0:0:0:0:0:0:0",
      "id": 33,
      "prefix": 64,
      "scope": "Global",
      "source": "Stateless",
      "type": "INUSE"
   }],
   "IPv6DHCPenabled": true,
   "IPv6enabled": true,
   "IPv6statelessEnabled": true,
   "IPv6staticEnabled": false,
   "label": "",
   "name": "ioe0"
}],
"ipv4Addresses": ["10.240.75.192"],
"firmware": [{
   "build": "",
   "date": "2017-04-24T04:00:00Z",
   "name": "Boot ROM",
   "status": "Active",
   "type": "Boot ROM",
   "version": "7.8.17.0"
},
...,
{
   "build": "",
   "date": "2016-11-18T05:00:00Z",
   "name": "Main Application 2",
   "status": "Not-Active",
   "type": "Main Application 2",
   "version": "7.8.16.0"
}],
"FRU": "49Y4273",
"fruSerialNumber": "Y250VT161664",
"ipv6Addresses": ["fd55:faaf:e1ab:20fc:a17:f4ff:fe77:1fef", "fe80:0:0:0:a17:f4ff:fe77:1fef"],
"leds": [{
   "color": "Blue",
   "location": "FrontPanel",
   "name": "Enclosure Identify",
   "state": "Off"
},
...,
{
   "color": "Green",
   "location": "FrontPanel",
   "name": "Power",
   "state": "On"
}],
"macAddresses": ["08:17:F4:77:1F:EF"],
"machineType": "",
"manufacturer": "IBM",
"manufacturerId": "20301",
"model": "",
"ntpPushEnabled": false,
"name": "IO Module 01",
"ntpPushFrequency": 15,
"overallHealthState": "Normal",
"parent": {
   "uri": "chassis/E053C9508C244F549011B2518DB71236",
```

```
            "uuid": "E053C9508C244F549011B2518DB71236"
         },
         "partNumber": "49Y4272",
         "posID": "23",
         "powerAllocation": {
            "maximumAllocatedPower": 100,
            "minimumAllocatedPower": 100
         },
         "powerState": "On",
         "productId": "322",
         "productName": "IBM Flex System Fabric EN4093 10Gb Scalable Switch",
         "protectedMode": "False",
         "serialNumber": "",
         "slots": [1],
         "stackMode": "Standby",
         "type": "Switch",
         "userDefinedName": "Switch1",
         "userDescription": "",
         "uri": "switch/1B33D6CA440EAEE167660817F4771F00",
         "uuid": "1B33D6CA440EAEE167660817F4771F00",
         "vpdID": "304"
      }],
      "switchSlots": 4,
      "tlsVersion": {
         "currentValue": "TLS_13",
         "possibleValues": ["unsupported","TLS_13","TLS_12","TLS_11"]
      },
      "type": "Chassis",
      "uri": "chassis/E053C9508C244F549011B2518DB71236",
      "userDefinedName": "Chassis1",
      "userDescription": "",
      "uuid": "E053C9508C244F549011B2518DB71236",
      "vpdID": "336",
   }]
}
```


/chassis/*{file_name}*.csv

Use this REST API to download inventory for a large number of specific Flex System chassis and chassis components in CSV format to the local system.

HTTP methods

GET

GET /chassis/*{file_name}*.csv

Use this method to download inventory for a large number of specific Flex System chassis and chassis components in CSV format to the local system.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/chassis/{file_name}.csv`

where <*file_name}*.csv is the file name of the CSV file that contains inventory data. Use the POST /chassis method to with the **formatType=csv** request parameter to create the CSV file. The POST /chassis method returns the file name in the request header.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/chassis/*{uuid}*

Use this REST API to retrieve or modify properties for a specific Flex System chassis and chassis resources.

HTTP methods

GET, PUT

GET /chassis/*{uuid_list}*

Use this method to return properties for one or more specific Flex System chassis and chassis components.

Note: Only the **lxc-sysmgr** user account has authority to perform this action

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/chassis/{uuid_list}`

where *{uuid_list}* is one or more UUIDs, separated by a comma, of the chassis to be retrieved. To obtain the chassis UUIDs, use the GET /chassis method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
formatType=*{type}*	Optional	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv** If the format type is not specified, JSON format is returned.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

The following example returns a CSV file that contains information about two specific chassis.

```
GET https://192.0.2.0/chassis/0E7D8E1CDF7D11D4ABB0D5D5D5313131,
409583E0BD27B7019F3758946B036818}?formatType=csv
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
413	Request Entity Too Large	Clients might impose limitations on the length of the request URI, and the request URI is too long to be handled. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
accessState	String	Access state of the chassis. This can be one of the following values. • **Online** • **Offline** • **Partial** • **Pending** • **Unknown**
accessStateRecords	Array of objects	Information about the access-state record for each network interface and protocol that is available for the chassis **Note:** This attribute is present only for chassis that are offline due to connectivity issues.
health	String	Connection health state of the chassis. This can be one of the following values. • **OFFLINE** • **PARTIAL** • **FAIL**
ipAddress	String	IP address that was used to check the network connectivity
isTrusted	Boolean	Indicates whether the connection to the server is trusted. This can be one of the following values. • **true**. The connection is trusted. • **false**. The connection is not trusted.
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle
messageDisplay	String	Translated label that corresponds to the message ID or to the pre-translated backup string if no message ID is specified
messageID	String	Message ID for the translatable connection error states
messageParameters	Array of strings	Attributes for the message if the translated message requires input. A JSON object that points to translated messages
protocol	String	Type of the protocol to check connectivity. This can be one of the following values. • **CIM** • **DCS** • **REDFISH** • **CLI**
timestamp	Long	Timestamp when connectivity was last checked and when this record was created
username	String	User name that was used to check connectivity
accountLockoutPeriod	Integer	Account lockout duration, in minutes, after certain login failures occur on the device The default value is 60 minutes.
activationKeys	Array	List of Feature On Demand (FOD) keys that are installed on the CMM

Attributes	Type	Description
backedBy	String	This can be one of the following values. • **real**. The inventory describes real hardware. • **demo**. The inventory describes demo (mock) hardware. • **proxy**. A proxy is temporarily serving to provide the inventory.
bladeSlots	Integer	Number of blade slots in the chassis
cmmDisplayName	String	Chassis name
cmmHealthState	String	Health summary that corresponds to the highest event severity of all the devices. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
cmms	Array	Information about CMMs (see GET /cmms)
cmmSlots	Integer	Number of CMM slots in the chassis
complex	Array	Information about scalable complexes (see GET /scalableComplex)
contact	String	Contact for the chassis
dataHandle	Long	Time stamp of the last status update
description	String	Chassis description that was provided by the CMM
domainName	String	Domain name for the chassis
encapsulation	Object	Information about encapsulation
encapsulationMode	String	Encapsulation (firewall settings) mode. This can be one of the following values. • **notSupported**. Encapsulation is not supported for this node. • **normal**. Encapsulation is disabled for this node.The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process. • **encapsulationLite**. Encapsulation is enabled for this node.When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.
nonBlockedIpAddressList	Array of strings	List of non-blocked IP addresses. This attribute is available only when the encapsulation mode is “encapsulationLite,”.

Attributes	Type	Description
energyPolicies	Object	Information about energy policies
accousticAttenuationMode	String	Acoustic attenuation mode. This can be one of the following values. • **Off** • **Least attenuation** • **Low level attenuation** • **Mid level attenuation** • **High level attenuation** • **Most attenuation** • **Unknown**
hotAirRecirculation	Object	Information about hot air recirculation
chassisBay	Array	Chassis bay hot air recirculation details
isExceeded	String	Sensor value exceeded or not
sensorName	String	Sensor name
sensorValue	Double	Sensor value
slot	Integer	Slot occupied
subSlot	Integer	Sub-slot occupied
isEnabled	Boolean	Identifies whether hot-air recirculation is enabled. This can be one of the following values. • **true**. Hot-air recirculation is enabled. • **false**. Hot-air recirculation is disabled.
maxVariation	Double	Hot-air recirculation maximum temperature variation.
powerCappingPolicy	Object	Information about the power-capping policy
cappingPolicy	String	Capping policy. This can be one of the following values. • **OFF** • **STATIC** • **UNKNOWN**
currentPowerCap	Long	Current power-capping policy level
maxPowerCap	Long	Maximum power-capping policy level
minPowerCap	Long	Minimum power-capping policy level
powerRedundancyMode	Long	Power-redundancy mode
errorFields	Array of objects that contain *{string, error-Code}*	Error Codes. This can be one of the following values. • **FETCH_SUCCESS** • **FETCH_FAILED** • **NO_CONNECTOR** • **FATAL_EXCEPTION** • **NETWORK_FAIL**

Attributes	Type	Description
excludedHealthState	String	Highest severity alert with exclusions. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
fanMuxes	Array	Information about fan logic modules (see GET /fanMuxes)
fanMuxSlots	Integer	Number of fan mux slots in the chassis
fans	Array	Information about fans (see GET /fans)
fanSlots	Integer	Number of fan slots in the chassis
height	Integer	Chassis height
hostname	String	Hostname for the chassis
isConnectionTrusted	Boolean	Identifies whether the CMM has a trusted connection. This can be one of the following values. • **true**. The CMM has a trusted connection. • **false**. The CMM does not have a trusted connection.
inventoryState	String	Inventory state. This can be one of the following values. • **INVENTORY_STARTING** • **INVENTORY_PARTIAL** • **INVENTORY_MINIMAL** • **INVENTORY_READY**
ledCardSlots	Integer	Number of LED card slots in the chassis
leds	Array	Information about LEDs
color	String	LED color. This can be one of the following values. • **Red** • **Amber** • **Yellow** • **Green** • **Blue** • **Unknown**
location	String	LED location. This can be one of the following values. • **Front panel** • **Lightpath Card** • **Planar** • **FRU** • **Rear Panel** • **Unknown**
name	String	LED name
state	String	LED state. This can be one of the following values. • **Off** • **On** • **Blinking** • **Unknown**
location	Object	Information about the chassis location

Attributes	Type	Description
location	String	Location
lowestRackUnit	Integer	Lowest rack unit
rack	String	Rack
room	String	Room
machineType	String	Chassis machine type
managedChassis	Boolean	(Flex System and dense chassis only) Indicates whether this chassis was explicitly managed by a user. This can be one of the following values. • **true**. (default) The chassis is managed. • **false**. The chassis is not managed. This attribute is supported in XClarity Administrator v4.1 and later.
managerName	String	This value is always set to “UNKNOWN.”
managerUuid	String	This value is always set to “UNKNOWN.”
manufacturer	String	Name of the manufacturer
manufacturerID	String	ID of the manufacturer
mgmtProcIPaddress	String	IP address used by the XClarity Administrator to manage this resource
model	String	Chassis model
name	String	Name that is displayed in the user interface for this device The value of this attribute is determined by **preferredDisplayName** attribute in the GET /aicc method. For example, if the **preferredDisplayName** attribute is set to “hostname,” then the value for this **name** attribute is the same as the **hostname** attribute in the GET /aicc method.
nist	Object	Information about NIST
currentValue	String	Cryptography mode that is set. This can be one of the following values. • **Unknown** • **Compatibility** • **Nist_800_131A_Strict** • **Nist_800_131A_Custom**
possibleValues	Array	All possible NIST values
nodes	Array	Information about servers (see GET /nodes)
overallHealthState	String	Highest severity of all alerts. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
partNumber	String	Chassis part number

Attributes	Type	Description
passThroughModules	Array	Information about pass-through modules (see GET /switches)
posID	String	Position ID
powerAllocation	Object	Information about power allocation
allocatedOutputPower	Long	Allocated output power
midPlaneCardMaximumAllocatedPower	Long	Maximum power that is allocated to the midplane card
midPlaneCardMinimumAllocatedPower	Long	Minimum power that is allocated to the midplane card
remainingOutputPower	Long	Remaining output power
totalInputPower	Long	Total input power
totalOutputPower	Long	Total output power
powerSupplySlots	Integer	Number of power supply slots in the chassis
powerSupplies	Array	Information about power supplies (see GET /powerSupplies)
productID	String	Product ID
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports the ability to choose managed authentication. • **false**. This device does not support the ability to choose managed authentication.
publicAccess	Boolean	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device
storedCredentials	Array of objects	Information about the stored credential that is associated with this device, if applicable
description	String	Description of the stored credential
id	String	ID of the stored credential
userName	String	Name of the stored credential
uri	String	URI of the device
SecurityPolicy	Object	Security level to adjust the system towards

Attributes	Type	Description
cmmPolicyLevel	String	Policy level that is set on the CMM. This can be one of the following values. • **LEGACY** • **SECURE**
cmmPolicyState	String	Policy state of the CMM. This can be one of the following values. • **ERROR** • **UNKNOWN** • **ACTIVE** • **PENDING**
serialNumber	String	Chassis serial number
status	Object	
message	String	MANAGED
name	String	MANAGED
switches	Array	Information about switches (see GET /switches)
switchSlots	Integer	Number of switch slots in the chassis
tlsVersion	Object	Information about the SSL or TLS protocol
currentValue	String	SSL or TLS protocol and version that is set. This can be one of the following values. • **unsupported** • **TLS_12**. TLS v1.2 • **TLS_13**. TLS v1.3
possibleValues	Array	All possible SSL or TLS protocol values
type	String	Resource type. This value is always “Chassis.”
uri	String	URI for the chassis
userDefinedName	String	User-defined name for the device
userDescription	String	Chassis description that was defined by the user
uuid	String	Chassis UUID
vpdID	String	Vital product data (VPD) ID

The following example is returned if the request is successful and the **formatType=json** query parameter is specified.


```
{
    "accessState": "Online",
    "accountLockoutPeriod": 60,
    "activationKeys": [],
    "backedBy": "real",
    "complex": [{
        "complexID": "1E495E5E",
        "nodeCount": 1,
        "orphanNodes": [{
            "activationKeys": [],
            "addinCards": [],
            "addinCardSlots": 0,
            "accessState": "Online",
            "arch": "x86",
            "backedBy": "real",
```

```
"bladeState": 1,
"bladeState_health": "GOOD",
"bladeState_string": "Newport213-14",
"bmuParamObject": null,
"bootMode": {
        "currentValue": "UEFI Mode",
        "possibleValues": ["UEFI Mode", "Legacy Mode"]
},
"bootOrder": {
    "bootOrderList": [{
        "bootType": "SingleUse",
        "currentBootOrderDevices": ["None"],
        "possibleBootOrderDevices": ["None", "PXE Network", "Hard Disk 0", "Diagnostics",
                                     "CD/DVD Rom", "Boot To F1", "Hypervisor", "Floppy Disk"]
    }, {
        "bootType": "Permanent",
        "currentBootOrderDevices": ["CD/DVD Rom", "Hard Disk 0", "PXE Network"],
        "possibleBootOrderDevices": ["CD/DVD Rom", "Hard Disk 0", "PXE Network", "Floppy Disk",
                                     "Hard Disk 1", "Hard Disk 2", "Hard Disk 3", "Hard Disk 4",
                                "USB Storage", "Diagnostics", "iSCSI", "iSCSI Critical",
                                "Embedded Hypervisor", "Legacy Only", "IMM1", "IMM2", "DSA",
                                "USB0", "USB1", "USB2", "USB3", "USB4", "SAS", "NIC1", "NIC2",
                                "NIC3", "NIC4", "VNIC1", "VNIC2", "VNIC3", "VNIC4", "VNIC5",
                                "VNIC6", "VNIC7", "VNIC8", "VNIC9", "VNIC10", "VNIC11", "VNIC12",
                                "Mezzanine1Device1", "Mezzanine1Device2", "Mezzanine1Device3",
                                "Mezzanine1Device4", "Mezzanine1Device5", "Mezzanine1Device6",
                                "Mezzanine2Device1", "Mezzanine2Device2", "Mezzanine2Device3",
                                "Mezzanine2Device4", "Mezzanine2Device5", "Mezzanine2Device6",
                                "Mezzanine3Device1", "Mezzanine3Device2", "Mezzanine4Device1",
                                "Mezzanine4Device2"]
    }, {
        "bootType": "WakeOnLAN",
        "currentBootOrderDevices": ["PXE Network", "CD/DVD Rom", "Hard Disk 0"],
        "possibleBootOrderDevices": ["PXE Network", "CD/DVD Rom", "Hard Disk 0", "Floppy Disk",
                                     "Hard Disk 1", "Hard Disk 2", "Hard Disk 3", "Hard Disk 4",
                                "USB Storage", "Diagnostics", "iSCSI", "iSCSI Critical",
                                "Embedded Hypervisor", "Legacy Only", "IMM1", "IMM2", "DSA",
                                "USB0", "USB1", "USB2", "USB3", "USB4", "SAS", "NIC1", "NIC2",
                                "NIC3", "NIC4", "VNIC1", "VNIC2", "VNIC3", "VNIC4", "VNIC5",
                                "VNIC6", "VNIC7", "VNIC8", "VNIC9", "VNIC10", "VNIC11", "VNIC12",
                                "Mezzanine1Device1", "Mezzanine1Device2", "Mezzanine1Device3",
                                "Mezzanine1Device4", "Mezzanine1Device5", "Mezzanine1Device6",
                                "Mezzanine2Device1", "Mezzanine2Device2", "Mezzanine2Device3",
                                "Mezzanine2Device4", "Mezzanine2Device5", "Mezzanine2Device6",
                                "Mezzanine3Device1", "Mezzanine3Device2", "Mezzanine4Device1",
                                "Mezzanine4Device2"]
    }],
    "uri": "nodes/F087DAB569F211E39C766CAE8B702C60/bootOrder"
},
"cmmDisplayName": "Node 13",
"cmmHealthState": "Normal",
"complexID": 508124766,
"contact": "test",
"dataHandle": 1701112556513,
"description": "Device data missing",
"dnsHostnames": ["192.0.12.253"],
"domainName": "",
"driveBays": 8,
"drives": [],
"embeddedHypervisorPresence": false,
"encapsulation": {
```

```
    "encapsulationMode": "notSupported"
},
"excludedHealthState": "Normal",
"errorFields": [{
    "ReleaseInfoData": "NO_CONNECTOR"
}, {
    "SingleSignOn": "NO_CONNECTOR"
}, {
        "MPFAHealthStatus": "NO_CONNECTOR"
}],
"expansionCards": [],
"expansionCardSlots": 4,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [{
    "deviceId": 0,
    "entityId": 0,
    "name": "front panel board 1",
    "posID": 0,
    "productId": 0,
    "vpdID": 0
}, {
    "deviceId": 0,
    "entityId": 0,
    "name": "system board 1",
    "posID": 0,
    "productId": 0,
    "vpdID": 0
}],
"firmware": [{
    "build": "1AOO87B",
    "classifications": [],
    "date": "2018-12-14T00:00:00Z",
    "name": "IMM2 Backup Firmware",
    "revision": "7.20",
    "role": "Backup",
    "status": "Inactive",
    "type": "IMM2-Backup",
    "version": "7.20"
},
...,
{
    "classifications": [],
    "build": "1AOO87B",
    "date": "2018-12-14T00:00:00Z",
    "name": "IMM2 Firmware",
    "revision": "7.20",
    "role": "Primary",
    "status": "Active",
    "type": "IMM2",
    "version": "7.20"
}],
"flashStorage": [],
"FRU": "47C2239",
"fruSerialNumber": "YC31BG3B503C"
"FQDN": "192.0.12.253",
"hasOS": false,
"hostMacAddresses": "6C:AE:8B:70:2C:60,6C:AE:8B:70:2C:64,6C:AE:8B:70:2C:68,6C:AE:8B:70:2C:6C",
"hostname": "IMM2-6cae8b6f0b11",
"inventoryState": "INVENTORY_READY",
"ipv4Addresses": ["192.0.12.253", "169.254.95.118"],
```

```
"ipInterfaces": [{
    "IPv4assignments": [{
            "id": 0,
            "address": "192.0.12.253",
            "gateway": "192.0.0.1",
            "subnet": "255.255.224.0",
            "type": "INUSE"
        }],
    "IPv4DHCPmode": "DHCP_ONLY",
    "IPv4enabled": true,
    "IPv6assignments": [{
            "id": 0,
            "address": "fe80:0:0:0:6eae:8bff:fe6f:b14",
            "gateway": "fe80:0:0:0:5:73ff:fea0:2c",
            "prefix": 64,
            "scope": "Unknown",
            "source": "Unknown",
            "type": "UNKNOWN"
        }, {
            "id": 0,
            "address": "fd55:faaf:e1ab:2021:6eae:8bff:fe6f:b14",
            "gateway": "fe80:0:0:0:5:73ff:fea0:2c",
            "prefix": 64,
            "scope": "Global",
            "source": "Stateless",
            "type": "INUSE"
        }],
    "IPv6DHCPenabled": true,
    "IPv6enabled": true,
    "IPv6statelessEnabled": true,
    "IPv6staticEnabled": false,
    "label": "unknown",
    "name": "eth0"
}, {
    "IPv4assignments": [],
    "IPv4DHCPmode": "STATIC_ONLY",
    "IPv4enabled": true,
    "IPv6assignments": [{
            "id": 0,
            "address": "fe80:0:0:0:6eae:8bff:fe6f:b14",
            "gateway": "fe80:0:0:0:5:73ff:fea0:2c",
            "prefix": 64,
            "scope": "Unknown",
            "source": "Unknown",
            "type": "UNKNOWN"
        }, {
            "id": 0,
            "address": "fd55:faaf:e1ab:2021:6eae:8bff:fe6f:b14",
            "gateway": "fe80:0:0:0:5:73ff:fea0:2c",
            "prefix": 64,
            "scope": "Global",
            "source": "Stateless",
            "type": "CONFIGURED"
        }],
    "IPv6DHCPenabled": true,
    "IPv6enabled": true,
    "IPv6statelessEnabled": false,
    "IPv6staticEnabled": false,
    "label": "unknown",
    "name": "ethernet-over-usb"
}],
```

```
"ipv6Addresses": ["fd55:faaf:e1ab:2021:6eae:8bff:fe6f:b14", "fe80:0:0:0:6eae:8bff:fe6f:b14"],
"isConnectionTrusted": "true",
"isITME": false,
"isRemotePresenceEnabled": true,
"lanOverUsb": "enabled",
"leds": [{
    "color": "Yellow",
    "location": "Planar",
    "name": "DIMM 48",
    "state": "Off"
},
...,
{
    "color": "Yellow",
    "name": "DIMM 10",
    "location": "Planar",
    "state": "Off"
}],
"isScalable": true,
"lanOverUsbPortForwardingModes": [{
    "externalIPAddress": "",
    "state": "disabled",
    "type": "DSA"
}],
"location": {
    "rack": "",
    "location": "test",
    "lowestRackUnit": 0,
    "room": ""
},
"machineType": "7903",
"logicalID": 0,
"m2Presence": false,
"macAddress": "6C:AE:8B:6F:0B:14,6C:AE:8B:6F:0B:16",
"manufacturer": "CITRIX_BLADE",
"manufacturerId": "20301",
"memoryModules": [{
    "capacity": 4,
    "displayName": "DIMM 1",
    "fruPartNumber": "",
    "healthState": "NA",
    "manufacturer": "Samsung",
    "model": "DDR3",
    "operatingMemoryMode": null,
    "partNumber": "M393B5270QB0-YK0",
    "present": false,
    "serialNumber": "01976141",
    "slot": 1,
    "speed": 1600,
    "speedMBs": 0,
    "type": "DDR3"
}],
"memorySlots": 48,
"mgmtProcIPaddress": "192.0.12.253",
"mgmtProcType": "IMM2",
"model": "AC1",
"name": "Newport213-14",
"nist": {
    "currentValue": "Unknown",
    "possibleValues": ["Nist_800_131A_Strict", "unsupported", "Compatibility"]
},
```

```
"onboardPciDevices": [{
    "class": "Display controller",
    "firmware": [],
    "fodUniqueID": "",
    "isAddOnCard": false,
    "isAgentless": false,
    "isPLDMUpdateSupported": false,
    "name": "",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "0",
    "pciBusNumber": "9",
    "pciRevision": "0",
    "pciSubID": "0",
    "pciSubVendorID": "0",
    "portInfo": {},
    "posID": "534",
    "vpdID": "102b"
}, {
    "class": "Network controller",
    "firmware": [{
        "build": "0",
        "classifications": [13],
        "date": "",
        "name": "OneConnect 10G/40G Flash Image",
        "revision": "0",
        "role": "Primary",
        "softwareID": "10DFE812",
        "status": "Active",
        "type": "Software Bundle",
        "version": "192.0.2.26"
    }],
    "fodUniqueID": "N/A",
    "isAddOnCard": false,
    "isAgentless": true,
    "isPLDMUpdateSupported": false,
    "name": "N/A",
    "pciBusNumber": "139",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "2",
    "pciRevision": "10",
    "pciSubID": "e812",
    "pciSubVendorID": "10df",
    "portInfo": {
            "physicalPorts": [{
                "logicalPorts": [{
                    "addresses": "6CAE8B702C68",
                    "logicalPortIndex": 1,
                    "portNumber": 1,
                    "portType": "ETHERNET",
                    "vnicMode": false
                }],
                "physicalPortIndex": 3,
                "peerBay": 0,
                "portNumber": 3,
                "portType": "ETHERNET",
                "speed": 0.0,
                "status": null
            }]
        },
    "posID": "720",
    "vpdID": "10df"
```

```
}],
"overallHealthState": "Normal",
"osInfo": {
            "description": "",
            "hostname": "",
            "storedCredential": ""
        },
"parent": {
    "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
    "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
},
"parentComplexID": "1E495E5E",
"partitionID": -1,
"partNumber": "00AN678",
"pciCapabilities": ["Raid Link", "OOB PCIe"],
"pciDevices": [{
    "class": "Display controller",
    "firmware": [],
    "fodUniqueID": "",
    "isAddOnCard": false,
    "isAgentless": false,
    "isPLDMUpdateSupported": false,
    "pciDeviceNumber": "0",
    "name": "",
    "pciBusNumber": "9",
    "pciFunctionNumber": "0",
    "pciRevision": "0",
    "pciSubID": "0",
    "pciSubVendorID": "0",
    "portInfo": {},
    "posID": "534",
    "vpdID": "102b",
},
...,
{
    "class": "Network controller",
    "firmware": [{
        "build": "0",
        "classifications": [13],
        "date": "",
        "name": "OneConnect 10G/40G Flash Image",
        "revision": "0",
        "role": "Primary",
        "softwareID": "10DFE812",
        "status": "Active",
        "type": "Software Bundle",
        "version": "192.0.2.26"
    }],
    "fodUniqueID": "N/A",
    "isAddOnCard": false,
    "isAgentless": true,
    "isPLDMUpdateSupported": false,
    "name": "N/A",
    "pciBusNumber": "139",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "2",
    "pciRevision": "10",
    "pciSubID": "e812",
    "pciSubVendorID": "10df",
    "portInfo": {
        "physicalPorts": [{
```

```
            "logicalPorts": [{
                "addresses": "6CAE8B702C68",
                "logicalPortIndex": 1,
                "portNumber": 1,
                "portType": "ETHERNET",
                "vnicMode": false
            }],
            "peerBay": 0,
            "physicalPortIndex": 3,
            "portNumber": 3,
            "portType": "ETHERNET",
            "speed": 0.0,
            "status": null
        }]
    },
    "posID": "720",
    "vpdID": "10df",
}],
"ports": [{
    "ioModuleBay": 1,
    "portNumber": 1
}, {
    "ioModuleBay": 2,
    "portNumber": 2
}, {
    "ioModuleBay": 0,
    "portNumber": 3
}, {
    "ioModuleBay": 0,
"portNumber": 4
}],
"posID": "30",
"powerAllocation": {
    "maximumAllocatedPower": 299,
    "minimumAllocatedPower": 211
},
"powerStatus": 5,
"powerSupplies": [],
"primary": false,
"processorIntelSpeedSelect": {
    "currentValue": "",
    "possibleValues": []
},
"processors": [{
    "cores": 12,
    "displayName": "Intel(R) Xeon(R) CPU E7-8850 v2 @ 2.30GHz",
    "family": "PENTIUM_R_4",
    "healthState": "NA",
    "manufacturer": "Intel(R) Corporation",
    "maxSpeedMHZ": 2300,
    "partNumber": "Unknown",
    "present": false,
    "productVersion": "Intel(R) Xeon(R) CPU E7-8850 v2 @ 2.30GHz",
    "serialNumber": "Unknown",
    "slot": 1,
    "speed": 2.3,
    "socket": "",
    "tdpWatts": -1,
}],
"processorSlots": 2,
"productId": "448",
```

```
            "productName": "",
            "raidSettings": [],
            "secureBootMode": {
                "currentValue": "Disabled",
                "possibleValues": ["Enabled", "Disabled"]
            },
            "securityDescriptor": {
                "identityManagementSystemEnabled": false,
                "managedAuthEnabled": true,
                "managedAuthSupported": true,
                "publicAccess": false,
                "roleGroups": ["lxc-supervisor", "lxc-recovery"],
                "storedCredentials": {
                    "id": "1752",
                    "description": "Credentials for IamMM1",
                    "userName": "userid"
                },
                "uri": "nodes/f087dab569f211e39c766cae8b702c60",
            },
            "serialNumber": "23YVLH4",
            "slots": [13, 14],
            "ssoEnabled": false,
            "status": {
                "message": "managed",
                "name": "MANAGED"
            },
            "subType": "Nantahala",
            "subSlots": [],
            "tlsVersion": {
                "currentValue": "Unknown",
                "possibleValues": ["unsupported", "TLS_12", "TLS_11", "TLS_10"]
            },
            "type": "ITE",
            "uri": "nodes/F087DAB569F211E39C766CAE8B702C60",
            "userDefinedName": "Newport213-14",
            "userDescription": "",
            "uuid": "F087DAB569F211E39C766CAE8B702C60",
            "vnicMode": "disabled",
            "vpdID": "256",
        }],
        "partition": [],
        "partitionCount": 0,
        "slots": [13, 14],
        "uuid": "F087DAB569F211E39C766CAE8B702C60"
    }],
    "cmmDisplayName": "IamMM1",
    "cmmHealthState": "Critical",
    "cmms": [...],
    "bladeSlots": 14,
    "contact": "No Contact Configured",
    "dataHandle": 1701192297537,
    "description": "Lenovo Flex System Chassis",
    "displayName": "IamMM1",
    "domainName": "",
    "encapsulation": {
        "encapsulationMode": "normal"
    },
    "energyPolicies": {
        "acousticAttenuationMode": "Off",
        "hotAirRecirculation": {
            "chassisBay": [{
```

```
            "isExceeded": "N",
            "sensorName": "Inlet 1 Temp",
            "sensorValue": 20.0,
            "slot": 13,
            "subSlot": -1
        },
        ...,
        {
            "isExceeded": "N",
            "sensorName": "Inlet Temp",
            "sensorValue": 22.0,
            "slot": 10,
            "subSlot": 1
        }],
        "isEnabled": true,
        "maxVariation": 5.0
    },
    "powerCappingPolicy": {
        "cappingACorDCMode": null,
        "cappingPolicy": "OFF",
        "currentPowerCap": 0,
        "maximumPowerCappingHotPlugLevel": null,
        "maxPowerCap": 12525,
        "minimumHardCapLevel": null,
        "minimumPowerCappingHotPlugLevel": null,
        "minPowerCap": 3049,
        "powerCappingAllocUnit": "watts"
    },
    "powerRedundancyMode": 3
},
"errorFields": [],
"excludedHealthState": "Critical",
"fans": [{
    "parent": {
        "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
        "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
    },
    "FRU": "81Y2911",
    "description": "Fan Module",
    "excludedHealthState": "Normal",
    "type": "Fan",
    "uuid": "586E241977E541DD884D3289F72BBDE6",
    "productName": "",
    "manufacturer": "IBM",
    "powerState": "Unknown",
    "overallHealthState": "Normal",
    "powerAllocation": {
        "maximumAllocatedPower": 60,
        "minimumAllocatedPower": 60
    },
    "manufactureDate": "3111",
    "model": "",
    "errorFields": [],
    "firmware": [{
        "build": "",
        "classifications": [],
        "date": "",
        "name": "Fan Controller",
        "revision": "226",
        "role": "",
        "status": "",
```

```
            "type": "Fan Controller",
            "version": "226",
        }],
        "machineType": "",
        "serialNumber": "",
        "userDescription": "",
        "productId": "339",
        "manufacturerId": "20301",
        "cmmDisplayName": "Fan 05",
        "uri": "fan/586E241977E541DD884D3289F72BBDE6",
        "cmmHealthState": "Normal",
        "posID": "8",
        "slots": [5],
        "hardwareRevision": "4.0",
        "vpdID": "373",
        "dataHandle": 0,
        "name": "Fan 05",
        "leds": [{
            "color": "Amber",
            "location": "FrontPanel",
            "name": "FAULT",
            "state": "Off"
        }],
        "partNumber": "88Y6670",
        "fruSerialNumber": "YK10GM17S067"
    }],
    "fanSlots": 10,
    "fanMuxes": [{
        "cmmHealthState": "Non-Critical",
        "cmmDisplayName": "Fan Logic 02",
        "dataHandle": 0,
        "description": "Fan Logic Module",
        "excludedHealthState": "Warning",
        "FRU": "81Y2912",
        "fruSerialNumber": "Y031BG16P017",
        "leds": [{
            "color": "Amber",
            "location": "FrontPanel",
            "name": "FAULT",
            "state": "On"
        }],
        "machineType": "",
        "hardwareRevision": "4.0",
        "manufactureDate": "2611",
        "manufacturer": "IBM",
        "manufacturerId": "20301",
        "model": "",
        "name": "Fan Logic 02",
        "overallHealthState": "Warning",
        "parent": {
            "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91".
            "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
        },
        "partNumber": "81Y2990",
        "productId": "338",
        "productName": "IBM Fan Pack Multiplexor Card",
        "serialNumber": "",
        "slots": [2],
        "status": "Non-Critical",
        "type": "FanMux",
        "uri": "fanMux/54D1E375A19F11E0ADA7D9E63ABF920B",
```

```
    "uuid": "54D1E375A19F11E0ADA7D9E63ABF920B"
}],
"fanMuxSlots": 2,
"FQDN": "",
"height": 10,
"hostname": "MM40F2E9BF07C4",
"isConnectionTrusted": "true",
"lastOfflineTimestamp": -1,
"ledCardSlots": 1,
"leds": [{
    "color": "Blue",
    "location": "FrontPanel",
    "name": "Location",
    "state": "Off"
}, {
    "color": "Amber",
    "location": "FrontPanel",
    "name": "Information",
    "state": "On"
}, {
    "color": "Amber",
    "location": "FrontPanel",
    "name": "FAULT",
    "state": "Off"
}],
"location": {
    "location": "No Location Configured",
    "lowestRackUnit": 0,
    "rack": "",
    "room": ""
},
"machineType": "8721",
"managedChassis": true,
"managerName": "UNKNOWN",
"managerUuid": "UNKNOWN",
"manufacturer": "IBM",
"manufacturerId": "20301",
"mgmtProcIPaddress": "192.0.3.55",
"mmSlots": 2,
"model": "HC1",
"name": "IamMM1",
"nist": {
    "currentValue": "Compatibility",
    "possibleValues": ["Nist_800_131A_Strict", "unsupported", "Nist_800_131A_Custom", "Compatibility"]
},
"nodes": [...],
"overallHealthState": "Critical",
"parent": {
    "uri": "cabinet/",
    "uuid": ""
},
"partNumber": "88Y6660",
"passThroughModules": [],
"posID": "14",
"powerAllocation": {
    "allocatedOutputPower": 3049,
    "midPlaneCardMaximumAllocatedPower": 38,
    "midPlaneCardMinimumAllocatedPower": 38,
    "remainingOutputPower": 9476,
    "totalInputPower": 13614,
    "totalOutputPower": 12525
```

```
},
"powerSupplies": [{
    "cmmDisplayName": "Power Supply 04",
    "cmmHealthState": "Non-Critical",
    "dataHandle": 0,
    "description": "Power Supply",
    "excludedHealthState": "Warning",
    "firmware": [{
        "build": "",
        "classifications": [],
        "date": "",
        "name": "Power Supply Firmware",
        "revision": "6",
        "role": "",
        "softwareID": "",
        "status": "",
        "type": "Power Supply Firmware",
        "version": "6"
    }],
    "FRU": "69Y5806",
    "fruSerialNumber": "ZK128117L00F",
    "hardwareRevision": "76.54",
    "healthState": "NA",
    "inputVoltageIsAC": true,
    "inputVoltageMax": -1,
    "inputVoltageMin": -1,
    "leds": [{
        "color": "Green",
        "location": "Planar",
        "name": "OUT",
        "state": "Off"
    },
    ...,
    {
        "color": "Green",
        "location": "Planar",
        "name": "IN",
        "state": "Off"
    }],
    "machineType": "",
    "manufactureDate": "2911",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Power Supply 04",
    "overallHealthState": "Warning",
    "parent": {
        "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
        "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
    },
    "partNumber": "69Y5802",
    "posID": "61",
    "powerAllocation": {
        "totalInputPower": 0,
        "totalOutputPower": 0
    },
    "powerState": "Unknown",
    "productId": "304",
    "productName": "IBM 2500 W Power Supply",
    "serialNumber": "",
    "type": "PowerSupply",
```

```
        "userDescription": "",
        "uuid": "388FA5B048634E47990B20EE420FA6BD",
        "uri": "powerSupply/388FA5B048634E47990B20EE420FA6BD",
        "slots": [4],
        "vpdID": "128",
    }],
    "powerSupplySlots": 6,
    "productId": "336",
    "productName": "IBM Chassis Midplane",
    "securityDescriptor": {
        "identityManagementSystemEnabled": false,
        "managedAuthEnabled": true,
        "managedAuthSupported": true,
        "publicAccess": false,
        "storedCredentials": {
            "id": "1752",
            "description": "Credentials for lamMM1",
            "userName": "userid"
        },
        "roleGroups": ["lxc-supervisor", "lxc-recovery"],
        "uri": "chassis/3d1d5931bdf84d30ada976e21f08cb91",
    },
    "SecurityPolicy": {
        "cmmPolicyLevel": "SECURE",
        "cmmPolicyState": "ACTIVE"
    },
    "serialNumber": "23PYP15",
    "status": {
        "message": "MANAGED",
        "name": "MANAGED"
    },
    "switches": [...],
    "switchSlots": 4,
    "tlsVersion": {
        "currentValue": "TLS_12_Server",
        "possibleValues": ["TLS_12_Server", "unsupported", "TLS_12_Server_Client", "SSL_30"]
    },
    "type": "Chassis",
    "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
    "userDefinedName": "lamMM1",
    "userDescription": "",
    "uuid": "3D1D5931BDF84D30ADA976E21F08CB91",
    "vpdID": "336"
}
```


PUT /chassis/*{uuid}*

Use this method to modify properties or refresh inventory for a specific Flex System chassis.

Note: You cannot modify properties for a DenseChassis.

The request body differs depending on the action that you want to perform. You can use this PUT method to perform the following management actions.

- Table 8 “Modify chassis properties” on page 197
- Table 9 “Refresh the inventory” on page 198
- Table 10 “Configure device authentication” on page 198
- Table 11 “Configure the security policy” on page 200
- Table 12 “Configure LED states” on page 200
- Table 13 “Configure the failover to a back CMM” on page 201

- Table 14 “Configure TLS and NIST mode” on page 201
- Table 15 “Configure the encapsulation mode” on page 202

This method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/chassis/{uuid}`

where *{uuid}* is the UUID of the chassis. To obtain the chassis UUID, use the GET /chassis method.

Query parameters

Attributes	Required / Optional	Description
synchronous=*{value}*	Optional	When modifying attributes, indicates when the job ID is returned • **true**. (default) Returns the job ID and job status after the job is complete. • **false**. Returns the job ID immediately. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. **Note:** This query parameter applies only when one or more property parameters are specified in the request body.

The following example returns the job ID and job status after the job is complete.

```
GET https://192.0.2.0/chassis/6ED2CB368C594C66C2BB066D5A306138?synchronous=true
```

Request body

You can specify attributes from one of the following tables in each request.

Note: If you specify one or more attributes in Table 8 “Modify chassis attributes” on page 197 (to modify properties) or Table 9 “Refresh the inventory” on page 198 (to refresh the inventory), this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, /tasks/12) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Table 8. Modify chassis attributes

Attributes	Required / Optional	Type	Description
cmmDisplayName	Optional	String	CMM display name
contact	Optional	String	Chassis contact information
domainName	Optional	String	Chassis domain name

Table 8. Modify chassis attributes (continued)

Attributes	Required / Optional	Type	Description
hostname	Optional	String	Chassis hostname
location	Optional	Array	Information about the chassis location **Important:** Changes made to the location of the chassis using this API method are not reflected in the rack view.
location	Optional	String	New location of the chassis
lowestRackUnit	Optional	Integer	Lowest rack unit where the chassis is installed in the rack
rack	Optional	String	Rack location
room	Optional	String	Room location
userDescription	Optional	String	Chassis description

The following example modifies the hostname, location, and contact information for a CMM:

```
{
   "contact": "new contact",
   "hostname":"",
   "location": {"location":"new location"}
}
```

Table 9. Refresh the inventory

Attributes	Required / Optional	Type	Description
refreshInventory	Optional	String	Refreshes inventory for the chassis If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

The following example refreshes inventory for the target chassis.

```
{
   "refreshInventory": "true"
}
```

Table 10. Configure device authentication and access control

Note: Only users with **lxc-supervisor** or **lxc-security-admin** privileges can modify the access-control settings.

Table 10. Configure device authentication and access control (continued)

Attributes	Required / Optional	Type	Description
securityDescriptor	Required	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Optional	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication
publicAccess	Optional	Boolean	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
roleGroups	Optional	Array of strings	List of role groups that are permitted to view and manage this device
storedCredentials	Required if **managedAuthEnabled** is set to `true`	Object	Information about the stored credential that is associated with this device, if applicable
id	Required if **managedAuthEnabled** is set to `true`	String	ID of the stored credential to associated with the device

The following example enables managed authentication and associates a stored credential account with the device.

```
{
   "securityDescriptor" : {
      "managedAuthEnabled" : true,
      "storedCredentials": {
         "id":"249721...",
      }
   }
}
```

The following example disables managed authentication to use local authentication instead.

```
{
   "securityDescriptor" : {
      "managedAuthEnabled" : false
   }
}
```

The following example restricts access to the managed device to members of the specified role groups.

```
{
   "securityDescriptor": {
```

```
      "publicAccess": false,
      "roleGroups": ["sales-os-admin","corp_fw_admin"]
   }
}
```

Table 11. Configure the security policy

Attributes	Required / Optional	Type	Description
securityPolicy	Optional	Object	Information about the security policy
mmPolicyLevel	Required	ID of the stored credential to associated with the device	Policy level to be used. This can be one of the following values. • **LEGACY** • **SECURE**

The following example modifies the security policy for a device.

```
{
   "securityPolicy: {
      "cmmPolicyLevel": "SECURE"
   }
}
```

Table 12. Configure LED states

Attributes	Required / Optional	Type	Description
leds	Optional	Object	Changes the state of the location LED
name	Required	String	Description of the LED (for example, “Fault” or “Power”. To obtain the names of LEDs for a specific chassis, use the GET /chassis/*{uuid_list}* method.
state	Required	String	State of LED. This can be one of the following values. • **off** • **on** • **blinking** To obtain the current state of the LED, use the GET /chassis/*{uuid_list}* method.

The following example turns off the Location LED.

```
{
   "leds":[{
      "name":"Location",
      "state":"off"
   }]
}
```

Table 13. Configure the failover to a back CMM

Attributes	Required / Optional	Type	Description
cmmFailover	Optional	Boolean	Indicates whether to initiate a failover. This can be one of the following values. • **true**. Initiate a failover. • **false**. Do not initiate a failover.

The following example configures failover to a backup CMM:

```
{
   "cmmFailover": true
}
```

Table 14. Configure TLS and NIST mode

Attributes	Required / Optional	Type	Description
nist	Optional	Object	Information about NIST settings
currentValue	Required	String	Cryptography mode to be used. This can be one of the following values. • **Unknown** • **Compatibility** • **Nist_800_131A_Strict** • **Nist_800_131A_Custom**
tlsVersion	Optional	Object	Information about TLS settings
currentValue	Required	String	SSL or TLS protocol and version to be used. This can be one of the following values. • **unsupported** • **TLS_12**. TLS v1.2 • **TLS_13**. TLS v1.3

The following example modifies the cryptographic settings for a device.

```
{
    "nist": {"currentValue": "NIST"}
}
```

Table 15. Configure the encapsulation mode

Attributes	Required / Optional	Type	Description
encapsulationMode	Optional	String	Encapsulation mode. This can be one of the following values. • **normal**. Encapsulation is disabled for this node.The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process. • **encapsulationLite**. Encapsulation is enabled for this node.When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.

The following example modifies the encapsulation mode.

```
{
   "encapsulationMode": "encapsulationLite"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response body provides information about the success or failure of the request. The attributes in the response body differ depending on the specified request attributes.

Note: A response body is not returned for some requests.

The following example is returned if the request is successful and the **"refreshInventory": "true"** request parameter is specified to refresh the device inventory.

```
{
   "statusCode": 200,
   "statusDescription": "The request completed successfully.",
   "messages": [{
      "explanation": "refreshInventory request for target 6ED2CB368C594C66C2BB066D5A306138 has
                      completed successfully.",
      "id": "FQXDM0200",
      "recovery": "",
      "recoveryUrl": "",
      "text": "The request completed successfully."
   }]
}
```

/cmms

Use this REST API to retrieve properties for all Chassis Management Modules (CMMs). Each chassis contains up to two CMMs.

HTTP methods

GET

GET /cmms

Use this method retrieve the properties for all CMMs.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/cmms`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
cmmList	Array	List of CMMs
See GET /cmms/*{uuid_list}*	Object	Detailed information for each CMM

The following example is returned if the request is successful.


```
{
"cmmList": [{
   "accessState": "Online",
   "backedBy": "real",
   "cmmDisplayName": "SN#Y033BG24B009",
   "cmmHealthState": "Non-Critical",
   "dataHandle": 1442012140925,
   "description": "Chassis Management Module",
   "dnsHostnames": ["demoblue1.labs.lenovo.com"],
   "domainName": "labs.lenovo.com",
   "errorFields": [],
   "excludedHealthState": "Warning",

   "firmware": [{
      "build": "2PET27F",
      "date": "2015-04-08T04:00:00Z",
      "name": "CMM firmware",
      "role": "",
      "status": "",
      "type": "CMM firmware",
      "version": "2.5.3"
   }],
   "FRU": "68Y7032",
   "fruSerialNumber": "Y033BG24B009",
   "hostConfig": [{
      "DDNSenabled": false,
      "DNSenabled": true,
      "IPversionPriority": "IPv4ThenIPv6",
      "priIPv4userDNSserver": "10.240.0.10"
      "priIPv6userDNSserver": "0:0:0:0:0:0:0:0",
      "secIPv4userDNSserver": "10.240.0.11",
      "secIPv6userDNSserver": "0:0:0:0:0:0:0:0",
      "terIPv4userDNSserver": "0.0.0.0",
      "terIPv6userDNSserver": "0:0:0:0:0:0:0:0",
```

```
}],
"hostname": "demoblue1",
"ipInterfaces": [{
   "IPv4assignments": [{
      "address": "10.240.70.134",
      "gateway": "10.240.70.1",
      "id": 2,
      "subnet": "255.255.254.0",
      "type": "CONFIGURED"
   },
   {
      "address": "10.240.70.134",
      "gateway": "10.240.70.1",
      "id": 2,
      "subnet": "255.255.254.0",
      "type": "INUSE"
   }],
   "IPv4DHCPmode": "STATIC_ONLY",
   "IPv4enabled": true,
   "IPv6assignments": [{
      "address": "fe80:0:0:0:5ef3:fcff:fe25:ea57",
      "gateway": "0:0:0:0:0:0:0:0",
      "id": 1,
      "prefix": 64,
      "scope": "LinkLocal",
      "source": "Other",
      "type": "INUSE"
   },
   {
      "address": "0:0:0:0:0:0:0:0",
      "gateway": "0:0:0:0:0:0:0:0",
      "id": 2,
      "prefix": 0,
      "scope": "Global",
      "source": "Static",
      "type": "CONFIGURED"
   }],
   "IPv6DHCPenabled": false,
   "IPv6enabled": true,
   "IPv6statelessEnabled": true,
   "IPv6staticEnabled": false
   "label": "External",
   "name": "eth0",
}],
"ipv4Addresses": ["10.240.70.134"],
"ipv6Addresses": ["fe80:0:0:0:5ef3:fcff:fe25:ea57"],
"leds": [{
   "color": "Blue",
   "location": "FrontPanel",
   "name": "Location",
   "state": "Off"
},
{
   "color": "Amber",
   "location": "FrontPanel",
   "name": "FAULT",
   "state": "On"
},
{
   "color": "Amber",
   "location": "FrontPanel",
```

```
      "name": "Information",
      "state": "On"
   }],
   "macAddresses": ["5C:F3:FC:25:EA:57"],
   "machineType": "",
   "mgmtProcIPaddress": "10.240.70.134",
   "model": "",
   "name": "SN#Y033BG24B009",
   "overallHealthState": "Warning",
   "parent": {
      "uri": "chassis/AB582DD17E604572A4679E24BE2938DE",
      "uuid": "AB582DD17E604572A4679E24BE2938DE"
   },
   "partNumber": "00D7179",
   "powerAllocation": {
      "maximumAllocatedPower": 20,
      "minimumAllocatedPower": 20
   },
   "productId": "432",
   "role": "primary",
   "serialNumber": "",
   "slots": [1],
   "type": "CMM",
   "uri": "cmm/2A14E8448B5B11E1B942C430BE6956C4"
   "userDefinedName": "CMM1",
   "userDescription": "",
   "uuid": "2A14E8448B5B11E1B942C430BE6956C4",
}]
}
```

/cmms/*{uuid}*

Use this REST API to retrieve or modify the properties for a specific Chassis Management Module (CMM). Each chassis contains up to two CMMs.

HTTP methods

GET, PUT

GET /cmms/*{uuid_list}*

Use this method retrieve the properties for one or more specific CMMs.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/cmms/{uuid_list}`

where *{uuid_list}* is one or more UUIDs, separated by a comma, of the CMMs to be retrieved. To obtain the CMM UUIDs, use the GET /cmms method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
accessState	String	Access state of the chassis. This can be one of the following values. • **Online** • **Offline** • **Partial** • **Pending** • **Unknown**
backedBy	String	Indicates whether the data is from a real or demo server. This can be one of the following values. • **real**. The inventory describes real hardware. • **demo**. The inventory describes demo (mock) hardware. • **proxy**. A proxy is temporarily serving to provide the inventory.

Attributes	Type	Description
cmmDisplayName	String	Display name provided by the CMM
cmmHealthState	String	Health summary that corresponds to the highest event severity of all the devices. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
dataHandle	Long	Time stamp of the last status update
description	String	Description that was provided by the CMM
dnsHostnames	Array of strings	List of DNS hostnames
domainName	String	User-defined domain name
errorFields	Array of objects that contain *{string, error-Code}*	Error code. This can be one of the following values. • **FETCH_SUCCESS** • **FETCH_FAILED** • **NO_CONNECTOR** • **FATAL_EXCEPTION** • **NETWORK_FAIL**
excludedHealthState	String	Highest severity alert with exclusions. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
firmware	Array	CMM firmware details
build	String	Firmware build
date	String	Firmware date
name	String	Firmware name
role	String	Firmware role
status	String	Firmware status
type	String	Firmware type
version	String	Firmware version
FRU	String	CMM FRU part number
fruSerialNumber	String	CMM FRU serial number
hostConfig	Array	Information about host configuration

Attributes	Type	Description
DDNSenabled	Boolean	Identifies whether dynamic DNS enabled. This can be one of the following values. • **true**. Dynamic DNS is enabled. • **false**. Dynamic DNS is disabled.
DNSenabled	Boolean	Identifies whether DNS enabled. This can be one of the following values. • **true**. DNS is enabled. • **false**. DNS is disabled.
IPversionPriority	String	IP version priority. This can be one of the following values. • **IPv6ThenIPv4** • **IPv4ThenIPv6**
priIPv4userDNSserver	String	Primary user assigned IPv4 DNS server
priIPv6userDNSserver	String	Primary user assigned IPv6 DNS server
secIPv4userDNSserver	String	Secondary user assigned IPv4 DNS server
secIPv6userDNSserver	String	Secondary user assigned IPv6 DNS server
terIPv4userDNSserver	String	Tertiary user assigned IPv4 DNS server
terIPv6userDNSserver	String	Ternary user assigned IPv6 DNS server
hostname	String	User-defined hostname
ipInterfaces	Array	Information about the CMM IP interfaces
IPv4assignments	Array	Information about IPV4 assignments
address	String	IP address
gateway	String	Gateway
id	Integer	IPv4 assignment ID
subnet	String	Subnet mask
type	String	IPv4 assignment type. This can be one of the following values. • **INUSE** • **CONFIGURED** • **ALIAS** • **UNKNOWN**
IPv4DHCPmode	String	IPv4 assignment method. This can be one of the following values. • **STATIC_ONLY** • **DHCP_ONLY** • **DHCP_THEN_STATIC** • **UNKNOWN**
IPv4enabled	Boolean	Identifies whether IPv4 is enabled. This can be one of the following values. • **true**. IPv4 is enabled. • **false**. IPv4 is disabled.
IPv6assignments	Array	Information about IPV6 assignments
address	String	IPv6 address
gateway	String	Gateway
id	Integer	IPv6 assignment ID
prefix	Integer	IPv6 prefix

Attributes	Type	Description
scope	String	IPv6 assignment scope. This can be one of the following values. • **Global** • **LinkLocal** • **Unknown**
source	String	IPv6 assignment source. This can be one of the following values. • **DHCP** • **Statelesss** • **Static** • **Other** • **Unknown**
type	String	IPv6 assignment type. This can be one of the following values. • **INUSE** • **CONFIGURED** • **ALIAS** • **UNKNOWN**
IPv6DHCPenabled	Boolean	Identifies whether IPv6 DHCP is enabled. This can be one of the following values. • **true**. IPv6 DHCP is enabled. • **false**. IPv6 DHCP is disabled.
IPv6enabled	Boolean	Identifies whether IPv6 is enabled. This can be one of the following values. • **true**. IPv6 is enabled. • **false**. IPv6 is disabled.
IPv6statelessEnabled	Boolean	Identifies whether IPv6 stateless is enabled. This can be one of the following values. • **true**. IPv6 stateless is enabled. • **false**. IPv6 stateless is disabled.
IPv6staticEnabled	Boolean	Identifies whether IPv6 static is enabled. This can be one of the following values. • **true**. IPv6 static is enabled. • **false**. IPv6 static is disabled.
label	String	Label
name	String	Name
ipv4Addresses	Array of strings	List of IPv4 addresses
ipv6Addresses	Array of strings	List of IPv6 addresses
leds	Object	Information about CMM LEDs
color	String	LED color. This can be one of the following values. • **Red** • **Amber** • **Yellow** • **Green** • **Blue** • **Unknown**

Attributes	Type	Description
location	String	LED location. This can be one of the following values. • **Front panel** • **Lightpath Card** • **Planar** • **FRU** • **Rear Panel** • **Unknown**
name	String	LED name
state	String	LED state. This can be one of the following values. • **Off** • **On** • **Blinking** • **Unknown**
macAddresses	Array of strings	List of MAC addresses
machineType	String	CMM machine type
manufacturer	String	Manufacturer
manufacturerId	String	Manufacturer ID
mgmtProcIPaddress	String	IP address used by the Lenovo XClarity Administrator to manage this resource
model	String	CMM model
name	String	Name that is displayed in the user interface for this device The value of this attribute is determined by **preferredDisplayName** attribute in the GET /aicc method. For example, if the **preferredDisplayName** attribute is set to “hostname,” then the value for this **name** attribute is the same as the **hostname** attribute in the GET /aicc method.
overallHealthState	String	Highest severity of all alerts. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
parent	Object	
uri	String	Parent URI
uuid	String	Parent UUID
partNumber	String	CMM part number
powerAllocation	Object	
maximumAllocatedPower	Long	Maximum power that is allocated
minimumAllocatedPower	Long	Minimum power that is allocated
productID	String	CMM product ID

Attributes	Type	Description
role	String	Role of the CMM. This can be one of the following values. • primary • backup
serialNumber	String	CMM serial number
slots	Integer	CMM primary slot
type	String	Resource type. This value is always “CMM”
uri	String	URI
userDefinedName	String	User-defined name for the device
userDescription	String	Description that was defined by the user
uuid	String	UUID

The following example is returned if the request is successful.


```
{
   "cmmList": [{
   "accessState": "Online",
   "backedBy": "real",
   "cmmDisplayName": "SN#Y010BG494063",
   "cmmHealthState": "Non-Critical",
   "dataHandle": 1548164031434,
   "description": "Chassis Management Module 2",
   "dnsHostnames": ["betacmm12.labs.lenovo.com","fd55:faaf:e1ab:2021:42f2:e9ff:febf:4e54"],
   "domainName": "labs.lenovo.com",
   "errorFields": [],
   "excludedHealthState": "Warning",
   "firmware": [{
      "build": "1AON24A",
      "date": "2018-09-18T04:00:00Z",
      "name": "CMM firmware",
      "role": "",
      "status": "",
      "type": "CMM firmware",
      "version": "2.0.0"
   }],
   "FRU": "00FG678",
   "fruSerialNumber": "Y010BG494063",
   "hostConfig": [],
   "hostname": "betacmm12",
   "ipInterfaces": [{
      "IPv4assignments": [{
      "address": "10.243.2.118",
      "gateway": "10.243.0.1",
      "id": 2,
      "subnet": "255.255.224.0",
      "type": "INUSE"
      }],
      "IPv4DHCPmode": "STATIC_ONLY",
      "IPv4enabled": true,
      "IPv6assignments": [{
      "address": "0:0:0:0:0:0:0:0",
      "gateway": "0:0:0:0:0:0:0:0",
      "id": 2,
      "prefix": 0,
      "scope": "Global",
```

```
      "source": "Static",
      "type": "CONFIGURED"
      },
      ...,
      {
      "address": "fe80:0:0:0:42f2:e9ff:febf:4e54",
      "gateway": "0:0:0:0:0:0:0:0",
      "id": 1,
      "prefix": 64,
      "scope": "LinkLocal",
      "source": "Other",
      "type": "INUSE"
      }],
      "IPv6DHCPenabled": true,
      "IPv6enabled": true,
      "IPv6statelessEnabled": true,
      "IPv6staticEnabled": false,
      "label": "External",
      "name": "eth0"
   }],
   "ipv4Addresses": ["10.243.2.118"],
   "ipv6Addresses": ["fe80:0:0:0:42f2:e9ff:febf:4e54","fd55:faaf:e1ab:2021:42f2:e9ff:febf:4e54"],
   "leds": [{
      "name": "FAULT",
"state": "Off",
"color": "Amber",
      "location": "FrontPanel"
   }],
   "macAddresses": ["40:F2:E9:BF:4E:54"],
   "machineType": "",
   "manufacturer": "LNVO",
   "manufacturerId": "19046",
   "mgmtProcIPaddress": "10.243.2.118",
   "model": "",
   "name": "SN#Y010BG494063",
   "overallHealthState": "Warning",
   "parent": {
      "uri": "chassis/78FB1DD279994B95BDBC4F75F063D241",
      "uuid": "78FB1DD279994B95BDBC4F75F063D241"
   },
   "partNumber": "00KH719",
   "powerAllocation": {
      "maximumAllocatedPower": 20,
      "minimumAllocatedPower": 20
   },
   "productId": "1032",
   "role": "primary",
   "serialNumber": "",
   "slots": [2],
   "type": "CMM",
   "uri": "cmm/FD98426A35C711E4972EE04173533818",
   "userDefinedName": "SN#Y010BG494063",
   "userDescription": "",
   "uuid": "FD98426A35C711E4972EE04173533818"
}
```


PUT /cmms/*{uuid}*

Use this method to modify properties , perform a power operation, or refresh inventory for a specific CMM.

The request body differs depending on the action that you want to perform. You can use this PUT method to perform the following management actions.

- Table 16 “Modify CMM properties” on page 214
- Table 17 “Modifying the power state” on page 216
- Table 18 “Refresh the inventory” on page 216

If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/cmms/{uuid}`

where *{uuid}* is the UUID of the CMM. To obtain the CMM UUID, use the GET /cmms method.

Query parameters

Attributes	Required / Optional	Description
synchronous=*{value}*	Optional	When modifying attributes, indicates when the job ID is returned • **true**. (default) Returns the job ID and job status after the job is complete. • **false**. Returns the job ID immediately. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. **Note:** This query parameter applies only when one or more property parameters are specified in the request body.

Request body

You can specify attributes from one of the following tables in each request.

Table 16. Modify CMM properties

Attributes	Required / Optional	Type	Description
domainName	Optional	String	Domain name
hostConfig	Optional	Array	
DDNSenabled	Optional	Boolean	Identifies whether Dynamic DNS is enabled. This can be one of the following values. • **true**. Dynamic DNS is enabled • **false**. Dynamic DNS is disabled

Table 16. Modify CMM properties (continued)

Attributes	Re-quired / Optional	Type	Description
DNSenabled	Optional	Boolean	Identifies whether DNS is enabled. This can be one of the following values. • **true**. DNS is enabled • **false**. DNS is disabled
globalIPv6enabled	Optional	String	Global IPv6 enablement
IPversionPriority	Optional	String	IP version priority. This can be one of the following values. • **IPv6ThenIPv4** • **IPv4ThenIPv6**
priIPv4userDNSserver	Optional	String	Primary user assigned IPv4 DNS server
priIPv6userDNSserver	Optional	String	Primary user assigned IPv6 DNS server
secIPv4userDNSserver	Optional	String	Secondary user assigned IPv4 DNS server
secIPv6userDNSserver	Optional	String	Secondary user assigned IPv6 DNS server
terIPv4userDNSserver	Optional	String	Ternary user assigned IPv4 DNS server
terIPv6userDNSserver	Optional	String	Ternary user assigned IPv6 DNS server
hostname	Optional	String	Hostname
ipInterfaces	Optional	Array	Information about the CMM IP addresses
IPv4assignments	Optional	Array	Information about IPv4 assignments
address	Optional	String	IPv4 address
gateway	Optional	String	IPv4 gateway
id	Required	Integer	IPv4 assignment ID
subnet	Optional	String	IPv4 subnet mask
IPv4DHCPmode	Optional	String	IP address assignment method. This can be one of the following values. • **STATIC_ONLY** • **DHCP_ONLY** • **DHCP_THEN_STATIC** • **UNKNOWN**
IPv4enabled	Optional	Boolean	Identifies whether IPv4 is enabled. This can be one of the following values. • **true**. IPv4 is enabled • **false**. IPv4 is disabled
IPv6assignments	Optional	Array	Information about IPv6 assignments
address	Optional	String	IPv6 address
gateway	Optional	String	IPv6 gateway
id	Required	Integer	IPv6 assignment ID
prefix	Optional	Integer	IPv6 prefix
IPv6DHCPenabled	Optional	Boolean	Identifies whether IPv6 DHCP is enabled. This can be one of the following values. • **true**. IPv6 DHCP is enabled • **false**. IPv6 DHCP is disabled

Table 16. Modify CMM properties (continued)

Attributes		Required / Optional	Type	Description
	IPv6enabled	Optional	Boolean	Identifies whether IPv6 is enabled. This can be one of the following values. • **true**. IPv6 is enabled • **false**. IPv6 is disabled
	IPv6statelessEnabled	Optional	Boolean	Identifies whether IPv6 stateless is enabled. This can be one of the following values. • **true**. IPv6 stateless is enabled • **false**. IPv6 stateless is disabled
	IPv6staticEnabled	Optional	Boolean	Identifies whether IPv6 static is enabled. This can be one of the following values. • **true**. IPv6 static is enabled • **false**. IPv6 static is disabled
	name	Required	String	IP Interface name

The following examples show how to use the PUT method to change CMM configuration settings:

```
{
    "contact": "new contact",
    "hostname":"",
    "location": {
        "location":"new location"
    }
}
```

Table 17. Modifying the power state

Attributes	Required / Optional	Type	Description
powerState	Optional	String	Performs a power operation on the CMM. This can be one of the following values. • **reset**. Restart the CMM. • **virtualReseat**. Simulates removing power from the bay

The following example restarts the CMM.

```
{
   "powerState":"reset"
}
```

Table 18. Refresh the inventory

Attributes	Required / Optional	Type	Description
refreshInventory	Optional	String	Refreshes inventory for the CMM

The following example refreshes inventory for the target CMM.

```
{
   "refreshInventory": "true"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/fans

Use this REST API to retrieve properties for all Flex System fans.

HTTP methods

GET

GET /fans

Use this method to return properties for all Flex System fans.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/fans`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=*<attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
fanList	Array	Information about each fan
See GET /fans/*{uuid}*	Objects	Detailed information about a specific fan

The following example is returned if the request is successful.

```
{
"fanList": [{
   "cmmDisplayName": "Fan 01",
```

```
   "cmmHealthState": "Normal",
   "dataHandle": 0,
   "description": "IBM Fan Pack",
   "errorFields": [],
   "firmware": [{
      "build": "",
      "date": "",
      "name": "Fan Controller",
      "role": "",
      "status": "",
      "type": "Fan Controller",
      "version": "226"
   }],
   "FRU": "88Y6685",
   "fruSerialNumber": "YK10JPB69H61",
   "hardwareRevision": "4.0",
   "leds": [{
      "color": "Amber",
      "location": "FrontPanel",
      "name": "FAULT",
      "state": "Off"
   }],
   "machineType": "",
   "manufactureDate": "2511",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "model": "",
   "name": "Fan 01",
    "parent": {
      "uri": "chassis/FBEF740B178F4EFAA846E7225EE256DC",
      "uuid": "FBEF740B178F4EFAA846E7225EE256DC"
   },
   "partNumber": "88Y6691",
   "posID": "373",
    "powerAllocation": {
      "maximumAllocatedPower": 0,
      "minimumAllocatedPower": 0
   },
   "powerState": "Unknown",
   "productId": "342",
   "productName": "80mm Fan Pack for ITE Cooling",
    "serialNumber": "",
   "slots": [1],
   "type": "Fan",
   "uri": "fan/192C7661981E11E091C2C0AC11247C9B",
   "userDescription": "",
   "uuid": "192C7661981E11E091C2C0AC11247C9B",
   "vpdID": "11"
}]
}
```


/fans/*{uuid}*

Use this REST API to retrieve properties for a specific Flex System fan.

HTTP methods

GET

GET /fans/*{uuid}*

Use this method to return properties for a specific Flex System fan.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/fans/{uuid}`

where *{uuid}* is the UUID of the fan to be retrieved. To obtain the fan UUID, use the GET /fans method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=*<attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
cmmDisplayName	String	Fan name provided by the CMM
cmmHealthState	String	Health summary that corresponds to the highest event severity of all fans. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
dataHandle	Long	
description	String	Description provided by the CMM
errorFields	Array of objects that contain *{string, error-Code}*	Error codes. This can be one of the following values. • **FETCH_SUCCESS** • **FETCH_FAILED** • **NO_CONNECTOR** • **FATAL_EXCEPTION** • **NETWORK_FAIL**
firmware	Array	Information about fan firmware
build	String	The firmware build
date	String	The firmware date
name	String	The firmware name
role	String	The firmware role
status	String	The firmware status
type	String	The firmware type
version	String	The firmware version
FRU	String	FRU part number
fruSerialNumber	String	FRU serial number
hardwareRevision	String	Hardware revision
LEDs	Array	Information about fan LEDs
color	String	LED color. This can be one of the following values. • **Red** • **Amber** • **Yellow** • **Green** • **Blue** • **Unknown**

Attributes	Type	Description
location	String	LED location. This can be one of the following values. • **Front panel** • **Lightpath Card** • **Planar** • **FRU** • **Rear Panel** • **Unknown**
name	String	LED name
state	String	LED state. This can be one of the following values. • **Off** • **On** • **Blinking** • **Unknown**
machine type	String	Machine type
manufactureDate	String	Manufacture date
manufacturer	String	Manufacturer
manufacturerID	String	Manufacturer ID
model	String	Model
name	String	Name that is displayed in the user interface for this device
parent	Object	
uri	String	Parent URI
uuid	String	Parent UUID
partNumber	String	Part number
posID	String	Position ID
powerAllocation	Object	Information about power allocation
maximumAllocatedPower	Long	Maximum power allocated to the fan
minimumAllocatedPower	Long	Minimum power allocated to the fa.
powerState	String	Current power state of the fan. This can be one of the following values. • **Off** • **On** • **ShuttingDown** • **Standby** • **Hibernate** • **Unknown**
productID	String	Product ID
productName	String	Product name
serialNumber	String	Serial number
slots	Integer	Fan primary slot
type	String	Resource type. This value is always “Power Supply.”
uri	String	URI
userDescription	String	User description

Attributes	Type	Description
uuid	String	UUID
vpdID	String	VPD ID

The following example is returned if the request is successful.


```
{
   "cmmDisplayName": "Fan 01",
   "cmmHealthState": "Normal",
   "dataHandle": 0,
   "description": "IBM Fan Pack",
   "errorFields": [],
   "firmware": [{
      "build": "",
      "date": "",
      "name": "Fan Controller",
      "role": "",
      "status": "",
      "type": "Fan Controller",
      "version": "226"
   }],
   "FRU": "88Y6685",
   "fruSerialNumber": "YK10JPB69H61",
   "hardwareRevision": "4.0",
   "leds": [{
      "color": "Amber",
      "location": "FrontPanel",
      "name": "FAULT",
      "state": "Off"
   }],
   "machineType": "",
   "manufactureDate": "2511",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "model": "",
   "name": "Fan 01",
    "parent": {
      "uri": "chassis/FBEF740B178F4EFAA846E7225EE256DC",
      "uuid": "FBEF740B178F4EFAA846E7225EE256DC"
   },
   "partNumber": "88Y6691",
   "posID": "373",
    "powerAllocation": {
      "maximumAllocatedPower": 0,
      "minimumAllocatedPower": 0
   },
   "powerState": "Unknown",
   "productId": "342",
   "productName": "80mm Fan Pack for ITE Cooling",
    "serialNumber": "",
   "slots": [1],
   "type": "Fan",
   "uri": "fan/192C7661981E11E091C2C0AC11247C9B",
   "userDescription": "",
   "uuid": "192C7661981E11E091C2C0AC11247C9B",
   "vpdID": "11"
}
```

/fanMuxes

Use this REST API to retrieve information about all Flex System fan logic modules (called *fan muxes*). Fan muxes enable the CMM to monitor the chassis fans.

HTTP methods

GET

GET /fanMuxes

Use this method to return information about all Flex System fan logic modules (called *fan muxes*), including properties and metrics for each of the fan logic modules.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/fanMuxes`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
fanMuxList	Array	List of all fan muxes
See GET /fanMuxes/*{uuid}*	Object	Detailed information about each individual fan mux

The following example is returned if the request is successful.


```
{
   "fanMuxList": [{
      "cmmDisplayName": "Fan Logic 01",
      "cmmHealthState": "Major-Failure",
      "dataHandle": 0,
      "description": "Fan Logic Module",
      "FRU": "81Y2912",
      "fruSerialNumber": "31gfbdRUKGmS",
      "hardwareRevision": "3.1",
      "leds": [{
         "color": "Amber",
         "location": "FrontPanel",
         "name": "FAULT",
         "state": "On"
      }],
      "machineType": "",
      "manufactureDate": "1011",
      "manufacturer": "IBM",
      "manufacturerId": "20301",
      "model": "",
      "name": "Fan Logic 01",
      "parent": {
         "uri": "chassis/48331A223BF34FBA90732B379B837B9C",
         "uuid": "48331A223BF34FBA90732B379B837B9C"
      },
      "partNumber": "49Y3309",
      "productId": "338",
      "productName": "IBM Accipiter Fan Logic Mux Card",
      "serialNumber": "",
      "slots": [1],
      "status": "Major-Failure",
      "type": "FanMux",
      "uri": "fanMux/5D3EC1A4F2064A2981457AC9A06B56F9",
      "uuid": "5D3EC1A4F2064A2981457AC9A06B56F9"
   },
   {
      "cmmDisplayName": "Fan Logic 02",
      "cmmHealthState": "Major-Failure",
      "dataHandle": 0,
      "description": "Fan Logic Module",
```

```
      "FRU": "81Y2912",
      "fruSerialNumber": "fL3eXhaYDWoU",
      "hardwareRevision": "3.1",
      "leds": [{
         "color": "Amber",
         "location": "FrontPanel",
         "name": "FAULT",
         "state": "On"
      }],
      "manufactureDate": "1011",
      "manufacturer": "IBM",
      "manufacturerId": "20301",
      "machineType": "",
      "model": "",
      "name": "Fan Logic 02",
      "parent": {
         "uri": "chassis/48331A223BF34FBA90732B379B837B9C",
         "uuid": "48331A223BF34FBA90732B379B837B9C"
      },
      "partNumber": "49Y3309",
      "productId": "338",
      "productName": "IBM Accipiter Fan Logic Mux Card",
      "serialNumber": "",
      "slots": [2],
      "status": "Major-Failure",
      "type": "FanMux",
      "uri": "fanMux/9D83BAB5D9AA4C1FA8D2E53ADED5DA08",
      "uuid": "9D83BAB5D9AA4C1FA8D2E53ADED5DA08"
   }]
}
```


/fanMuxes/*{uuid}*

Use this REST API to retrieve information about a specific Flex System fan logic module (called a *fan mux*). *Fan muxes* enable the CMM to monitor the chassis fans.

HTTP methods

GET

GET /fanMuxes/*{uuid}*

Use this method to return properties and metrics for a specific Flex System fan logic module (fan mux).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/fanMuxes/{uuid}`

where *{uuid}* is the UUID of the fan to be retrieved. To obtain the fan UUID, use the GET /fanMuxes method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
cmmDisplayName	String	Fan mux name that is provided by the CMM
cmmHealthState	String	Health summary that corresponds to the highest event severity of all the devices. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**

Attributes	Type	Description
dataHandle	Long	Time stamp of the last status update
description	String	Description provided by the CMM
FRU	String	FRU part number
fruSerialNumber	String	FRU serial number
hardwareRevision	String	Hardware revision
leds	Array	Information about fan mux LEDs
color	String	LED color. This can be one of the following values. • **Red** • **Amber** • **Yellow** • **Green** • **Blue** • **Unknown**
location	String	LED location. This can be one of the following values. • **Front panel** • **Lightpath Card** • **Planar** • **FRU** • **Rear Panel** • **Unknown**
name	String	LED name
state	String	LED state. This can be one of the following values. • **Off** • **On** • **Blinking** • **Unknown**
machineType	String	Machine type
manufacturer	String	Manufacturer
manufactureDate	String	Manufacture date
manufacturerID	String	Manufacturer ID
model	String	Fan mux model
name	String	Name that is displayed in the user interface for this device
parent	Object	Parent device
uri	String	Parent URI
uuid	String	Parent UUID
partNumber	String	Part number
productID	String	Product ID
productName	String	Product name
serialNumber	String	Serial number
slots	Integer	Primary slot

Attributes	Type	Description
status	String	Status. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
type	String	Resource type. This value is always “FanMux.”
uri	String	URI
uuid	String	UUID

The following example is returned if the request is successful.


```
{
   "cmmDisplayName": "Fan Logic 01",
   "cmmHealthState": "Major-Failure",
   "dataHandle": 0,
   "description": "Fan Logic Module",
   "FRU": "81Y2912",
   "fruSerialNumber": "31gfbdRUKGmS",
   "hardwareRevision": "3.1",
   "leds": [{
      "color": "Amber",
      "location": "FrontPanel",
      "name": "FAULT",
      "state": "On"
   }],
   "machineType": "",
   "manufactureDate": "1011",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "model": "",
   "name": "Fan Logic 01",
   "parent": {
      "uri": "chassis/48331A223BF34FBA90732B379B837B9C",
      "uuid": "48331A223BF34FBA90732B379B837B9C"
   },
   "partNumber": "49Y3309",
   "productId": "338",
   "productName": "IBM Accipiter Fan Logic Mux Card",
   "serialNumber": "",
   "slots": [1],
   "status": "Major-Failure",
   "type": "FanMux",
   "uri": "fanMux/5D3EC1A4F2064A2981457AC9A06B56F9",
   "uuid": "5D3EC1A4F2064A2981457AC9A06B56F9"
}
```


/nodes

Use this REST API to retrieve properties for all servers and Flex System storage devices.

HTTP methods

GET

GET /nodes

Use this method to return properties for all servers, Flex System storage devices, and Flex System storage controllers (canisters).

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/nodes
```

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
formatType=*{type}*	Optional	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv** If the format type is not specified, JSON format is returned.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.
mgmtProcType	Optional	Returns a response that includes servers with the specified baseboard management controller. This can be one of the following values. • **FSP** • **IMM2** • **lenovo-AMI-controller** • **XCC** • **XCC2** • **UNKNOWN**
status=*{string}*	Optional	Status. This can be one of the following values. • **unmanaged**. Returns unmanaged nodes only • **managed**. Returns managed nodes only

The following example returns a CSV file that contains information about all managed servers and storage devices.

```
GET https://192.0.2.0/nodes?status=managed&formatType=csv
```

The following example returns only the UUID and type of management controller for all managed servers with XCC2.

```
GET https://192.0.2.0/nodes?status=managed&mgmtProcType=XCC2
&includeAttributes=uuid,mgmtProcType
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Note: GET /nodes returns the **canister** attribute as a child under the **enclosure** attribute and also as a peer to the **enclosure** attribute (in duplication).For GET /nodes/*{uuid_list}*, the **canister** attribute is only returned as a child under the **enclosure** attribute.

Attributes	Type	Description
nodeList	Array	List of all servers and storage devices
See GET /nodes/*{uuid_list}*	Object	Detailed information about the individual server or storage device

The following example response lists information about a System x server in JSON format.

```
{ "nodeList": [
{
    "accessState": "Online",
    "accountLockoutPeriod": 1,
    "activationKeys": [{
        "description": "Lenovo XClarity Controller 2 Platinum Upgrade",
        "keyExpirationDate": "",
        "keyFeatureType": 74,
        "keyIdentiferList": [{
            "keyIdentifierType": "MT",
            "keyIdentifier": "7D75SR650R112"
        }],
        "keyStatus": "VALID",
        "keyUseCount": 0,
        "keyUseLimit": 0,
        "uuid": ""
    }],
```

```
"addinCards": [{
    "class": "Unclassified device",
    "firmware": [{
        "build": "0",
        "classifications": [13],
        "date": "",
        "name": "Gen5 Riser1 LP Retimer",
        "revision": "0",
        "softwareID": "1D494050",
        "role": "",
        "status": "Active",
        "type": "Software Bundle",
        "version": "0.0.0"
    }],
    "fodUniqueID": "",
    "FRU": "",
    "fruSerialNumber": "",
    "isAddOnCard": true,
    "isAgentless": false,
    "isPLDMUpdateSupported": true,
    "manufacturer": "Lenovo",
    "name": "Gen5 Riser1 LP Retimer",
    "partNumber": "STA7A95479",
    "pciBusNumber": "0",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "0",
    "pciRevision": "0",
    "pciSubID": "0",
    "pciSubVendorID": "0",
    "portInfo": {},
    "posID": "0",
    "productName": "Gen5 Riser1 LP Retimer",
    "slotName": "PCIe 4",
    "slotNumber": "4",
    "slotSupportsHotPlug": "false",
    "vpdID": "0"
},
...,
{
    "class": "Network controller",
    "firmware": [{
        "build": "0",
        "classifications": [13],
        "date": "",
        "name": "Firmware Bundle",
        "role": "",
        "revision": "0",
        "softwareID": "17AA4104",
        "status": "Active",
        "type": "Software Bundle",
        "version": "222.0.2.1"
    }],
    "fodUniqueID": "",
    "FRU": "01PE761",
    "fruSerialNumber": "L0NV1A2004Y",
    "isAddOnCard": true,
    "isAgentless": false,
    "isPLDMUpdateSupported": false,
    "pciBusNumber": "22",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "3",
```

```
    "pciRevision": "1",
    "pciSegmentNumber": "0",
    "pciSubID": "4104",
    "pciSubVendorID": "17aa",
    "manufacturer": "Broadcom Limited",
    "name": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
    "partNumber": "SN37A28309",
    "portInfo": {
        "physicalPorts": [{
            "logicalPorts": [{
                "addresses": "e4:3d:1a:61:88:8f",
                "logicalPortIndex": 1,
                "portNumber": 1,
                "portType": "ETHERNET",
                "vnicMode": false
            }],
            "peerBay": 0,
            "physicalPortIndex": 4,
            "portNumber": 4,
            "portType": "ETHERNET",
            "speed": -1.0,
            "status": "Down"
        }]
    },
    "posID": "1657",
    "productName": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
    "slotName": "PCIe 13",
    "slotNumber": "13",
    "slotSupportsHotPlug": "false",
    "vpdID": "14e4"
}],
"addinCardSlots": 0,
"arch": "x86",
"assetTag": "",
"backedBy": "real",
"bladeState": 0,
"bmuParamObject": null,
    "uri": "nodes/40BDB5F8D609B801C183337C180D3F29/bootOrder",
    "bootOrderList": [{
        "bootType": "BootOrder",
        "currentBootOrderDevices": ["Red Hat Enterprise Linux"],
        "possibleBootOrderDevices": ["Red Hat Enterprise Linux","CD/DVD Rom","Hard Disk",
                                     "Network","USB Storage"]
    },
    ...,
    {
        "bootType": "CDDVDROMBootOrder",
        "currentBootOrderDevices": [],
        "possibleBootOrderDevices": []
    }]
},
"bootMode": {
    "currentValue": "UEFI Mode",
    "possibleValues": ["UEFI Mode","Legacy Mode"]
},
"bootOrder": {
"bundleRepoAvailableSpaceInKB": 1951586,
"cimEnabled": false,
"cmmDisplayName": "Management Controller UUID-40BDB5F8D609B801C183337C180D3F29",
"cmmHealthState": "Normal",
"complexID": -1,
```

```
"contact": "",
"dataHandle": 1688376857592,
"description": "This resource is used to represent a chassis or other physical enclosure for a Redfish implementation.",
"deviceDrivers": null,
"diskDriveSensorInfo": ["Drive 0","Drive 1","Drive 2","Drive 3","Drive 4","Drive 5","Drive 6",
                        "Drive 7","Drive 8","Drive 9","Drive 10","Drive 11","Drive 12",
                        "Drive 13","Drive 14","Drive 15","Ext Drive","Drive Mismatch",
                        "Drive Key Fault"],
"domainName": "",
"driveBays": 2,
"drives": [],
"embeddedHypervisorPresence": false,
"encapsulation": {
    "encapsulationMode": "normal"
},
"errorFields": [],
"excludedHealthState": "Normal",
"expansionCards": [],
"expansionCardSlots": 0,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [{
    "deviceId": 84,
    "entityId": 15,
    "fruNumber": "02YH952",
    "name": "HDD_BP_2",
    "partNumber": "STA7A43893"
    "posID": 145,
    "productId": 0,
    "serialNumber": "R4SH29D0024",
    "vpdID": 112,
},
{
    "deviceId": 83,
    "entityId": 15,
    "fruNumber": "02YE087",
    "name": "HDD_BP_1",
    "partNumber": "SC57A26298"
    "posID": 144,
    "productId": 0,
    "serialNumber": "R5SH235006X",
    "vpdID": 112,
}],
"fans": [{
    "description": "Fan Fan 4 Front Tach",
    "healthState": "Normal",
    "name": "Fan 4 Front Tach",
    "slot": "4",
    "slots": 4,
    "speed": 6642,
    "status": "OK"
},
...,
{
    "description": "Fan Fan 1 Rear Tach",
    "healthState": "Normal",
    "name": "Fan 1 Rear Tach",
    "slot": "1",
    "slots": 1,
    "speed": 6300,
    "status": "OK"
```

```
}],
"FeaturesOnDemand": {
    "features": ["RDOC","REMOTE MEDIA","REMOTE CONTROL 6 USERS"],
    "tierLevel": 3
},
"firmware": [{
    "build": "*",
    "classifications": [],
    "date": "",
    "name": "Firmware:LXPM-LinuxDrivers",
    "revision": "*",
    "role": "Primary",
    "status": "Active",
    "type": "LXPMLinuxDriver",
    "version": "*"
},
...,
{
    "build": "*",
    "classifications": [],
    "date": "",
    "name": "Firmware:LXPM-WindowsDrivers",
    "revision": "*",
    "role": "Primary",
    "status": "Active",
    "type": "LXPMWindowsDriver",
    "version": "*"
}],
"flashStorage": [],
"FQDN": "Shanghai-SR650V3",
"FRU": "XXXXXXX",
"fruSerialNumber": "XXXXXXX",
"hasOS": false,
"height": 2,
"hostMacAddresses": "E4:3D:1A:61:88:8C,E4:3D:1A:61:88:8D,E4:3D:1A:61:88:8E,E4:3D:1A:61:88:8F",
"hostname": "Shanghai-SR650V3",
"inventoryState": "INVENTORY_READY",
"ipInterfaces": [{
    "name": "Manager Ethernet Interface",
    "label": "unknown",
    "IPv4assignments": [{
        "id": 0,
        "subnet": "255.255.254.0",
        "gateway": "10.240.210.1",
        "address": "10.240.211.178",
        "type": "INUSE"
    }],
    "IPv4DHCPmode": "STATIC_ONLY",
    "IPv4enabled": true,
    "IPv6assignments": [{
        "address": "2002:97b:c2bb:830:10:240:211:178",
        "id": 0,
        "gateway": "0:0:0:0:0:0:0:0",
        "prefix": 64,
        "scope": "Global",
        "source": "Static",
        "type": "INUSE"
    },
    ...,
    {
        "address": "fe80:0:0:0:922e:16ff:fe10:9806",
```

```
            "gateway": "0:0:0:0:0:0:0:0",
            "id": 0,
            "prefix": 64,
            "scope": "LinkLocal",
            "source": "Other",
            "type": "INUSE"
        }],
        "IPv6DHCPenabled": false,
        "IPv6enabled": true,
        "IPv6statelessEnabled": false,
        "IPv6staticEnabled": true
    },
    {
        "IPv4assignments": [],
        "IPv4DHCPmode": "UNKNOWN",
        "IPv4enabled": false,
        "IPv6assignments": [{
            "address": "fe80:0:0:0:922e:16ff:fe10:9806",
            "gateway": "0:0:0:0:0:0:0:0",
            "id": 0,
            "prefix": 64,
            "scope": "LinkLocal",
            "source": "Other",
            "type": "INUSE"
        }],
        "IPv6DHCPenabled": false,
        "IPv6enabled": false,
        "IPv6statelessEnabled": false,
        "IPv6staticEnabled": false,
        "label": "unknown",
        "name": "Manager Ethernet Over USB Interface"
    }],
    "isConnectionTrusted": "true",
    "isITME": false,
    "isScalable": false,
    "ipv4Addresses": ["10.240.211.178","169.254.95.118"],
    "ipv6Addresses": ["2002:97b:c2bb:830:10:240:211:178","fe80::922e:16ff:fe10:9805",
                      "fe80::922e:16ff:fe10:9806"],
    "isRemotePresenceEnabled": true,
    "lanOverUsb": "enabled",
    "lanOverUsbPortForwardingModes": [{
        "externalIPAddress": "",
        "state": "disabled",
        "type": "OSDeploy"
    }],
    "lastOfflineTimestamp": -1,
    "leds": [{
        "color": "Amber",
        "location": "Planar",
        "name": "DIMM 21",
        "state": "Off"
    },
    ...,
    {
        "color": "Amber",
        "location": "Planar",
        "name": "DIMM 20",
        "state": "Off"
    }],
    "location": {
        "lowestRackUnit": 28,
```

```
    "location": "",
    "rack": "lab123",
    "room": "test_room"
},
"logicalID": -1,
"m2Presence": false,
"macAddress": "90:2E:16:10:98:05,90:2E:16:10:98:06",
"machineType": "7D75",
"manufacturer": "Lenovo",
"manufacturerId": "Lenovo",
"memoryModules": [{
    "capacity": 16,
    "displayName": "DIMM 7",
    "fruPartNumber": "",
    "healthState": "NA",
    "manufacturer": "Samsung",
    "metrics": {
        "alarmTrips": {}
    },
    "model": "DDR5",
    "mpfa": {
            "mpfaHealthStatus": {
            "major": 0,
            "minor": 0
        },
        "mpfaSevereFaults": null
    },
    "operatingMemoryMode": ["Volatile"],
    "partNumber": "M321R2GA3BB0-CQKVG",
    "present": false,
    "serialNumber": "80CE01212401CD4F96",
    "slot": 7,
    "speed": 4800,
    "speedMBs": 0,
    "type": "DDR5",
},
{
    "capacity": 16,
    "displayName": "DIMM 23",
    "fruPartNumber": "",
    "healthState": "NA",
    "manufacturer": "Samsung",
    "metrics": {
        "alarmTrips": {}
    },
    "model": "DDR5",
    "mpfa": {
        "mpfaHealthStatus": {
            "major": 0,
            "minor": 0
        },
        "mpfaSevereFaults": null
    },
    "operatingMemoryMode": ["Volatile"],
    "partNumber": "M321R2GA3BB6-CQKEG",
    "present": false,
    "serialNumber": "80CE012210029F85AE",
    "slot": 23,
    "speed": 4800,
    "speedMBs": 0,
    "type": "DDR5",
```

```
}],
"memorySlots": 0,
"mgmtProcIPaddress": "10.240.211.178",
"mgmtProcType": "XCC2",
"model": "RCZ000",
"mpfahealthStatus": false,
"name": "Shanghai-SR650V3",
"nist": {
    "currentValue": "Unknown",
    "possibleValues": ["Nist_800_131A_Strict","unsupported","Compatibility"]
},
"onboardPciDevices": [{
    "class": "Mass storage controller",
    "firmware": [],
    "fodUniqueID": "",
    "isAddOnCard": false,
    "isAgentless": false,
    "isPLDMUpdateSupported": false,
    "name": "PCH Integrated SATA Controller 2",
    "pciBusNumber": "0",
    "pciDeviceNumber": "25",
    "pciFunctionNumber": "0",
    "pciRevision": "11",
    "pciSegmentNumber": "0",
    "pciSubID": "7824",
    "pciSubVendorID": "17aa",
    "portInfo": {},
    "posID": "1bd2",
    "vpdID": "8086"
},
...,
{
    "class": "Unclassified device",
    "firmware": [{
        "name": "Gen5 Riser 2B Retimer",
        "date": "",
        "type": "Software Bundle",
        "build": "0",
        "version": "1.27.35",
        "role": "",
        "status": "Active",
        "classifications": [13],
        "revision": "0",
        "softwareID": "1D494054"
    }],
    "fodUniqueID": "",
    "isAddOnCard": false,
    "isAgentless": false,
    "isPLDMUpdateSupported": false,
    "name": "Retimer Riser 2",
    "pciBusNumber": "0",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "0",
    "pciRevision": "0",
    "pciSubID": "0",
    "pciSubVendorID": "0",
    "portInfo": {},
    "posID": "0",
    "vpdID": "0"
}],
"osInfo": {
```

```
    "description": "",
    "hostname": "",
    "storedCredential": ""
},
"overallHealthState": "Normal",
"parent": {
    "uri": "cabinet/",
    "uuid": ""
},
"partitionID": -1,
"partNumber": "STA7B05327",

"pciCapabilities": ["RaidLink","OOB_PCIe","RaidLinkConfig","RaidLinkAlert","OOB_PCIe_Config",
                    "OOB_Option_Firmware_Update","PreStandardPLDM","StandardPLDM","Storlib","M2"],
"pciDevices": [{
    "class": "Network controller",
    "firmware": [{
        "build": "0",
        "classifications": [13],
        "date": "",
        "name": "Firmware Bundle",
        "revision": "0",
        "role": "",
        "softwareID": "17AA4104",
        "status": "Active",
        "type": "Software Bundle",
        "version": "222.0.2.1"
    }],
    "fodUniqueID": "",
    "FRU": "01PE761",
    "fruSerialNumber": "L0NV1A2004Y",
    "isAddOnCard": true,
    "isAgentless": false,
    "isPLDMUpdateSupported": false,
    "manufacturer": "Broadcom Limited",
    "name": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
    "partNumber": "SN37A28309",
    "pciBusNumber": "22",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "1",
    "pciRevision": "1",
    "pciSegmentNumber": "0",
    "pciSubID": "4104",
    "pciSubVendorID": "17aa",
    "portInfo": {
        "physicalPorts": [{
            "logicalPorts": [{
                "addresses": "e4:3d:1a:61:88:8d",
                "logicalPortIndex": 1,
                "portNumber": 1,
                "portType": "ETHERNET",
                "vnicMode": false
            }],
            "peerBay": 0,
            "physicalPortIndex": 2,
            "portNumber": 2,
            "portType": "ETHERNET",
            "speed": -1.0,
            "status": "Down"
        }]
    },
```

```
    "posID": "1657",
    "productName": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
    "slotName": "PCIe 13",
    "slotNumber": "13",
    "slotSupportsHotPlug": "false",
    "vpdID": "14e4"
}],    "physicalID": 0,
"ports": [{
    "ioModuleBay": 0,
    "portNumber": 3
},
...,
{
    "ioModuleBay": 0,
    "portNumber": 2
}],
"posID": "",
"powerAllocation": {
    "maximumAllocatedPower": 1100,
    "minimumAllocatedPower": 0
},
"powerCappingPolicy": {
    "cappingACorDCMode": "AC",
    "minimumHardCapLevel": 726000,
    "cappingPolicy": "OFF",
    "maxPowerCap": 1100000,
    "minimumPowerCappingHotPlugLevel": -1,
    "powerCappingAllocUnit": "watts*10^-3",
    "maximumPowerCappingHotPlugLevel": -1,
    "currentPowerCap": 0,
    "minPowerCap": 0
},
"powerStatus": 8,
"powerSupplies": [{
    "cmmDisplayName": "Power Supply 1",
    "cmmHealthState": "Unknown",
    "dataHandle": 0,
    "description": "Power Supply 1",
    "excludedHealthState": "Normal",
    "firmware": [{
        "build": null,
        "classifications": [10],
        "date": "",
        "name": "PSU1",
        "role": "OK",
        "softwareID": "PSUACBE8100",
        "status": "OK",
        "type": "Firmware",
        "version": "14.13"
    }],
    "FRU": "",
    "fruSerialNumber": "",
    "hardwareRevision": "",
    "healthState": "GOOD",
    "inputVoltageIsAC": true,
    "inputVoltageMax": -1,
    "inputVoltageMin": -1,
    "leds": [],
    "machineType": "",
    "manufactureDate": "",
    "manufacturer": "ACBE",
```

```
    "manufacturerId": "",
    "model": "",
    "name": "Power Supply 1",
    "overallHealthState": "Normal",
    "parent": {
        "uri": "chassis/",
        "uuid": ""
    },
    "partNumber": "SP57A88785",
    "posID": "",
    "powerAllocation": {
        "totalInputPower": 0,
        "totalOutputPower": 1100
    },
    "powerState": "Unknown",
    "productId": "",
    "productName": "",
    "serialNumber": "A1DB24110DX",
    "slots": [1],
    "type": "PowerSupply",
    "uri": "powerSupply/",
    "userDescription": "",
    "uuid": "",
    "vpdID": ""
}],    "primary": false,
"processorIntelSpeedSelect": {
    "currentValue": "Auto",
    "possibleValues": ["Auto","SST-PP V2","Config1","Config2","Base"]
},
"processors": [{
    "cores": 44,
    "displayName": "Intel(R) Xeon(R) Platinum 8458P",
    "family": "INTEL_R_XEON_TM",
    "healthState": "GOOD",
    "manufacturer": "Intel(R) Corporation",
    "maxSpeedMHZ": 3800,
    "partNumber": "",
    "present": false,
    "productVersion": "Intel(R) Xeon(R) Platinum 8458P",
    "serialNumber": "0x5583BC1F3716456E",
    "slot": 1,
    "socket": "CPU 1",
    "speed": 2.7,
    "tdpWatts": 350
}],
"processorSlots": 0,
"productId": "664A00",
"productName": "ThinkSystem SR650 V3 MB,EGS,DDR5,SH,2U",
"raidSettings": [{
    "batteryData": [],
    "description": "ThinkSystem RAID 940-16i 8GB Flash PCIe Gen4 12Gb Adapter",
    "diskDrives": [{
        "bay": 1,
        "blockSize": 512,
        "capacity": 300000000000,
        "description": "300GB 10K 6Gbps SAS HDD",
        "diskState": "Online",
        "encryptionStatus": "Unencrypted",
        "firmware": [{
            "build": "0",
            "classifications": [10],
```

```
            "date": "",
            "name": "ST9300603SS",
            "revision": "0",
            "role": "",
            "softwareID": "41Y8473",
            "status": "Active",
            "type": "Firmware",
            "version": "B53B"
        }],
        "FRU": "42D0628",
        "healthState": "OK",
        "hotSpareType": "None",
        "interfaceType": "SAS",
        "largestAvailableSize": 512,
        "m2Location": "",
        "manufacturer": "IBM-ESXS",
        "mediaType": "HDD",
        "model": "ST9300603SS",
        "name": "Disk.1",
        "numberOfBlocks": 585937500,
        "partNumber": "42D0631",
        "remainingLife": -1,
        "serialNumber": "6SE2SSGD",
        "temperature": 33,
        "uuid": ""
    }],
    "firmware": [{
        "classifications": [],
        "build": "0",
        "date": "",
        "name": "",
        "revision": "0",
        "role": "",
        "softwareID": "",
        "status": "",
        "type": "",
        "version": "52.22.0-4633"
    }],
    "isAddOnCard": true,
    "model": "SAS3916",
    "name": "ThinkSystem RAID 940-16i 8GB Flash PCIe Gen4 12Gb Adapter",
    "pciFirmware": []
    "slotNumber": "1",
    "storagePools": [{
        "arrayStatus": "",
        "arrayUid": "0",
        "combinedRaidLevel": "0",
        "description": "The resource is used to represent a storage pool for a Redfish implementation.",
        "diskDrives": [{
            "bay": 1,
            "blockSize": 512,
            "capacity": 300000000000,
            "description": "300GB 10K 6Gbps SAS HDD",
            "diskState": "Online",
            "encryptionStatus": "Unencrypted",
            "firmware": [{
                "build": "0",
                "classifications": [10],
                "date": "",
                "name": "ST9300603SS",
                "revision": "0",
```

```
            "role": "",
            "status": "Active",
            "softwareID": "41Y8473",
            "type": "Firmware",
            "version": "B53B"
        }],
        "FRU": "42D0628",
        "healthState": "OK",
        "hotSpareType": "None",
        "interfaceType": "SAS",
        "largestAvailableSize": 512,
        "m2Location": "",
        "manufacturer": "IBM-ESXS",
        "mediaType": "HDD",
        "model": "ST9300603SS",
        "name": "Disk.1",
        "numberOfBlocks": 585937500,
        "partNumber": "42D0631",
        "remainingLife": -1,
        "serialNumber": "6SE2SSGD",
        "temperature": 33,
        "uuid": "",
    }],
    "name": "Pool_6_7",
    "raidLevel": 0,
    "remainingSpace": 0,
    "storageVolumes": [{
        "accessPermission": "READ_WRITE",
        "accessPolicy": "ReadWrite",
        "blockSize": 512,
        "bootable": true,
        "description": "This resource is used to represent a volume for a Redfish implementation.",
        "driveCachePolicy": "Unchanged",
        "driveIndex": 0,
        "health": "OK",
        "ioPolicy": "DirectIO",
        "isSDRAID": null,
        "LUN": -1,
        "name": "",
        "numberOfBlocks": 1167966208,
        "primaryPartition": 0,
        "raidType": "RAID 0",
        "readPolicy": "",
        "removable": false,
        "stripeSize": 262144,
        "targetType": null,
        "volumeID": "239",
        "volumeOwner": null,
        "volumeStatus": "",
        "volumeType": "RAID",
        "volumeUID": "0",
        "writePolicy": "WriteThrough"
    }],
    "totalManagedSpace": 597998698496
}],
"storageVolumes": [{
    "accessPermission": "READ_WRITE",
    "accessPolicy": "ReadWrite",
    "blockSize": 512,
    "bootable": true,
    "description": "This resource is used to represent a volume for a Redfish implementation.",
```

```
            "driveIndex": 0,
            "driveCachePolicy": "Unchanged",
            "health": "OK",
            "ioPolicy": "DirectIO",
            "isSDRAID": null,
            "LUN": -1,
            "name": "",
            "numberOfBlocks": 1167966208,
            "primaryPartition": 0,
            "raidType": "RAID 0",
            "readPolicy": "",
            "removable": false,
            "stripeSize": 262144,
            "targetType": null,
            "volumeID": "239",
            "volumeOwner": null,
            "volumeStatus": "",
            "volumeType": "RAID",
            "volumeUID": "0",
            "writePolicy": "WriteThrough"
        }],
        "uuid": "4BEF9CA0-830B-49F4-8589-1705132EF6F6"
    }],
    "releaseName": "egs_gp_ga",
    "secureBootMode": {
        "currentValue": "Disabled",
        "possibleValues": ["Enabled","Disabled"]
    },
    "securityDescriptor": {
        "identityManagementSystemEnabled": false,
        "managedAuthEnabled": true,
        "managedAuthSupported": true,
        "publicAccess": false,
        "roleGroups": ["lxc-supervisor"],
        "storedCredentials": {
            "description": "Passw0rd@01",
            "id": "1652",
            "userName": "USERID"
        },
        "uri": "nodes/40bdb5f8d609b801c183337c180d3f29"
    },
    "securityMode": "Compatibility  Security",
    "selLog": true,
    "serialNumber": "SR650R112",
    "slots": [],
    "ssoEnabled": true,
    "ssdWearThreshold": 8,
    "status": {
        "message": "managed",
        "name": "MANAGED"
    },
    "subSlots": [],
    "subType": "",
    "systemGuardSetting": {
        "lockDownPolicy": "PreventOSBooting",
        "osBootPreventing": false,
        "status": "Compliant",
        "systemGuardEnabled": false
    },
    "userDefinedName": "Shanghai-SR650V3",
    "tlsVersion": {
```

```
        "currentValue": "TLS_12",
        "possibleValues": ["unsupported","TLS_12","TLS_11","TLS_10"]
    },
    "type": "Rack-Tower  Server",
    "uri": "nodes/40BDB5F8D609B801C183337C180D3F29",
    "userDescription": "",
    "uuid": "40BDB5F8D609B801C183337C180D3F29",
    "vnicMode": "disabled",
    "vpdID": ""
}]}
```


POST /nodes

Use this method to return properties for a large number of specific servers, Flex System storage devices, and Flex System storage controllers (canisters).

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/nodes`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
formatType	Optional	String	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv** **Note:** If you choose **formatType=csv**, this request creates a file in CSV format and returns the filename in the request header. You can use to download the file using GET /nodes/*{file_name}*.csv.
uuids	Required	String	List of device UUIDs, separated by a comma

The following example returns properties for two devices in JSON.


```
{
   "uuids": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
}
```


The following example returns properties for two devices as a CSV file.


```
{
   "formatType": "csv",
   "uuids": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

If **formatType=csv** is specified, the response header includes the URI of the downloaded file. If data for a single node is requested, the file name includes the node UUID. If multiple nodes are requested, the file name is `allNodes_<unique_ID}.csv`. For example:

```
Status Code: 201 Created
Location: /chassis/EF6D424FAACA4E539771B812AAEE0F73.csv
```

Response body

If the **formatType=csv** request attribute is specified, no response body is returned.

If the **formatType=json** request attribute is specified, the following JSON object is returned.

Note: GET /nodes returns the **canister** attribute as a child under the **enclosure** attribute and also as a peer to the **enclosure** attribute (in duplication).For GET /nodes/*{uuid_list}*, the **canister** attribute is only returned as a child under the **enclosure** attribute.

Attributes	Type	Description
nodeList	Array	List of all servers and storage devices
See GET /nodes/*{uuid_list}*	Object	Detailed information about the individual server or storage device

The following example is returned if the request is successful.


```
{
   "nodeList": [{
      "accessState": "Online",
      "activationKeys": [{
         "description": "IBM Integrated Management Module Advanced Upgrade",
         "keyExpirationDate": "",
         "keyFeatureType": 1,
         "keyIdentifierList": [{
            "keyIdentifier": "5463KVD0153",
            "keyIdentifierType": "MT"
         }],
         "keyStatus": "VALID",
         "keyUseCount": 0,
```

```
    "keyUseLimit": 0,
    "uuid": "8f0f1789295e78f9"
}],
"addinCardSlots": 0,
"addinCards": [{
    "FRU": "N/A",
    "firmware": [{
        "build": "0",
        "classifications": [13],
        "date": "2015-04-06T00:00:00Z",
        "name": "LSI MegaRAID Adapter Firmware",
        "revision": "0",
        "role": "Primary",
        "softwareID": "10140454",
        "status": "Active",
        "type": "Software Bundle",
        "version": "24.7.0-0052"
    }],
    "fodUniqueID": "N/A",
    "fruSerialNumber": "SV42100396",
    "isAddOnCard": true,
    "isAgentless": true,
    "manufacturer": "IBM",
    "name": "ServeRAID M5210",
    "partNumber": "N/A",
    "pciBusNumber": "1",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "0",
    "pciRevision": "2",
    "pciSubID": "454",
    "pciSubVendorID": "1014",
    "portInfo": { },
    "posID": "5d",
    "productName": "ServeRAID M5210",
    "slotName": "SlotDesig4_Slot 4",
    "slotNumber": "4",
    "slotSupportsHotPlug": "false",
    "vpdID": "1000"
}],
"arch": "x86",
"backedBy": "real",
"bladeState": 0,
"bootMode": {
    "currentValue": "UEFI Mode",
    "possibleValues": ["UEFI Mode",
    "Legacy Mode"]
},
"bootOrder": {
    "bootOrderList": [{
        "bootType": "SingleUse",
        "currentBootOrderDevices": ["None"],
        "possibleBootOrderDevices": ["None",
        "PXE Network",
        "Disk Drive 0",
        "Diagnostics",
        "CD/DVD Rom",
        "Boot To F1",
        "Hypervisor",
        "Floppy Disk"]
    },
    ...,
```

```
   {
      "bootType": "WakeOnLAN",
      "currentBootOrderDevices": ["PXE Network", "CD/DVD Rom","Disk Drive 0"],
      "possibleBootOrderDevices": ["PXE Network",
      "CD/DVD Rom",
      "Disk Drive 0",
      "Floppy Disk",
      ...,
      "sSATA Port 2",
      "sSATA Port 3",
      "DSA"]
   }],
   "uri": "node/425AF828DF7D11D4B0F8E76767BBBBBB/bootOrder"
},
"cmmDisplayName": "Management Controller UUID-425AF828DF7D11D4B0F8E76767BBBBBB",
"cmmHealthState": "Normal",
"complexID": -1,
"contact": "",
"dataHandle": 1440525606363,
"description": "Chassis",
"dnsHostnames": ["10.243.6.69",
"fd55:faaf:e1ab:2021:42f2:e9ff:feb8:1585"],
"domainName": "",
"driveBays": 0,
"drives": [],
"embeddedHypervisorPresence": false,
"encapsulation": {
   "encapsulationMode": "normal",
}
"errorFields": [{
   "ChassisMounted": "NO_CONNECTOR"
}],
"excludedHealthState": "Normal",
"expansionCardSlots": 0,
"expansionCards": [],
"expansionProductType": "",
"expansionProducts": [],
"featuresOnDemand": {
   "tierLevel": 3,
   "features": ["RDOC", "REMOTE CONTROL 6 USERS", "REMOTE MEDIA"]
},
"firmware": [{
   "build": "TBE105KUS",
   "date": "2015-04-17T00:00:00Z",
   "name": "UEFI Firmware/BIOS",
   "role": "Primary",
   "status": "Active",
   "type": "UEFI",
   "version": "1.10"
},
...,
{
   "build": "TCOOO9D",
   "date": "2015-04-17T00:00:00Z",
   "name": "IMM2 Backup Firmware",
   "role": "Backup",
   "status": "Inactive",
   "type": "IMM2-Backup",
   "version": "1.71"
}],
"flashStorage": [],
```

```
"FRU": "None",
"fruSerialNumber": "None",
"hasOS": false,
"height": 1,
"hostMacAddresses": "40:F2:E9:B8:15:80,40:F2:E9:B8:15:81,40:F2:E9:B8:15:82,40:F2:E9:B8:15:83",
"hostname": "IMM2-40f2e9b81585",
"ipInterfaces": [{
   "IPv4DHCPmode": "STATIC_ONLY",
   "IPv4assignments": [{
      "address": "10.243.6.69",
      "gateway": "0.0.0.0",
      "id": 0,
      "subnet": "255.255.240.0",
      "type": "INUSE"
   }],
   "IPv4enabled": true,
   "IPv6DHCPenabled": true,
   "IPv6assignments": [{
      "address": "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:1585",
      "gateway": "0:0:0:0:0:0:0:0",
      "id": 0,
      "prefix": 64,
      "scope": "Global",
      "source": "Stateless",
      "type": "INUSE"
   },
   {
      "address": "fe80:0:0:0:42f2:e9ff:feb8:1585",
      "gateway": "0:0:0:0:0:0:0:0",
      "id": 0,
      "prefix": 64,
      "scope": "LinkLocal",
      "source": "Other",
      "type": "INUSE"
   }],
   "IPv6enabled": true,
   "IPv6statelessEnabled": true,
   "IPv6staticEnabled": false,
   "label": "unknown",
   "name": "eth0"
}],
"ipv4Addresses": ["10.243.6.69",
"169.254.95.118"],
"ipv6Addresses": ["fd55:faaf:e1ab:2021:42f2:e9ff:feb8:1585",
"fe80::42f2:e9ff:feb8:1585"],
"isConnectionTrusted": "true",
"isITME": false,
"isRemotePresenceEnabled": true,
"isScalable": false,
"lanOverUsb": "enabled",
"leds": [{
   "color": "Yellow",
   "location": "Unknown",
   "name": "Fault",
   "state": "Off"
},
{
   "color": "Blue",
   "location": "Unknown",
   "name": "Identify",
   "state": "Off"
```

```
},
...,
{
   "color": "Yellow",
   "location": "Planar",
   "name": "SDRAID Error",
   "state": "Off"
}],
"location": {
   "location": "",
   "lowestRackUnit": 0,
   "rack": "",
   "room": ""
},
"macAddress": "40:F2:E9:B8:15:85,40:F2:E9:B8:15:86",
"machineType": "5463",
"manufacturer": " IBM(WIST)",
"manufacturerId": " IBM(WIST)",
"memoryModules": [{
   "capacity": 4,
   "displayName": "DIMM 1",
   "manufacturer": "Unknown",
   "model": "DDR4",
   "partNumber": "HMA451R7MFR8N-TFTD ",
   "serialNumber": "103D4F44",
   "slot": 1,
   "speed": 2133,
   "type": "DDR4"
}],
"memorySlots": 0,
"mgmtProcIPaddress": "10.243.6.69",
"model": "45Z",
"name": "DaAn5",
"nist": {
   "currentValue": "Compatibility",
   "possibleValues": ["Compatibility",
   "Nist_800_131A_Strict"]
},
"onboardPciDevices": [{
   "firmware": [{
      "build": "0",
      "classifications": [0],
      "date": "",
      "name": "PCIFirmware",
      "revision": "0",
      "role": "Primary",
      "softwareID": "1014:405",
      "status": "Active",
      "type": "",
      "version": ""
   }],
   "fodUniqueID": "",
   "isAddOnCard": false,
   "isAgentless": false,
   "name": "",
   "pciBusNumber": "25",
   "pciDeviceNumber": "0",
   "pciFunctionNumber": "0",
   "pciRevision": "1",
   "pciSubID": "405",
   "pciSubVendorID": "1014",
```

```
    "portInfo": {

    },
    "posID": "534",
    "vpdID": "102b"
},
...,
{
    "firmware": [{
       "build": "0",
       "classifications": [33024],
       "date": "",
       "name": "17.0.4.4a",
       "revision": "0",
       "role": "Primary",
       "softwareID": "101404D1",
       "status": "Active",
       "type": "VPD-V0",
       "version": "17.0.4.4a"
    }],
    "fodUniqueID": "11SBCM957190123456789",
    "isAddOnCard": false,
    "isAgentless": true,
    "name": "Broadcom NetXtreme Gigabit Ethernet Adapter",
    "pciBusNumber": "27",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "3",
    "pciRevision": "1",
    "pciSubID": "4d1",
    "pciSubVendorID": "1014",
    "portInfo": {
       "logicalPorts": [{
          "addresses": "40F2E9B81583",
          "portNumber": 1,
          "portType": "ETHERNET",
          "vnicMode": false
       }],
       "peerBay": 0,
       "portNumber": 4,
       "portType": "ETHERNET"
    },
    "posID": "1657",
    "vpdID": "14e4"
}],
"overallHealthState": "Normal",
"partNumber": "00KC903",
"partitionID": -1,
"pciCapabilities": ["Raid Link",
"OOB PCIe",
"Raid Link Config",
"Raid Link Alert",
"OOB PCIe Config"],
"pciDevices": [{
    "FRU": "N/A",
    "firmware": [{
       "build": "0",
       "classifications": [13],
       "date": "2015-04-06T00:00:00Z",
       "name": "LSI MegaRAID Adapter Firmware",
       "revision": "0",
       "role": "Primary",
```

```
            "softwareID": "10140454",
            "status": "Active",
            "type": "Software Bundle",
            "version": "24.7.0-0052"
        }],
        "fodUniqueID": "N/A",
        "fruSerialNumber": "SV42100396",
        "isAddOnCard": true,
        "isAgentless": true,
        "manufacturer": "IBM",
        "name": "ServeRAID M5210",
        "partNumber": "N/A",
        "pciBusNumber": "1",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "0",
        "pciRevision": "2",
        "pciSubID": "454",
        "pciSubVendorID": "1014",
        "portInfo": {

        },
        "posID": "5d",
        "productName": "ServeRAID M5210",
        "slotName": "SlotDesig4_Slot 4",
        "slotNumber": "4",
        "slotSupportsHotPlug": "false",
        "vpdID": "1000"
    },
    ...,
    {
        "firmware": [{
            "build": "0",
            "classifications": [33024],
            "date": "",
            "name": "17.0.4.4a",
            "revision": "0",
            "role": "Primary",
            "softwareID": "101404D1",
            "status": "Active",
            "type": "VPD-V0",
            "version": "17.0.4.4a"
        }],
        "fodUniqueID": "11SBCM957190123456789",
        "isAddOnCard": false,
        "isAgentless": true,
        "name": "Broadcom NetXtreme Gigabit Ethernet Adapter",
        "pciBusNumber": "27",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "3",
        "pciRevision": "1",
        "pciSubID": "4d1",
        "pciSubVendorID": "1014",
        "portInfo": {
            "logicalPorts": [{
                "addresses": "40F2E9B81583",
                "portNumber": 1,
                "portType": "ETHERNET",
                "vnicMode": false
            }],
            "peerBay": 0,
            "portNumber": 4,
```

```
      "portType": "ETHERNET"
   },
   "posID": "1657",
   "vpdID": "14e4"
}],
"ports": [{
   "ioModuleBay": 0,
   "portNumber": 1
},
...,
{
   "ioModuleBay": 0,
   "portNumber": 4
}],
"posID": "",
"powerAllocation": {
   "maximumAllocatedPower": 660,
   "minimumAllocatedPower": 26
},
"powerCappingPolicy": {
   "cappingACorDCMode": "DC",
   "cappingPolicy": "OFF",
   "currentPowerCap": 0,
   "maxPowerCap": 319000,
   "maximumPowerCappingHotPlugLevel": 367000,
   "minPowerCap": 85300,
   "minimumHardCapLevel": 246200,
   "minimumPowerCappingHotPlugLevel": 268000,
   "powerCappingAllocUnit": "watts*10^-3"
},
"powerStatus": 5,
"powerSupplies": [{
   "FRU": "",
   "cmmDisplayName": "Power Supply 1",
   "dataHandle": 0,
   "description": "",
   "firmware": [],
   "fruSerialNumber": "",
   "hardwareRevision": "",
   "healthState": "CRITICAL",
   "inputVoltageIsAC": true,
   "inputVoltageMax": -1,
   "inputVoltageMin": -1,
   "leds": [],
   "machineType": "",
   "manufactureDate": "",
   "manufacturer": "EMER",
   "manufacturerId": "",
   "model": "",
   "name": "Power Supply 1",
   "partNumber": "94Y8136",
   "posID": "",
   "powerAllocation": {
      "totalInputPower": 0,
      "totalOutputPower": 550000
   },
   "powerState": "Unknown",
   "productId": "",
   "productName": "",
   "serialNumber": "K118146600A",
   "slots": [1],
```

```
      "type": "PowerSupply",
      "uri": "powerSupply/",
      "userDescription": "",
      "uuid": "",
      "vpdID": ""
   },
   {
      "FRU": "",
      "cmmDisplayName": "Power Supply 2",
      "dataHandle": 0,
      "description": "",
      "firmware": [],
      "fruSerialNumber": "",
      "hardwareRevision": "",
      "healthState": "CRITICAL",
      "inputVoltageIsAC": true,
      "inputVoltageMax": -1,
      "inputVoltageMin": -1,
      "leds": [],
      "machineType": "",
      "manufactureDate": "",
      "manufacturer": "EMER",
      "manufacturerId": "",
      "model": "",
      "name": "Power Supply 2",
      "partNumber": "94Y8136",
      "posID": "",
      "powerAllocation": {
         "totalInputPower": 0,
         "totalOutputPower": 550000
      },
      "powerState": "Unknown",
      "productId": "",
      "productName": "",
      "serialNumber": "K1181466087",
      "slots": [2],
      "type": "PowerSupply",
      "uri": "powerSupply/",
      "userDescription": "",
      "uuid": "",
      "vpdID": ""
   }],
   "processorSlots": 0,
   "processors": [{
      "cores": 10,
      "displayName": "Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz",
      "family": "INTEL_R_XEON_TM",
      "manufacturer": "Intel(R) Corporation",
      "productVersion": "Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz",
      "slot": 1,
      "speed": 2.2999999999999998
   }],
   "productId": "4D4F00",
   "productName": "Lenovo System x3550 M5",
   "raidSettings": [{
      "description": "ServeRAID M5210",
      "diskDrives": [{
         "FRU": "42D0631",
         "bay": 0,
         "blockSize": 512,
         "description": "AL13SEB300",
```

```
        "diskState": "System",
        "healthState": "Normal",
        "interfaceType": "SAS",
        "manufacturer": "IBM-ESXS",
        "mediaType": "Rotational",
        "model": "AL13SEB300",
        "name": "Disk 0_0",
        "numberOfBlocks": 585937500,
        "partNumber": "42D0628",
        "serialNumber": "44P012H5",
        "uuid": ""
    },
    ...,
    {
        "FRU": "81Y3810",
        "bay": 1,
        "blockSize": 512,
        "description": "ST9300653SS",
        "diskState": "System",
        "healthState": "Normal",
        "interfaceType": "SAS",
        "manufacturer": "IBM-ESXS",
        "mediaType": "Rotational",
        "model": "ST9300653SS",
        "name": "Disk 2_2",
        "numberOfBlocks": 585937500,
        "partNumber": "81Y9667",
        "serialNumber": "6XN3J9M9",
        "uuid": ""
    }],
    "firmware": [{
        "build": "0",
        "classifications": [],
        "date": "2015-04-06T00:00:00Z",
        "name": "LSI MegaRAID Adapter Firmware",
        "revision": "0",
        "role": "Primary",
        "softwareID": "10140454",
        "status": "Active",
        "type": "",
        "version": "24.7.0-0052"
    }],
    "isAddOnCard": false,
    "name": "ServeRAID M5210",
    "slotNumber": "2",
    "uuid": "00000000000000000500605B008E48280"
}],
"secureBootMode": {
    "currentValue": "Disabled",
    "possibleValues": ["Disabled",
    "Enabled"]
},
"serialNumber": "KVD0153",
"slots": [1],
"status": {
    "message": "managed",
    "name": "MANAGED"
},
"subSlots": [],
"subType": "",
"tlsVersion": {
```

```
        "currentValue": "TLS_10",
        "possibleValues": ["TLS_10",
        "TLS_11",
        "TLS_12"]
    },
    "type": "Rack-Tower Server",
    "uri": "node/425AF828DF7D11D4B0F8E76767BBBBBB",
    "userDescription": "",
    "uuid": "425AF828DF7D11D4B0F8E76767BBBBBB",
    "vnicMode": "disabled",
    "vpdID": ""
}
{
    accessState: "Online",
    activationKeys: [],
    addinCards: [],
    addinCardSlots: 0,
    arch: "x86_64",
    backedBy: "real",
    bladeState: 0,
    bootMode: {
        possibleValues: ["Legacy Only",
        "UEFI and Legacy",
        "UEFI Only"],
        currentValue: "UEFI and Legacy"
    },
    bootOrder: {
        bootOrderList: [{
            bootType: "SingleUse",
            currentBootOrderDevices: ["None"],
            possibleBootOrderDevices: ["Boot To F1",
            "CD/DVD Rom",
            "Diagnostics",
            "Floppy Disk",
            "Disk Drive 0",
            "Hypervisor",
            "None",
            "PXE Network"]
        },
        ...],
        uri: "node/00DD973D1C2CE511B19E3C18A000F4F0/bootOrder"
    },
    cmmDisplayName: "",
    cmmHealthState: "Warning",
    complexID: -1,
    contact: "",
    dataHandle: 0,
    description: "chassis RD650",
    domainName: "lenovo.com",
    driveBays: 2,
    drives: [{
        bay: 0,
        capacity: 953,
        interfaceType: "SATA",
        mediaType: "HDD",
        speed: "6.0 Gb/s",
        state: "stopped",
        raidPresence: "Regular"
    },
    {
        bay: 1,
```

```
    capacity: 953,
    interfaceType: "SATA",
    mediaType: "HDD",
    raidPresence: "Regular",
    speed: "6.0 Gb/s",
    state: "stopped"
}],
embeddedHypervisorPresence: false,
errorFields: [],
excludedHealthState: "Warning",
expansionCards: [],
expansionCardSlots: 0,
expansionProducts: [],
expansionProductType: "",
fans: [],
firmware: [{
    build: "",
    date: "",
    name: "BIOS",
    role: "PRIMARY",
    status: "ACTIVE",
    type: "BIOS",
    version: "PB2TS154"
},
...,
{
    build: "",
    date: "",
    name: "Windows Driver Bundle",
    role: "",
    status: "ACTIVE",
    type: "Windows Driver Bundle",
    version: "1.02.0004"
}],
flashStorage: [],
FRU: "",
fruSerialNumber: "8SSB20A05917R2SH54D005X",
hasOS: false,
height: 2,
hostMacAddresses: "",
hostname: "blah",
ipInterfaces: [],
ipv4Addresses: ["10.35.106.142"],
ipv6Addresses: [""],
isConnectionTrusted: "true",
isITME: false,
isRemotePresenceEnabled: true,
isScalable: false,
lanOverUsb: "disabled",
leds: [{
    conditions: "Fault",
    color: "Red",
    location: "FrontPanel",
    name: "Fault",
    state: "Off"
},
...,
{
    conditions: "Fault",
    color: "Red",
    location: "PSU",
```

```
    name: "PSU1 FAULT",
    state: "Off"
}],
location: {
    location: "",
    lowestRackUnit: 0,
    rack: "",
    room: ""
},
macAddress: "00:8C:FA:E7:E8:D0,00:8C:FA:E7:E8:D1",
machineType: "RD650",
manufacturer: "LENOVO",
manufacturerId: "",
memoryModules: [{
    capacity: 8,
    displayName: "DIMM 1",
    manufacturer: "Micron Technology",
    model: "",
    partNumber: "18ASF1G72PZ-2G1A2",
    serialNumber: "da90356",
    slot: 1,
    speed: 1866,
    type: "RDIMM",
    voltage: "1.2V"
}],
memorySlots: 0,
mgmtProcIPaddress: "",
model: "70DR000SUX",
name: "blah",
nist: {
    currentValue: "Nist_800_131A_Strict",
    possibleValues: ["Compatibility",
    "Nist_800_131A_Custom",
    "Nist_800_131A_Strict"]
},
onboardPciDevices: [{
    fodUniqueID: "",
    isAddOnCard: false,
    isAgentless: false,
    name: "",
    pciBusNumber: "4",
    pciDeviceNumber: "0",
    pciRevision: "0",
    pciSubID: "1051",
    pciSubVendorID: "17aa",
    pciFunctionNumber: "0",
    portInfo: {

    },
    posID: "73",
    vpdID: "1000"
}],
overallHealthState: "Warning",
partitionID: -1,
partNumber: "",
pciCapabilities: [],
pciDevices: [{
    fodUniqueID: "",
    isAddOnCard: false,
    isAgentless: false,
    name: "",
```

```
    pciBusNumber: "4",
    pciFunctionNumber: "0",
    pciRevision: "0",
    pciSubID: "1051",
    pciSubVendorID: "17aa",
    pciDeviceNumber: "0",
    portInfo: {

    },
    posID: "73",
    vpdID: "1000"
}],
ports: [],
posID: "",
powerAllocation: {
    maximumAllocatedPower: 0,
    minimumAllocatedPower: 0
},
powerCappingPolicy: {
    cappingACorDCMode: "UNKNOWN",
    cappingPolicy: "UNKNOWN",
    currentPowerCap: 0,
    maxPowerCap: -1,
    maximumPowerCappingHotPlugLevel: -1,
    minimumHardCapLevel: -1,
    minPowerCap: -1minimumPowerCappingHotPlugLevel: -1,
    powerCappingAllocUnit: "watts",

},
powerStatus: 8,
powerSupplies: [{
    cmmDisplayName: null,
    dataHandle: 0,
    description: "Power Supply 1",
    firmware: [],
    FRU: null,
    fruSerialNumber: null,
    hardwareRevision: "01F",
    healthState: "GOOD",
    inputVoltageIsAC: false,
    inputVoltageMax: 0,
    inputVoltageMin: 0,
    leds: [{
        color: "Green",
        location: "FRU",
        name: "IN",
        state: "On"
    },
    ...,
    {
        color: "Amber",
        location: "FRU",
        name: "FAULT",
        state: "Off"
    }],
    machineType: null,
    manufactureDate: "Feb 5, 2015",
    manufacturer: null,
    manufacturerId: "DELTA",
    model: "DPS-1100EB A",
    name: "0F33323D1DG525001X",
```

```
   partNumber: null,
   posID: null,
   powerAllocation: {
      totalInputPower: 0,
      totalOutputPower: 0
   },
   powerState: null,
   productId: null,
   productName: null,
   serialNumber: "0F33323D1DG525001X",
   slots: [0],
   type: "PowerSupply",
   uri: "powerSupply/null",
   userDescription: null,
   uuid: null,
   vpdID: null
}],
processors: [{
   cores: 8,
   displayName: "",
   family: "Intel Nehalem Family",
   manufacturer: "GenuineIntel",
   productVersion: "Haswell Server Model",
   slot: 1,

   speed: 3.4
}],
processorSlots: 0,
productId: "",
productName: "RD650",
raidSettings: [],
secureBootMode: {
   currentValue: "",
   possibleValues: []
},
"securityDescriptor": {
   "managedAuthEnabled": true,
   "managedAuthSupported": false,
   "publicAccess": false,
   "roleGroups": [],
   "storedCredentials": {
      "id":"249721...",
      "userName":"user1",
      "description":"A valid user"
   },
   "uri": "nodes/200b8108289d11e3878e000af725674c"
},
serialNumber: "MJ02SC2F",
slots: [1],
status: {
   message: "managed",
   name: "MANAGED"
},
subType: "",
subSlots: [],
thinkServerFru: [{
   deviceName: "12GBP 8xS",
   description: "BackPlane1 FRU",
   manufatucturer: "LENOVO",
   manufatucturerDate: "Dec 24, 2014",
   partNumber: "SSF0A47711",
```

```
            serial: "8SSSF0A47711V1SH4CR0079"
        },
        ...,
        {
            deviceName: "Riser2U 3x8",
            description: "Riser1 FRU",
            manufatucturer: "LENOVO",
            manufatucturerDate: "Dec 15, 2014",
            partNumber: "SC50A06667",
            serial: "8SSC50A06667V1SH4CE00JW"
        }],
        tlsVersion: {
            currentValue: "Unknown",
            possibleValues: ["TLS_10",
            "TLS_11",
            "TLS_12"]
        },
        type: "Lenovo ThinkServer",
        uri: "node/00DD973D1C2CE511B19E3C18A000F4F0",
        "userDefinedName": "Server1",
        userDescription: "",
        uuid: "00DD973D1C2CE511B19E3C18A000F4F0",
        vnicMode: "disabled",
        vpdID: ""
    }]
}
```


/nodes/*{file_name}*.csv

Use this REST API to download inventory for a large number of specific servers, Flex System storage devices, and Flex System storage controllers (canisters) in CSV format to the local system.

HTTP methods

GET

GET /nodes/*{file_name}*.csv

Use this method to download inventory for a large number of specific servers, Flex System storage devices, and Flex System storage controllers (canisters) in CSV format to the local system.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{file_name}.csv`

where *{file_name}*.csv is the file name of the CSV file that contains inventory data. Use the POST /nodes method to with the **formatType=csv** request parameter to create the CSV file. The POST /nodes method returns the file name in the request header.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/nodes/*{uuid}*

Use this REST API to retrieve or modify properties and turn LEDs on and off for a specific server or Flex System storage node.

HTTP methods

GET, PUT

GET /nodes/*{uuid_list}*

Use this method to return properties for one or more specific servers, Flex System storage devices, and Flex System storage controllers (canisters).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{UUID_list}`

where *{UUID_list}* is one or more UUIDs, separated by a comma, of the servers, Flex System storage devices, and canisters to be retrieved. To obtain the UUIDs, use the GET /nodes and GET /canisters methods.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
formatType=*{type}*	Optional	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv** If the format type is not specified, JSON format is returned.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.
mgmtProcType	Optional	Returns a response that includes servers with the specified baseboard management controller. This can be one of the following values. • **FSP** • **IMM2** • **lenovo-AMI-controller** • **XCC** • **XCC2** • **UNKNOWN**
status=*{string}*	Optional	Status. This can be one of the following values. • **unmanaged**. Returns unmanaged nodes only • **managed**. Returns managed nodes only

The following example returns a CSV file that contains information about two specific servers.

```
GET https://192.0.2.0 /nodes/0E7D8E1CDF7D11D4ABB0D5D5D5313131,
409583E0BD27B7019F3758946B036818?formatType=csv
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
413	Request Entity Too Large	Clients might impose limitations on the length of the request URI, and the request URI is too long to be handled. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Note: The attributes that are returned vary, depending on the type of server or Flex System storage device being retrieved.

Attributes	Type	Description
accessState	String	Access state of the server. This can be one of the following values. • **Online** • **Offline** • **Partial** • **Pending** • **Unknown**
accessStateRecords	Array of objects	Information about the access-state record for each network interface and protocol that is available for the server **Note:** This attribute is present only for rack servers that are offline due to connectivity issues.
health	String	Connection health state of the server. This can be one of the following values. • **OFFLINE** • **PARTIAL** • **FAIL**
ipAddress	String	IP address that was used to check the network connectivity
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle
messageDisplay	String	Translated label that corresponds to the message ID or to the pre-translated backup string if no message ID is specified
messageID	String	Message ID for the translatable connection error states
messageParameters	Array of strings	List of attributes for the message if the translated message requires input. A JSON object that points to translated messages
protocol	String	Type of the protocol to check connectivity. This can be one of the following values. • **CIM** • **DCS** • **REDFISH** • **CLI**
timestamp	Long	Timestamp when connectivity was last checked and when this record was created
trusted	Boolean	Indicates whether the connection to the server is trusted. This can be one of the following values. • **true**. The connection is trusted. • **false**. The connection is not trusted.

Attributes	Type	Description
username	String	User name that was used to check connectivity
accountLockoutPeriod	Integer	Account lockout duration, in minutes, after certain login failures occur on the device The default value is 60 minutes.
activationKeys	Array of objects	Information about each Feature On Demand (FoD) key
description	String	FoD key description
keyExpirationDate	String	Date when the FoD key expires
keyFeatureType	Integer	FoD feature type
keyIdentiferList	Array of objects	List of FoD key IDs
keyIdentifier	String	Identifier key value
keyIdentifierType	String	Identifier key type. This can be one of the following values. • **ASIC**. • **MAC**. MAC address • **MT**. Machine type • **UNKNOWN**
keyStatus	String	Status of the FoD key. This can be one of the following values. • **UNKNOWN** • **OTHER** • **VALID** • **INVALID** • **INPROCESS** • **EXPIRED** • **LIMIT_REACHED** • **NEED_VALID_ELSEWHERE** • **KEY_NOT_FOUND**
keyUseCount	Integer	Key usage count
keyUseLimit	Integer	Key usage limit
uuid	String	Unique identifier for the FoD key
addinCards	Array of objects	Information about each add-in card **Note:** Multiple instances of the same adapter card with different data (such as the pciFunctionNumber) might be returned in this response. In the UI, only one instance of each adapter card (only the first function number) is listed.

Attributes	Type	Description
class	String	Class (basic function) of the PCI device. This can be one of the following values. • **Bridge** • **Communication** controller • **Coprocessor** • **Display** controller • **Docking** station • **Encryption controller** • **Generic system peripheral** • **Input device controller** • **Intelligent controller** • **Mass storage controller** • **Memory controller** • **Multimedia controller** • **Network controller** • **Non-Essential Instrumentation** • **Processing accelerators** • **Processor** • **Satellite communications controller** • **Serial bus controller** • **Signal processing controller** • **Unassigned class** • **Unclassified device** • **Unknown device** • **Wireless controller**
firmware	Array of objects	Information about each add-in card firmware
build	String	Firmware build
classifications	Array of integers	List of firmware type codes
date	String	Firmware date
name	String	Firmware name
revision	String	Firmware revision
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
softwareID		Firmware ID
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive**
type	String	Firmware type, such as UEFI, MP, or DSA
version	String	Firmware version
fodUniqueID	String	FoD unique ID
FRU	String	Add-in card FRU part number
fruSerialNumber	String	

Attributes	Type	Description
isAddOnCard	Boolean	Identifies whether the device is an add-in card. This can be one of the following values. • **true**. The device is an add-on card • **false**. The device is not an add-on card
isAgentless	Boolean	Identifies whether the device is agentless. This can be one of the following values. • **true**. The device is agentless. • **false**. The device is not agentless. **Note:** If **isAgentless** is false, some inventory values might be empty.
isPLDMUpdateSupported	Boolean	Identifies whether the Platform Level Data Model updates are supported. This can be one of the following values. • **true**. PLDM update is supported. • **false**. PLDM update is not supported.
manufacturer	String	Add-in card manufacturer
name	String	Add-in card description
partNumber	String	Add-in card part number
pciBusNumber	String	PCI bus number
pciDeviceNumber	String	PCI device number
pciFunctionNumber	String	PCI function number
pciRevision	String	PCI revision number
pciSubID	String	PCI subsystem ID
pciSubVendorID	String	PCI sub-vendor ID
portInfo	Object	Information about the port
physicalPorts	Array of objects	Information about each physical port
logicalPorts	Array of objects	Information about each logical port
addresses	String	Assigned addresses
logicalPortIndex	Integer	Number of logical ports
portNumber	Integer	Number of the logical port
portType	String	Logical port type. This can be one of the following values. • **ATM** • **BLUETOOTH** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **INFRARED** • **OTHER** • **TOKENRING** • **UNKNOWN** • **WIRELESSLAN**

Attributes	Type	Description
vnicMode	Boolean	Identifies whether this is a vNIC port. This can be one of the following values. • **true**. This is a vNIC port. • **false**. This is not a vNIC port.
peerBay	Integer	Peer I/O Module bay
physicalPortIndex	Integer	Number of physical ports
portNumber	Integer	Number of the physical port
portType	String	Physical port type. This can be one of the following values. • **ATM** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **OTHER** • **TOKENRING** • **UNKNOWN**
speed	Long	Link speed, in Gbps (for example, 2.5)
status	String	Link status. This can be one of the following values.Link status. This can be one of the following values. • **up** • **down** • **unknown**
posID	String	Device ID
productName	String	Product name
slotName	String	Name for add-in card slot
slotNumber	String	Number for add-in card slot
slotSupportsHotPlug	Boolean	Indicates whether the add-in card supports hot plug. This can be one of the following values. • **true**. Hot plug is supported. • **false**. Hot plug is not supported.
vpdID	String	VPD ID
addinCardSlots	Integer	Number of used add-in card slot
arch	String	Architecture. This can be one of the following values. • **ia64** • **ppc** • **ppc64** • **x86** • **x86_64** • **Unknown**
agentVersion	String	(Edge devices only) Version of the XClarity management agent that is running on the device
assetTag	String	(ThinkSystem rack servers only) Name or Tag that represents the server or other physical enclosure
backedBy	String	This can be one of the following values. • **real**. The inventory describes real hardware. • **demo**. The inventory describes demo (mock) hardware. • **proxy**. A proxy is temporarily serving to provide the inventory.

Attributes	Type	Description
bladeState	Integer	State of the server. This can be one of the following values. • **0**. Initializing • **1**. Active • **2**. Discovering • **3**. Provisioning • **4**. Provision passed • **5**. Provision failed • **6**. Provisioning failed with isolate • **7**. Pre initialization • **8**. SDR load • **9**. POST initialization • **10**. Communications error • **11**. Init failed • **12**. Kernel mode • **13**. Maintenance mode • **14**. Fire hose dump mode • **15**. Flashing • **16**. No power • **17**. Unknown • **255**. Not Applicable
bladeState_health	String	
bladeState_string	String	
bmuParamObject	Object	
bootMode	Object	Information about the boot mode
currentValue	String	Current boot mode from the baseboard management controller
possibleValues	Array of strings	List of possible boot mode values
bootOrder	Object	Information about the boot order
bootOrderList	Array of objects	Information about each boot order
bootType	String	Boot type. This can be one of the following values. • **BootOrder** • **CDDVDROMBootOrder** • **HardDiskBootOrder** • **NetworkBootOrder** • **Permanent** • **SingleUse** • **USBBootOrder** • **WakeOnLan** • **Unknown**
currentBootOrderDevices	Array of strings	List of current boot order devices
possibleBootOrderDevices	Array of strings	List of possible boot order devices
uri	String	Boot order URI
BundleRepoAvailableSpaceInKB	Long	(servers with XCC2 only) Amount of available space in the repository, in KB
canisters	Array of objects	(Flex System storage devices only) Information about each storage canister. See GET /canisters for details.

Attributes	Type	Description
canisterSlots	Integer	(Flex System storage devices only) Canister slots
cimEnabled	Boolean	
cmmDisplayName	String	Display name provided by the CMM
cmmHealthState	String	Health summary that corresponds to the highest event severity of all the devices For servers or storage devices in a chassis, this can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown** For rack servers, this can be one of the following values. • **Informational** • **Warning** • **Minor** • **Major** • **Critical** • **Fatal** • **Unknown**
complexID	Integer	Complex ID
contact	String	Contact
dataHandle	Long	Time stamp of the last status update
description	String	Description that was provided by the CMM
deviceDrivers	Array of objects	Information about each device drivers in the server
displayName	String	Display name
driverClass	String	Class
driverClassId	String	Class ID
driverFiles	Array of objects	Information about each device driver file
path	String	File path
version	String	File version
installDate	String	Installation date
instID	String	Installation ID
localInfName	String	Local INF file name
name	String	Name
releaseDate	String	Release date
version	String	Version
diskDriveSensorInfo	Array of strings	List of disk-drive sensor names

Attributes	Type	Description
dnsHostnames	Array of strings	List of DNS hosts that are configured in the baseboard management controller
domainName	String	Domain name
driveBays	Integer	Drive bays
drives	Array of objects	(IMM and ThinkServer based servers only) Information about each drive details
bay	Integer	Drive bay
capacity	Integer	Drive capacity
interfaceType	String	(ThinkServer servers only) Drive interface type
mediaType	String	(ThinkServer servers only) Drive media type
raidPresence	String	(ThinkServer servers only) Type of RAID method. This can be one of the following values. • **Regular**. The drive is part of a RAID. • **Non-RAID drive**. This drive is not part of a RAID.
speed	String	(ThinkServer servers only) Drive speed
state	String	(ThinkServer servers only) Drive state. This can be one of the following values. • **active** • **stopped** • **transitioning**
embeddedHypervisorPresence	Boolean	This can be one of the following values. • **true** • **false**
encapsulation	Object	Information about encapsulation
encapsulationMode	String	Encapsulation (firewall settings) mode. This can be one of the following values. • **notSupported**. Encapsulation is not supported for this node. • **normal**. Encapsulation is disabled for this node.The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process. • **encapsulationLite**. Encapsulation is enabled for this node.When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.
nonBlockedIpAddressList	Array of strings	List of non-blocked IP addresses. This attribute is available only when the encapsulation mode is “encapsulationLite”.
errorFields	Array of objects	Information about each component with an error status. The status value can be one of the following values. • **FETCH_SUCCESS** • **FETCH_FAILED** • **NO_CONNECTOR** • **FATAL_EXCEPTION** • **NETWORK_FAIL**

Attributes	Type	Description
excludedHealthState	String	Highest severity alert with exclusions. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
expansionCards	Array of objects	Information about each expansion card
bay	Integer	Number of available bays
class	String	Class (basic function) of the PCI device. This can be one of the following values. • **Bridge** • **Communication** controller • **Coprocessor** • **Display** controller • **Docking** station • **Encryption controller** • **Generic system peripheral** • **Input device controller** • **Intelligent controller** • **Mass storage controller** • **Memory controller** • **Multimedia controller** • **Network controller** • **Non-Essential Instrumentation** • **Processing accelerators** • **Processor** • **Satellite communications controller** • **Serial bus controller** • **Signal processing controller** • **Unassigned class** • **Unclassified device** • **Unknown device** • **Wireless controller**
firmware	Array of objects	Information about each PCI device firmware
build	String	Firmware build
classifications	Array of integers	List of firmware type codes
date	String	Firmware date
name	String	Firmware name
revision	String	Firmware revision
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**

Attributes	Type	Description
softwareID	String	Firmware ID
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive** • **Pending**
type	String	Firmware type, such as UEFI, MP, or DSA
version	String	Firmware version
fodUniqueID	String	Feature on demand (FoD) unique ID
isAddOnCard	Boolean	Identifies whether the device is an add-on card. This can be one of the following values. • **true**. The device is an add-on card • **false**. The device is not an add-on card
isAgentless	Boolean	Identifies whether the device is agentless. This can be one of the following values. • **true**. The device is agentless. • **false**. The device is not agentless.
isPLDMUpdateSupported	Boolean	Identifies whether the Platform Level Data Model updates are supported. This can be one of the following values. • **true**. PLDM update is supported. • **false**. PLDM update is not supported.
manufacturer	String	Add-in card manufacturer
name	String	Description
pciBusNumber	String	PCI bus number
pciDeviceNumber	String	PCI device number
pciFunctionNumber	String	PCI function number
pciRevision	String	PCI revision number
pciSubID	String	PCI subsystem ID
pciSubVendorID	String	PCI sub-vendor ID
portInfo	Object	Information about the ports
physicalPorts	Array of objects	Information about each physical port
logicalPorts	Array of objects	Information about each associated logical port
addresses	String	Assigned addresses
logicalPortIndex	Integer	Number of logical ports
portNumber	Integer	Number of the logical port

Attributes	Type	Description
portType	String	Logical port type. This can be one of the following values. • **ATM** • **BLUETOOTH** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **INFRARED** • **OTHER** • **TOKENRING** • **UNKNOWN** • **WIRELESSLAN**
vnicMode	Boolean	Identifies whether this is a vNIC port. This can be one of the following values. • **true**. This is a vNIC port. • **false**. This is not a vNIC port.
peerBay	Integer	Peer I/O Module bay
physicalPortIndex	Integer	Number of physical ports
portNumber	Integer	Number of the physical port
portType	String	Physical port type. This can be one of the following values. • **ATM** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **OTHER** • **TOKENRING** • **UNKNOWN**
speed	Long	Link speed, in Gbps (for example, 2.5)
status	String	Link status. This can be one of the following values.Link status. This can be one of the following values. • **up** • **down** • **unknown**
posID	String	Device ID
vpdID	String	VPD ID
expansionCardSlots	Integer	Expansion card slots
expansionProducts	Array of strings	(Servers with blade expanders installed only) List of expansion hardware. This can be one or more of the following values. • **expansionProducts** • **expansionCards** • **addinCards** • **pciExpressCards**
expansionProductSlots	Integer	(Servers with blade expanders installed only) Expansion product slots

Attributes	Type	Description
expansionProductType	String	Expansion product type. This can be one of the following values. • **SEN**. StorageExpansionNode • **PEN**. PciExpansionNode • **Expansion card** • **Addin Card** • **PCI Express Card** • **Unknown**
faceplateIDs	Array of objects	Information about each faceplate ID
deviceId	Integer	
entityId	Integer	
fruNumber	String	(ThinkSystem rack servers only)
name	String	
partNumber	String	(ThinkSystem rack servers only)
posID	Integer	
productId	Integer	
serialNumber	String	(ThinkSystem rack servers only)
vpdID	Integer	
fans	Array of objects	Information about each fan in the device
description	String	Fan description
healthState	String	Fan health status. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
name	String	Fan name
slot	String	Slot number for this fan
slots	Integer	Number of fan slots
speed	Integer	Fan speed
status	String	Fan activity status. This can be one of the following values. • **Active** • **Inactive**
FeaturesOnDemand	Object	Information about each Features on Demand (FoD) key installed on the device
features	Array of strings	List of features that are active for the tier

Attributes	Type	Description
tierLevel	Integer	Tier level of the XClarity Controller feature key that is installed. This can be one of the following values. • **0**. • **1**. XClarity Controller Standard • **2**. XClarity Controller Advanced • **3**. XClarity Controller Enterprise
firmware	Array of objects	Information about each firmware that is installed on the device
build	String	Firmware build
classifications	Array of strings	
date	String	Firmware date
name	String	Firmware name
revision	String	
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive** • **Pending**
type	String	Firmware type, such as BMC-Primary, BMC-Backup, UEFI, MP, or DSA
version	String	Firmware version
flashStorage	Array of objects	Information about each flash-storage device
defaultBlockSize	Long	Flash storage device block size
description	String	Flash storage description
serialNumber	String	Flash storage serial number
firmware	Array of objects	Information about each flash-storage firmware
build	String	Firmware build
classifications	Array of integers	List of firmware type codes
date	String	Firmware date
name	String	Firmware name
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
softwareID	String	Software identifier

Attributes	Type	Description
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive**
type	String	Firmware type, such as UEFI, MP, or DSA
version	String	Firmware version
manufacturer	String	Flash storage manufacturer
maxMediaSize	Long	Flash storage device media size
name	String	Flash storage description
partNumber	String	Flash storage part number
slotNumber	Integer	Flash storage slot number
uuid	String	Flash storage UUID
FQDN	String	Fully qualified domain name
FRU	String	FRU part number
fruSerialNumber	String	FRU serial number
hasOS	String	Identifies whether an operating system is installed. This can be one of the following values. • **true**. Operating system is installed. • **false**. Operating system is not installed.
height	Integer	(Rack Server only) Height of the server
hostMacAddresses	String	Host MAC address
hostname	String	Hostname
ipInterfaces	Array of objects	Information about each IP address assigned to the baseboard management controller
IPv4assignments	Array of objects	Information about each IPv4 address
address	String	IPv4 address
gateway	String	IPv4 gateway
id	Integer	IPv4 assignment ID
subnet	String	IPv6 subnet mask
type	String	Type of the IPv4 assignment. This can be one of the following values. • **INUSE** • **CONFIGURED** • **ALIAS** • **UNKNOWN**
IPv4DHCPmode	String	IP address assignment method. This can be one of the following values. • **STATIC_ONLY** • **DHCP_ONLY** • **DHCP_THEN_STATIC** • **UNKNOWN**

Attributes	Type	Description
IPv4enabled	Boolean	Identifies whether IPv4 is enabled. This can be one of the following values. • **true**. IPv4 is enabled • **false**. IPv4 is disabled
IPv6assignments	Array of objects	Information about each IPv6 address
address	String	IPv6 address
gateway	String	IPv6 gateway
id	Integer	IPv6 assignment ID
prefix	Integer	IPv6 prefix
scope	String	Scope of the IPv6 assignment. This can be one of the following values. • **Global** • **LinkLocal** • **Unknown**
source	String	Source of the IPv6 assignment. This can be one of the following values. • **DHCP** • **Statelesss** • **Static** • **Other** • **Unknown**
type	String	Type of the IPv6 assignment. This can be one of the following values. • **INUSE** • **CONFIGURED** • **ALIAS** • **UNKNOWN**
IPv6DHCPenabled	Boolean	Identifies whether IPv6 DHCP is enabled. This can be one of the following values. • **true**. IPv6 DHCP is enabled • **false**. IPv6 DHCP is disabled
IPv6enabled	Boolean	Identifies whether IPv6 is enabled. This can be one of the following values. • **true**. IPv6 is enabled • **false**. IPv6 is disabled
IPv6statelessEnabled	Boolean	Identifies whether IPv6 stateless is enabled. This can be one of the following values. • **true**. IPv6 stateless is enabled • **false**. IPv6 stateless is disabled
IPv6staticEnabled	Boolean	Identifies whether IPv6 static is enabled. This can be one of the following values. • **true**. IPv6 static is enabled • **false**. IPv6 static is disabled
label	String	Label
name	String	Name
ipv4Addresses	Array of strings	List of IPv4 addresses
ipv6Addresses	Array of strings	List of IPV6 addresses

Attributes	Type	Description
isConnectionTrusted	Boolean	Identifies whether communication with the device is trusted using peer certificate authentication. This can be one of the following values. • **true**. The connection is trusted. • **false**. The connection is not trusted.
isITME	Boolean	Indicates whether the server is a Flex System compute node. This can be one of the following values. • **true**. The node is a compute node. • **false**. The node is a rack or tower server, or storage device
isRemotePresenceEnabled	Boolean	Indicates whether remote presence is enabled. This can be one of the following values. • **true**. Remote presence is enabled • **false**. Remote presence is disabled
isScalable	Boolean	This can be one of the following values. • **true** • **false**
lanOverUsb	String	Identifies whether LAN over USB is enabled. This can be one of the following values. • **enabled**. LAN over USB is enabled. • **disabled**. LAN over USB is disabled.
lanOverUsbPortForwardingModes	Array of objects	Information about each Ethernet-over-USB port forwarding mode This attribute requires Lenovo XClarity Administrator v1.2.0.
externalIPAddress	String	IP address of the port
state	String	Identifies whether the Ethernet over USB port forwarding mode is enabled or disabled. This can be one of the following values. • **enabled**. • **disabled**.
type	String	Type of LAN over USB port. This can be one of the following values. • **OSDeploy**.
lastOfflineTimestamp	String	Timestamp when the device was offline last
leds	Array of objects	Information about each server LED
color	String	LED color. This can be one of the following values. • **Red** • **Amber** • **Yellow** • **Green** • **Blue** • **Unknown**
conditions	String	(ThinkServer servers only) LED condition. This can be one of the following values. • **Fault**. • **Warning**.
location	String	LED location. This can be one of the following values. • **Front panel** • **Lightpath Card** • **Planar** • **FRU** • **Rear Panel** • **Unknown**
name	String	LED name

Attributes	Type	Description
state	String	LED state. This can be one of the following values. • **Off** • **On** • **Blinking** • **Unknown**
location	Object	Information about the location of the server or Flex System storage device
location	String	Location
lowestRackUnit	Integer	Lowest rack unit
rack	String	Rack
room	String	Room
logicalID	Integer	Logical ID (Scalable complex and **partitionEnabled** is true)
m2Presence	Boolean	Indicates whether the node contains M.2 storage. This can be one of the following values. • **true**. M.2 storage is present. • **false**. M.2 storage is not present.
macAddress	String	MAC address
machineType	String	Server machine type
manufacturer	String	Manufacturer
manufacturerId	String	Manufacturer ID
memoryModules	Array of objects	(Intel Optane Persistence Memory only) Information about each memory module
additionalInfo	Object	Additional information about the memory module
appDirectCapacity	Integer	Capacity, in MiB, that is allocated for AppDirect
firmware	Object	Information about memory module firmware
build	String	Firmware build
classifications	Array of integers	List of firmware type codes
date	String	Firmware date
name	String	Firmware name
revision	String	Firmware revision
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
softwareID		Firmware ID
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive**
type	String	Firmware type
version	String	Firmware version

Attributes	Type	Description
inaccessibleCapacity	Integer	Capacity, in MiB, that cannot be accessed due to licensing issues
memoryCapacity	Integer	Capacity, in MiB, that is allocated for memory
securityStateString	String	
capacity	Long	Capacity
displayName	String	Display name
healthState	String	
fipsMode	String	
fruPartNumber	String	FRU part number, if applicable
manufacturer	String	Manufacturer
metrics	Object	
aitDramStatus	String	
alarmTrips	Object	
spareBlock	String	
temperature	String	
healthStatusReason	String	
healthStatusString	String	
latchedDirtyShutdown-Count	String	
latchedDirtyShutdownSta-tus	String	
predictedMediaLifeLeftPer-cent	String	
mpfa	Object	Information about memory failure prediction analytics
mpfaHealthStatus	Object	Information about health status
major	Integer	Number of major health events
minor	Integer	Number of warning (minor) health events
mpfaSevereFaults	Array of objects	Information about each severe fault
errorCnt	Integer	Number of errors
faultType	Integer	Fault type
location	String	Fault location
timestamp	Long	Timestamp when the fault occurred
model	String	Model
operatingMemoryMode	Array of strings	List of memory operating modes. This can be one of the following values. • Volatile • Persistent
partNumber	String	Part number

Attributes	Type	Description
present	Boolean	
serialNumber	String	Serial number
slot	Integer	Slot
speed	Long	Number of data-transfer operations that occur in each second, in MT/s (megatransfers per second)
speedMBs	Long	Amount of data that is transferred in each second, in MB/s (megabytes per second)
type	String	Type
memorySlots	Integer	Number of memory slots
mgmtProcIPaddress	String	IP address used by Lenovo XClarity Administrator to manage this resource
mgmtProcType	String	Type of management controller. This can be one of the following values. • **FSP** • **IMM2** • **lenovo-AMI-controller** • **XCC** • **XCC2** • **UNKNOWN**
model	String	Server model
name	String	Name that is displayed in the user interface for this device The value of this attribute is determined by **preferredDisplayName** attribute in the GET /aicc method. For example, if the **preferredDisplayName** attribute is set to “hostname,” then the value for this **name** attribute is the same as the **hostname** attribute in the GET /aicc method.
nist	Object	Information about NIST compliance
currentValue	String	Cryptography mode to be used. This can be one of the following values. • **Unknown** • **Compatibility** • **Nist_800_131A_Strict** • **Nist_800_131A_Custom**
possibleValues	Array of strings	List of possible values
onboardPciDevices	Array of objects	Information about each-board PCI device

Attributes	Type	Description
class	String	Class (basic function) of the PCI device. This can be one of the following values. • **Bridge** • **Communication** controller • **Coprocessor** • **Display** controller • **Docking** station • **Encryption controller** • **Generic system peripheral** • **Input device controller** • **Intelligent controller** • **Mass storage controller** • **Memory controller** • **Multimedia controller** • **Network controller** • **Non-Essential Instrumentation** • **Processing accelerators** • **Processor** • **Satellite communications controller** • **Serial bus controller** • **Signal processing controller** • **Unassigned class** • **Unclassified device** • **Unknown device** • **Wireless controller**
firmware	Array of objects	Information about each PCI-device firmware
build	String	Firmware build
classifications	Array of integers	List of firmware type codes
date	String	Firmware date
name	String	Firmware name
revision		Firmware revision
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
softwareID	String	Firmware ID
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive**
type	String	Firmware type, such as UEFI, MP, or DSA
version	String	Firmware version
fodUniqueID	String	FoD unique ID
isAddOnCard	Boolean	Identifies whether the device is an add-on card. This can be one of the following values. • **true**. The device is an add-on card • **false**. The device is not an add-on card

Attributes	Type	Description
isAgentless	Boolean	Identifies whether the device is agentless. This can be one of the following values. • **true**. The device is agentless. • **false**. The device is not agentless.
isPLDMUpdateSupported	Boolean	Identifies whether the Platform Level Data Model updates are supported. This can be one of the following values. • **true**. PLDM update is supported. • **false**. PLDM update is not supported.
name	String	Description
pciBusNumber	String	PCI bus number
pciDeviceNumber	String	PCI device number
pciFunctionNumber	String	PCI function number
pciRevision	String	PCI revision
pciSubID	String	PCI subsystem ID
pciSubVendorID	String	PCI sub-vendor ID
portInfo	Object	Information about the ports
physicalPorts	Array of objects	Information about each physical port
logicalPorts	Array of objects	Information about each associated logical ports
addresses	String	Assigned addresses
logicalPortIndex	Integer	Number of logical ports
portType	String	Logical port type. This can be one of the following values. • **ATM** • **BLUETOOTH** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **INFRARED** • **OTHER** • **TOKENRING** • **UNKNOWN** • **WIRELESSLAN**
portNumber	Integer	Number of the logical port
vnicMode	Boolean	Identifies whether this is a vNIC port. This can be one of the following values. • **true**. This is a vNIC port. • **false**. This is not a vNIC port.
peerBay	Integer	Peer I/O Module bay
physicalPortIndex	Integer	Number of physical ports
portNumber	Integer	Number of the physical port

Attributes	Type	Description
portType	String	Physical port type. This can be one of the following values. • **ATM** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **OTHER** • **TOKENRING** • **UNKNOWN**
posID	String	Device ID
vpdID	String	VPD ID
osInfo	Object	Information about the operating system that is installed on the server
description	String	Operating system name and version
hostname	String	Hostname or IP address of the operating system
os_country	String	(Lenovo ThinkEdge servers only) Country
os_language	String	(Lenovo ThinkEdge servers only) Language
os_name	String	(Lenovo ThinkEdge servers only) Name
os_version	String	(Lenovo ThinkEdge servers only) Version
storedCredential	String	URI of the stored-credential account that is used to access the operating system (for example, `storedCredentials/2653`)
overallHealthState	String	Highest severity of all alerts. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
parent	Object	Information about the parent of the server or Flex System storage device, if applicable
uri	String	Parent URI
uuid	String	Parent UUID
parentComplexID	String	(Scalable complex only) Parent complex ID
parentPartitionUUID	String	(Scalable complex only) Parent partition UUID
partitionID	Integer	Partition ID
partitionEnabled	Boolean	(Scalable complex only) Indicates whether partition is enabled. This can be one of the following values. • **true**. Partition is enabled • **false**. Partition is disabled
partNumber	String	Part number
pciCapabilities	Array of strings	List of PCI capabilities

Attributes	Type	Description
pciDevices	Array of objects	Information about each PCI device
class	String	Class (basic function) of the PCI device. This can be one of the following values. • **Bridge** • **Communication** controller • **Coprocessor** • **Display** controller • **Docking** station • **Encryption controller** • **Generic system peripheral** • **Input device controller** • **Intelligent controller** • **Mass storage controller** • **Memory controller** • **Multimedia controller** • **Network controller** • **Non-Essential Instrumentation** • **Processing accelerators** • **Processor** • **Satellite communications controller** • **Serial bus controller** • **Signal processing controller** • **Unassigned class** • **Unclassified device** • **Unknown device** • **Wireless controller**
device	String	(ThinkServer severs only) PCI device name
firmware	Array of objects	Information about each PCI device firmware
build	String	Firmware build
classifications	Array of integers	List of firmware type codes
date	String	Firmware date
name	String	Firmware name
revision	String	Firmware revision
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
softwareID	String	Firmware ID
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive** • **Pending**
type	String	Firmware type, such as UEFI, MP, or DSA
version	String	Firmware version
fodUniqueID	String	FoD unique ID

Attributes	Type	Description
FRU	String	FRU part number
fruSerialNumber	String	FRU serial number
isAddOnCard	Boolean	Identifies whether the device is an add-on card. This can be one of the following values. • **true**. The device is an add-on card • **false**. The device is not an add-on card
isAgentless	Boolean	Identifies whether the device is agentless. This can be one of the following values. • **true**. The device is agentless. • **false**. The device is not agentless.
isPLDMUpdateSupported	Boolean	Identifies whether the Platform Level Data Model updates are supported. This can be one of the following values. • **true**. PLDM update is supported. • **false**. PLDM update is not supported.
manufacturer	String	Manufacturer
name	String	Description
partNumber	String	Part number
pciBusNumber	String	PCI bus number
pciDeviceNumber	String	PCI device number
pciFunctionNumber	String	PCI function number
pciRevision	String	PCI revision
pciSegmentNumber	String	PCI segment number, if supported
pciSubID	String	PCI subsystem ID
pciSubVendorID	String	PCI sub-vendor ID
portInfo	Object	Information about the ports
physicalPorts	Array of objects	Information about each physical port
logicalPorts	Array of objects	Information about each associated logical port
addresses	String	Assigned addresses
logicalPortIndex	Integer	Number of logical ports
portNumber	Integer	Number of the logical port
portType	String	Logical port type. This can be one of the following values. • **ATM** • **BLUETOOTH** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **INFRARED** • **OTHER** • **TOKENRING** • **UNKNOWN** • **WIRELESSLAN**

Attributes	Type	Description
vnicMode	Boolean	Identifies whether this is a vNIC port. This can be one of the following values. • **true**. This is a vNIC port. • **false**. This is not a vNIC port.
peerBay	Integer	Peer Flex switch bay
physicalPortIndex	Integer	Number of physical ports
portNumber	Integer	Number of the physical port
portType	String	Physical port type. This can be one of the following values. • **ATM** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **OTHER** • **TOKENRING** • **UNKNOWN**
speed	Long	Link speed, in Gbps (for example, 2.5)
status	String	Link status. This can be one of the following values. • **up** • **down** • **unknown**
posID	String	Device ID
productName	String	PCI device product name
slotName	String	Name of the PCI device slot
slotNumber	String	Number of the PCI device slot
slotSupportsHotPlug	Boolean	Indicates whether the PCI device supports hot plug. This can be one of the following values. • **true**. Hot plug is supported. • **false**. Hot plug is not supported.
subClass	String	(ThinkServer servers only)
subDevice	String	(ThinkServer servers only)
subVendor	String	(ThinkServer servers only)
type	String	(ThinkServer servers only)
uuid	String	UUID of the PCI device
vpdID	String	VPD ID
pciExpressCards	Array of objects	(Servers with PCI Express cards installed only) Information about each PCI express card
fodUniqueID	String	Feature on demand (FoD) unique ID
isAddOnCard	Boolean	Identifies whether the device is an add-on card. This can be one of the following values. • **true**. The device is an add-on card • **false**. The device is not an add-on card

Attributes	Type	Description
isAgentless	Boolean	Identifies whether the device is agentless. This can be one of the following values. • **true**. The device is agentless. • **false**. The device is not agentless.
name	String	Description
pciBusNumber	String	PCI bus number
pciDeviceNumber	String	PCI device number
pciFunctionNumber	String	PCI function number
pciSubID	String	PCI subsystem ID
pciSubVendorID	String	PCI sub-vendor ID
portInfo	Object	Information about the ports
physicalPorts	Array of objects	Information about each physical port
logicalPorts	Array of objects	Information about each associated logical port
addresses	String	Assigned addresses
logicalPortIndex	Integer	Number of logical ports
portNumber	Integer	Number of the logical port
portType	String	Logical port type. This can be one of the following values. • **ATM** • **BLUETOOTH** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **INFRARED** • **OTHER** • **TOKENRING** • **UNKNOWN** • **WIRELESSLAN**
vnicMode	Boolean	Identifies whether this is a vNIC port. This can be one of the following values. • **true**. This is a vNIC port. • **false**. This is not a vNIC port.
peerBay	Integer	Peer Flex switch bay
physicalPortIndex	Integer	Number of physical ports
portNumber	Integer	Number of the physical port

Attributes	Type	Description
portType	String	Physical port type. This can be one of the following values. • **ATM** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **OTHER** • **TOKENRING** • **UNKNOWN**
posID	String	Device ID
vpdID	String	VPD ID
pciExpressCardSlots	Integer	(Servers with PCI Express cards installed only) PCI Express card slots
physicalID	Integer	(Scalable complex only) Position of server in the complex
ports	Array of objects	Information about each port
ioModuleBay	Integer	Attached IO module bay number
portNumber	Integer	Port number
posID	String	Position ID
powerAllocation	Object	Information about power allocation.
maximumAllocatedPower	Long	Maximum power allocated to the server
minimumAllocatedPower	Long	Minimum power allocated to the server
powerCappingPolicy	Object	(Rack Server only)
cappingACorDCMode	String	Capping AC or DC mode. This can be one of the following values. • **AC** • **DC** • **Unknown**
cappingPolicy	String	Capping policy. This can be one of the following values. • **OFF** • **STATIC** • **UNKNOWN**
currentPowerCap	Long	Current power cap
currentPowerCap	Long	Current power cap
maximumPowerCappingHot-PlugLevel	Long	Maximum power capping hot plug level
maxPowerCap	Long	Maximum power capping level
minimumHardCapLevel	Long	Minimum hard capping level
minimumPowerCappingHot-PlugLevel	Long	Minimum power capping hot plug level
minPowerCap	Long	Minimum power capping level
powerCappingAllocUnit	String	Power capping allocation unit

Attributes	Type	Description
powerStatus	Integer	This can be one of the following values. • **0**. Unknown • **5**. Off • **8**. On • **17**. Standby
powerSupplies	Array of objects	(Rack servers only) Information about each power supply
cmmDisplayName	String	Assigned CMM display name
cmmHealthState	String	Health state of the CMM. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
dataHandle	Long	Time stamp of the last status update
description	String	Assigned component description
excludedHealthState	String	Excluded health status. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
firmware	Array of objects	Information about each power-supply firmware
build	String	Firmware build
classifications	Array of integers	List of firmware type codes
date	String	Firmware date
name	String	Firmware name
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
softwareID	String	Firmware ID
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive**
type	String	Firmware type, such as UEFI, MP, or DSA
version	String	Firmware version
FRU	String	FRU part number

Attributes	Type	Description
fruSerialNumber	String	FRU serial number
hardwareRevision	String	Hardware revision
healthState	String	Health state of the server. This can be one of the following values. • **NA** • **BLADE_INIT_FAILED** • **COMMUNICATION_FAILURE** • **CRITICAL** • **DISCOVERY** • **GOOD** • **FLASHING** • **INSUFFICIENT_POWER** • **KERNEL_MODE** • **MAINTENANCE** • **MAJOR_FAILURE** • **MINOR_FAILURE** • **NO_POWER** • **NONRECOVERABLE** • **POWER_DENIED** • **SAVING** • **WARNING**
inputVoltageIsAC	Boolean	Identifies whether the input voltage is ac or dc. This can be one of the following values. The value is valid only if **inputVoltageMin** and **inputVoltageMax** are valid. • **true**. ac • **false**. dc
inputVoltageMax	Integer	Maximum input voltage. A value of -1 mean it has not been set yet.
inputVoltageMin	Integer	Minimum input voltage. A value of -1 means it has not been set yet.
leds	Array of objects	Information about each power-supply LED
color	String	LED color. This can be one of the following values. • **Red** • **Amber** • **Yellow** • **Green** • **Blue** • **Unknown**
location	String	LED location. This can be one of the following values. • **Front panel** • **Lightpath Card** • **Planar** • **FRU** • **Rear Panel** • **Unknown**
name	String	LED name
state	String	LED state. This can be one of the following values. • **Off** • **On** • **Blinking** • **Unknown**
machineType	String	Machine type
manufactureDate	String	Manufacture date

Attributes	Type	Description
manufacturer	String	Manufacturer
manufacturerId	String	Manufacturer ID
model	String	Power-supply model
name	String	User-defined name, if available. Otherwise, this is one of the following values. • component name • serial number • UUID
overallHealthState	String	Overall health state of the server. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
parent	Object	Information about the power allocation
uri	String	URI of the parent device
uuid	String	UUID of the parent device
partNumber	String	Part number
posID	String	Position ID
powerAllocation	Object	Information about the power allocation
totalInputPower	Long	Total input power
totalOutputPower	Long	Total output power
powerState	String	Current power state of the power supply. This can be one of the following values. • **Off** • **On** • **ShuttingDown** • **Standby** • **Hibernate** • **Unknown**
productId	String	Product ID
productName	String	Product name
serialNumber	String	Serial number
slots	Array of strings	List of used power-supply primary slots
type	String	Resource type. This value is always “PowerSupply.”
uri	String	URI
userDescription	String	User description
uuid	String	UUID

Attributes	Type	Description
vpdID	String	VPD ID
primary	Boolean	(Scalable complex only) Identifies whether the host platform is the primary node when the host platform is configured as a scalable complex. This can be one of the following values. • **true**. This is the primary node. • **false**. This is not the primary node.
processors	Array of objects	Information about each processor
ProcessorIntelSpeedSelect	Object	Information about the Intel processor speed setting
currentValue	String	Current setting from the baseboard management controller
possibleValues	Array of strings	List of possible values
cores	Integer	Number of cores
displayName	String	Display name
family	String	Family
healthState	String	Health state of the processor. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
manufacturer	String	Manufacturer
maxSpeedMHZ	Integer	Maximum processor speed, in MHz
partNumber	String	
present	Boolean	
productVersion	String	Product version
serialNumber	String	
slot	Integer	Slot
socket	String	Socket information. For servers, this is the socket number (for example, “Socket 1”). For scalable complexes, this is the node and socket number (for example, “Node 1 Socket 1”).
speed	Double (float)	Speed
tdpWatts	Integer	Thermal design power usage, in Watts
processorSlots	Integer	Number of processor slots
productID	String	Product ID
productName	String	Product name
raidSettings	Array of object	Information about each RAID device

Attributes	Type	Description
batteryData	Array	
description	String	RAID devices description
diskDrives	Array of objects	XCC-based servers only Information about each disk drive
bay	Integer	Bay or slot number
blockSize	Long	Block size
capacity	Integer	(M.2 drives only) Storage capacity, in KB
description	String	Description
diskState	String	Disk-drive state
encryptionStatus	Sting	Indicates whether the disk drive is encrypted. This can be one of the following values. • **unencrypted**. The drive is not encrypted. • **locked**. The drive is encrypted, and the host is power off. • **unlocked**. The drive is encrypted, and the host is power on.
firmware	Array of objects	(M.2 and NVM3 drives only) Information about each disk-drive firmware
build	String	Firmware build.
classifications	Array of integers	List of firmware type codes
date	String	Firmware date.
name	String	Firmware name.
revision	String	Firmware revision
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
softwareID	String	Firmware ID
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive**
type	String	Firmware type, such as UEFI, MP, or DSA
version	String	Firmware version.
FRU	String	FRU
healthState	String	Device health state
hotSpareType	String	Type of hot spare drive. This can be one of the following values. • **Global** • **None**
interfaceType	String	Interface type
largestAvailableSize	Integer	
m2Location	String	(M.2 drives only) Location of M.2 drive and bay

Attributes	Type	Description
manufacturer	String	Manufacturer
mediaType	String	Media type
model	String	Model
name	String	Drive name
numberOfBlocks	Long	Number of blocks
partNumber	String	Part number
remainingLife	Integer	Indicate the amount of life that remains for a solid-state drive (SSD). This can be one of the following values. • **0 - 100**. The percent of remaining life • **-1**. Unknown (default) • **-2**. Information is not available • **-3**. The drive is not an SSD
serialNumber	String	Serial number
temperature	Integer	Device temperature
uuid	String	UUID
firmware	Array of objects	Information about each RAID firmware
build	String	Firmware build
classifications	Array of integers	List of firmware type codes
date	String	Firmware date
name	String	Firmware name
revision	String	Firmware revision
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
softwareID		Firmware ID
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive** • **Pending**
type	String	Firmware type, such as UEFI, MP, or DSA
version	String	Firmware version
isAddOnCard	Boolean	Identifies whether the RAID adapter is an add-on card. This can be one of the following values. • **true**. The RAID adapter is an add-on adapter. • **false**. The RAID adapter is an on-board adapter.
model	String	
name	String	RAID devices name
pciFirmware	Array of objects	

Attributes	Type	Description
slotNumber	String	RAID adapter slot number If the RAID adapter is an on-board adapter, this value is null.
storagePools	Array of objects	Information about each storage pool
arrayUid	String	
arrayStatus	String	
combinedRaidLevel	String	Combined RAID level. This can be one of the following values. • **0**. Striping • **1**. Mirroring • **5**. Distributed dual-parity • **6**. Striping with-parity • **10**. Disk mirroring and disk striping (1+0) • **50**. Distributed parity and disk striping (5+0) • **60**. Distributed dual-parity and disk striping (6+0) • **00**. **Note:** RAID level 0, 1, or 5 are supported on all serves. RAID level 6, 10, 50, 60, and 00 are supported only on ThinkSystem servers with XCC version 2.1 and later. (ThinkSystem SR950 requires XCC version 1.4 or later).
diskDrives	Array of objects	Information about each disk drive in the storage pool
bay	Integer	
blockSize	Integer	
capacity	Long	
description	String	
diskState	String	
firmware	Array of objects	Information about each disk-drive firmware
build	String	Firmware build
classifications	Array of integers	List of firmware type codes
date	String	Firmware date
name	String	Firmware name
revision	String	Firmware revision
role	String	Firmware role. This can be one of the following values. • **Primary** • **Backup** • **Temporary** • **Permanent**
softwareID	String	Firmware ID
status	String	Firmware status. This can be one of the following values. • **Active** • **Inactive** • **Pending**
type	String	Firmware type, such as UEFI, MP, or DSA

Attributes	Type	Description
version	String	Firmware version
FRU	String	
healthState	String	
interfaceType	String	
largestAvailableSize	Integer	
m2Location	String	
manufacturer	String	
mediaType	String	
model	String	
name	String	
numberOfBlocks	Long	
remainingLife	Integer	Indicate the amount of life that remains for a solid-state drive (SSD). This can be one of the following values. • **0 - 100**. The percent of remaining life • **-1**. Unknown (default) • **-2**. Information is not available • **-3**. The drive is not an SSD
partNumber	String	
serialNumber	String	
uuid	String	
description	String	
name	String	
raidLevel	Integer	
remainingSpace	Integer	
storageVolumes	Array of objects	Information about each storage volume
accessPermission	String	
blockSize	Integer	
bootable	Boolean	
description	String	
driveIndex	Integer	
health	String	
isSDRAID	String	
LUN	Integer	
name	String	
numberOfBlocks	Long	
primaryPartition	Integer	

Attributes	Type	Description
removable	Boolean	
stripeSize	Integer	
targetType	String	
volumeID	String	
volumeStatus	String	
volumeType	String	
volumeOwner	String	
volumeUID	String	
totalManagedSpace	Long	
storageVolumes	Array of objects	
uuid	String	RAID devices UUID
releaseName	String	
secureBootMode	Object	Information about the secure boot mode
currentValue	String	Current secure boot mode from the baseboard management controller
possibleValues	Array of strings	List of possible boot mode values
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
identityManagementSyste-mEnabled	String	
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports the ability to choose managed authentication. • **false**. This device does not support the ability to choose managed authentication.
publicAccess	Boolean	Indicates whether the device can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device
storedCredentials	Array of objects	Information about each stored credential that is associated with this device, if applicable
description	String	Description of the stored credential
id	String	ID of the stored credential

Attributes	Type	Description
userName	String	Name of the stored credential
uri	String	URI of the device
securityMode	String	(servers with XCC2 only) Security Mode. This can be one of the following values. • **NIST SP 800-131A** • **Compatibility Security** • **Standard Security** • **Enterprise Strict Security**
selLog	Boolean	Indicates whether the SEL log is supported and present on this server. This can be one of the following values. • **true**. SEL log is supported. • **false**. SEL log is not supported.
serialNumber	String	Server serial number
slots	Array of integers	List of occupied slots
ssdWearThreshold	Integer	(ThinkSystem and ThinkAgile only) SSD remaining-life alert threshold When this threshold is exceeded, an alert is generated. The default value is 8% of remaining life.
ssoEnabled	Boolean	Indicates whether single sign-on is enabled. This can be one of the following values. • **true**. Single sign-on is enabled. • **false**. Single sign-on is disabled.
status	Object	Management status
message	String	This can be one of the following values. • **managed** • **unmanaged**
name	String	This can be one of the following values. • **MANAGED** • **UNMANAGED**
subSlots	Array of integers	List of occupied sub-slots
subType	String	Sub-type
systemGuardSetting	Object	(servers with XCC2 only) Information about System Guard settings on the device.
lockDownPolicy	String	Indicates the behavior when System Guard is enabled. This can be one of the following values. • **GenerateEventOnly**. When any inventory change is detected, an event is raised, but no other action is taken. This is default behavior on devices. • **PreventOSBooting**. When a processor or memory inventory change is detected, an event is raised. If you attempt to boot into the OS, you are warned if System Guard detects configuration changes. In this case, you are prompted to log into the baseboard management controller if the changes are unexpected; otherwise, you can continue the boot or shutdown process.

Attributes	Type	Description
osBootPreventing	Boolean	Indicates whether to prevent booting the OS when deviations are detected between the snapshot and the current inventory (when the status is **noncompliant**). This can be one of the following values. • **true**. Rebooting the OS is prevented when deviations are detected. • **false**. Rebooting the OS is allowed when deviations are detected.
status	String	Compliance status. This can be one of the following values. • **Compliant**. The snapshot matches the current inventory for the device. • **Noncompliant**. The snapshot does not match the current inventory for the device.
systemGuardEnabled	Boolean	Indicates whether System Guard is enabled. This can be one of the following values. • **true**. System Guard is enabled. • **false**. System Guard is disabled.
thinkServerFru	Array of objects	(ThinkServer servers only) Information about each ThinkServer FRU
description	String	FRU description
deviceName	String	FRU device name
manufatucturer	String	FRU manufacturer
manufatucturerDate	String	FRU manufacture date
serial	String	FRU serial number
partNumber	String	FRU part number
tlsVersion	Object	Information about the SSL or TLS protocol and version
currentValue	String	SSL or TLS protocol and version to be used. This can be one of the following values. • **unsupported** • **TLS_12**. TLS v1.2 • **TLS_13**. TLS v1.3
possibleValues	Array of strings	List of possible values
type	String	Resource type. This can be one of the following values. • **Edge Server**. ThinkSystem SE server • **ITE**. Flex System server • **Lenovo ThinkServer**. ThinkServer server • **NeXtScale**. NeXtScale server • **Rack-Tower Server**. ThinkSystem SD, ThinkSystem SR, or ThinkSystem ST, System x, Converged, or NeXtScale server • **SCU**. storage device.
udcVersion	String	(ThinkEdge servers only) Version of the management agent that is installed on the server
uri	String	URI
userDefinedName	String	User-defined name for the device
userDescription	String	User description
uuid	String	UUID

Attributes	Type	Description
vnicMode	String	VNIC mode. This can be one of the following values. • **enabled** • **disabled**
vpdID	String	VPD ID

The following example of ThinkSystem server information is returned if the request is successful.


```
{
    "accessState": "Online",
    "accountLockoutPeriod": 1,
    "activationKeys": [{
        "description": "Lenovo XClarity Controller 2 Platinum Upgrade",
        "keyExpirationDate": "",
        "keyFeatureType": 74,
        "keyIdentiferList": [{
            "keyIdentifierType": "MT",
            "keyIdentifier": "7D75SR650R112"
        }],
        "keyStatus": "VALID",
        "keyUseCount": 0,
        "keyUseLimit": 0,
        "uuid": ""
    }],
    "addinCards": [{
        "class": "Unclassified device",
        "firmware": [{
            "build": "0",
            "classifications": [13],
            "date": "",
            "name": "Gen5 Riser1 LP Retimer",
            "revision": "0",
            "softwareID": "1D494050",
            "role": "",
            "status": "Active",
            "type": "Software Bundle",
            "version": "0.0.0"
        }],
        "fodUniqueID": "",
        "FRU": "",
        "fruSerialNumber": "",
        "isAddOnCard": true,
        "isAgentless": false,
        "isPLDMUpdateSupported": true,
        "manufacturer": "Lenovo",
        "name": "Gen5 Riser1 LP Retimer",
        "partNumber": "STA7A95479",
        "pciBusNumber": "0",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "0",
        "pciRevision": "0",
        "pciSubID": "0",
        "pciSubVendorID": "0",
        "portInfo": {},
        "posID": "0",
        "productName": "Gen5 Riser1 LP Retimer",
        "slotName": "PCIe 4",
        "slotNumber": "4",
        "slotSupportsHotPlug": "false",
```

```
    "vpdID": "0"
},
...,
{
    "class": "Network controller",
    "firmware": [{
        "build": "0",
        "classifications": [13],
        "date": "",
        "name": "Firmware Bundle",
        "role": "",
        "revision": "0",
        "softwareID": "17AA4104",
        "status": "Active",
        "type": "Software Bundle",
        "version": "222.0.2.1"
    }],
    "fodUniqueID": "",
    "FRU": "01PE761",
    "fruSerialNumber": "L0NV1A2004Y",
    "isAddOnCard": true,
    "isAgentless": false,
    "isPLDMUpdateSupported": false,
    "pciBusNumber": "22",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "3",
    "pciRevision": "1",
    "pciSegmentNumber": "0",
    "pciSubID": "4104",
    "pciSubVendorID": "17aa",
    "manufacturer": "Broadcom Limited",
    "name": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
    "partNumber": "SN37A28309",
    "portInfo": {
        "physicalPorts": [{
            "logicalPorts": [{
                "addresses": "e4:3d:1a:61:88:8f",
                "logicalPortIndex": 1,
                "portNumber": 1,
                "portType": "ETHERNET",
                "vnicMode": false
            }],
            "peerBay": 0,
            "physicalPortIndex": 4,
            "portNumber": 4,
            "portType": "ETHERNET",
            "speed": -1.0,
            "status": "Down"
        }]
    },
    "posID": "1657",
    "productName": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
    "slotName": "PCIe 13",
    "slotNumber": "13",
    "slotSupportsHotPlug": "false",
    "vpdID": "14e4"
}],
"addinCardSlots": 0,
"arch": "x86",
"assetTag": "",
"backedBy": "real",
```

```
"bladeState": 0,
"bmuParamObject": null,
    "uri": "nodes/40BDB5F8D609B801C183337C180D3F29/bootOrder",
    "bootOrderList": [{
        "bootType": "BootOrder",
        "currentBootOrderDevices": ["Red Hat Enterprise Linux"],
        "possibleBootOrderDevices": ["Red Hat Enterprise Linux","CD/DVD Rom","Hard Disk",
                                     "Network","USB Storage"]
    },
    ...,
    {
        "bootType": "CDDVDROMBootOrder",
        "currentBootOrderDevices": [],
        "possibleBootOrderDevices": []
    }]
},
"bootMode": {
    "currentValue": "UEFI Mode",
    "possibleValues": ["UEFI Mode","Legacy Mode"]
},
"bootOrder": {
"bundleRepoAvailableSpaceInKB": 1951586,
"cimEnabled": false,
"cmmDisplayName": "Management Controller UUID-40BDB5F8D609B801C183337C180D3F29",
"cmmHealthState": "Normal",
"complexID": -1,
"contact": "",
"dataHandle": 1688376857592,
"description": "This resource is used to represent a chassis or other physical enclosure for a Redfish implementation.",
"deviceDrivers": null,
"diskDriveSensorInfo": ["Drive 0","Drive 1","Drive 2","Drive 3","Drive 4","Drive 5","Drive 6",
                        "Drive 7","Drive 8","Drive 9","Drive 10","Drive 11","Drive 12",
                        "Drive 13","Drive 14","Drive 15","Ext Drive","Drive Mismatch",
                        "Drive Key Fault"],
"domainName": "",
"driveBays": 2,
"drives": [],
"embeddedHypervisorPresence": false,
"encapsulation": {
    "encapsulationMode": "normal"
},
"errorFields": [],
"excludedHealthState": "Normal",
"expansionCards": [],
"expansionCardSlots": 0,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [{
    "deviceId": 84,
    "entityId": 15,
    "fruNumber": "02YH952",
    "name": "HDD_BP_2",
    "partNumber": "STA7A43893"
    "posID": 145,
    "productId": 0,
    "serialNumber": "R4SH29D0024",
    "vpdID": 112,
},
{
    "deviceId": 83,
    "entityId": 15,
```

```
    "fruNumber": "02YE087",
    "name": "HDD_BP_1",
    "partNumber": "SC57A26298"
    "posID": 144,
    "productId": 0,
    "serialNumber": "R5SH235006X",
    "vpdID": 112,
}],
"fans": [{
    "description": "Fan Fan 4 Front Tach",
    "healthState": "Normal",
    "name": "Fan 4 Front Tach",
    "slot": "4",
    "slots": 4,
    "speed": 6642,
    "status": "OK"
},
...,
{
    "description": "Fan Fan 1 Rear Tach",
    "healthState": "Normal",
    "name": "Fan 1 Rear Tach",
    "slot": "1",
    "slots": 1,
    "speed": 6300,
    "status": "OK"
}],
"FeaturesOnDemand": {
    "features": ["RDOC","REMOTE MEDIA","REMOTE CONTROL 6 USERS"],
    "tierLevel": 3
},
"firmware": [{
    "build": "*",
    "classifications": [],
    "date": "",
    "name": "Firmware:LXPM-LinuxDrivers",
    "revision": "*",
    "role": "Primary",
    "status": "Active",
    "type": "LXPMLinuxDriver",
    "version": "*"
},
...,
{
    "build": "*",
    "classifications": [],
    "date": "",
    "name": "Firmware:LXPM-WindowsDrivers",
    "revision": "*",
    "role": "Primary",
    "status": "Active",
    "type": "LXPMWindowsDriver",
    "version": "*"
}],
"flashStorage": [],
"FQDN": "Shanghai-SR650V3",
"FRU": "XXXXXXX",
"fruSerialNumber": "XXXXXXX",
"hasOS": false,
"height": 2,
"hostMacAddresses": "E4:3D:1A:61:88:8C,E4:3D:1A:61:88:8D,E4:3D:1A:61:88:8E,E4:3D:1A:61:88:8F",
```

```
"hostname": "Shanghai-SR650V3",
"inventoryState": "INVENTORY_READY",
"ipInterfaces": [{
    "name": "Manager Ethernet Interface",
    "label": "unknown",
    "IPv4assignments": [{
        "id": 0,
        "subnet": "255.255.254.0",
        "gateway": "10.240.210.1",
        "address": "10.240.211.178",
        "type": "INUSE"
    }],
    "IPv4DHCPmode": "STATIC_ONLY",
    "IPv4enabled": true,
    "IPv6assignments": [{
        "address": "2002:97b:c2bb:830:10:240:211:178",
        "id": 0,
        "gateway": "0:0:0:0:0:0:0:0",
        "prefix": 64,
        "scope": "Global",
        "source": "Static",
        "type": "INUSE"
    },
    ...,
    {
        "address": "fe80:0:0:0:922e:16ff:fe10:9806",
        "gateway": "0:0:0:0:0:0:0:0",
        "id": 0,
        "prefix": 64,
        "scope": "LinkLocal",
        "source": "Other",
        "type": "INUSE"
    }],
    "IPv6DHCPenabled": false,
    "IPv6enabled": true,
    "IPv6statelessEnabled": false,
    "IPv6staticEnabled": true
},
{
    "IPv4assignments": [],
    "IPv4DHCPmode": "UNKNOWN",
    "IPv4enabled": false,
    "IPv6assignments": [{
        "address": "fe80:0:0:0:922e:16ff:fe10:9806",
        "gateway": "0:0:0:0:0:0:0:0",
        "id": 0,
        "prefix": 64,
        "scope": "LinkLocal",
        "source": "Other",
        "type": "INUSE"
    }],
    "IPv6DHCPenabled": false,
    "IPv6enabled": false,
    "IPv6statelessEnabled": false,
    "IPv6staticEnabled": false,
    "label": "unknown",
    "name": "Manager Ethernet Over USB Interface"
}],
"isConnectionTrusted": "true",
"isITME": false,
"isScalable": false,
```

```
"ipv4Addresses": ["10.240.211.178","169.254.95.118"],
"ipv6Addresses": ["2002:97b:c2bb:830:10:240:211:178","fe80::922e:16ff:fe10:9805",
                  "fe80::922e:16ff:fe10:9806"],
"isRemotePresenceEnabled": true,
"lanOverUsb": "enabled",
"lanOverUsbPortForwardingModes": [{
    "externalIPAddress": "",
    "state": "disabled",
    "type": "OSDeploy"
}],
"lastOfflineTimestamp": -1,
"leds": [{
    "color": "Amber",
    "location": "Planar",
    "name": "DIMM 21",
    "state": "Off"
},
...,
{
    "color": "Amber",
    "location": "Planar",
    "name": "DIMM 20",
    "state": "Off"
}],
"location": {
    "lowestRackUnit": 28,
    "location": "",
    "rack": "lab123",
    "room": "test_room"
},
"logicalID": -1,
"m2Presence": false,
"macAddress": "90:2E:16:10:98:05,90:2E:16:10:98:06",
"machineType": "7D75",
"manufacturer": "Lenovo",
"manufacturerId": "Lenovo",
"memoryModules": [{
    "capacity": 16,
    "displayName": "DIMM 7",
    "fruPartNumber": "",
    "healthState": "NA",
    "manufacturer": "Samsung",
    "metrics": {
        "alarmTrips": {}
    },
    "model": "DDR5",
    "mpfa": {
            "mpfaHealthStatus": {
            "major": 0,
            "minor": 0
        },
        "mpfaSevereFaults": null
    },
    "operatingMemoryMode": ["Volatile"],
    "partNumber": "M321R2GA3BB0-CQKVG",
    "present": false,
    "serialNumber": "80CE01212401CD4F96",
    "slot": 7,
    "speed": 4800,
    "speedMBs": 0,
    "type": "DDR5",
```

```
},
{
    "capacity": 16,
    "displayName": "DIMM 23",
    "fruPartNumber": "",
    "healthState": "NA",
    "manufacturer": "Samsung",
    "metrics": {
        "alarmTrips": {}
    },
    "model": "DDR5",
    "mpfa": {
        "mpfaHealthStatus": {
            "major": 0,
            "minor": 0
        },
        "mpfaSevereFaults": null
    },
    "operatingMemoryMode": ["Volatile"],
    "partNumber": "M321R2GA3BB6-CQKEG",
    "present": false,
    "serialNumber": "80CE012210029F85AE",
    "slot": 23,
    "speed": 4800,
    "speedMBs": 0,
    "type": "DDR5",
}],
"memorySlots": 0,
"mgmtProcIPaddress": "10.240.211.178",
"mgmtProcType": "XCC2",
"model": "RCZ000",
"mpfahealthStatus": false,
"name": "Shanghai-SR650V3",
"nist": {
    "currentValue": "Unknown",
    "possibleValues": ["Nist_800_131A_Strict","unsupported","Compatibility"]
},
"onboardPciDevices": [{
    "class": "Mass storage controller",
    "firmware": [],
    "fodUniqueID": "",
    "isAddOnCard": false,
    "isAgentless": false,
    "isPLDMUpdateSupported": false,
    "name": "PCH Integrated SATA Controller 2",
    "pciBusNumber": "0",
    "pciDeviceNumber": "25",
    "pciFunctionNumber": "0",
    "pciRevision": "11",
    "pciSegmentNumber": "0",
    "pciSubID": "7824",
    "pciSubVendorID": "17aa",
    "portInfo": {},
    "posID": "1bd2",
    "vpdID": "8086"
},
...,
{
    "class": "Unclassified device",
    "firmware": [{
        "name": "Gen5 Riser 2B Retimer",
```

```
            "date": "",
            "type": "Software Bundle",
            "build": "0",
            "version": "1.27.35",
            "role": "",
            "status": "Active",
            "classifications": [13],
            "revision": "0",
            "softwareID": "1D494054"
        }],
        "fodUniqueID": "",
        "isAddOnCard": false,
        "isAgentless": false,
        "isPLDMUpdateSupported": false,
        "name": "Retimer Riser 2",
        "pciBusNumber": "0",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "0",
        "pciRevision": "0",
        "pciSubID": "0",
        "pciSubVendorID": "0",
        "portInfo": {},
        "posID": "0",
        "vpdID": "0"
    }],
    "osInfo": {
        "description": "",
        "hostname": "",
        "storedCredential": ""
    },
    "overallHealthState": "Normal",
    "parent": {
        "uri": "cabinet/",
        "uuid": ""
    },
    "partitionID": -1,
    "partNumber": "STA7B05327",

    "pciCapabilities": ["RaidLink","OOB_PCIe","RaidLinkConfig","RaidLinkAlert","OOB_PCIe_Config",
                        "OOB_Option_Firmware_Update","PreStandardPLDM","StandardPLDM","Storlib","M2"],
    "pciDevices": [{
        "class": "Network controller",
        "firmware": [{
            "build": "0",
            "classifications": [13],
            "date": "",
            "name": "Firmware Bundle",
            "revision": "0",
            "role": "",
            "softwareID": "17AA4104",
            "status": "Active",
            "type": "Software Bundle",
            "version": "222.0.2.1"
        }],
        "fodUniqueID": "",
        "FRU": "01PE761",
        "fruSerialNumber": "L0NV1A2004Y",
        "isAddOnCard": true,
        "isAgentless": false,
        "isPLDMUpdateSupported": false,
        "manufacturer": "Broadcom Limited",
```

```
    "name": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
    "partNumber": "SN37A28309",
    "pciBusNumber": "22",
    "pciDeviceNumber": "0",
    "pciFunctionNumber": "1",
    "pciRevision": "1",
    "pciSegmentNumber": "0",
    "pciSubID": "4104",
    "pciSubVendorID": "17aa",
    "portInfo": {
        "physicalPorts": [{
            "logicalPorts": [{
                "addresses": "e4:3d:1a:61:88:8d",
                "logicalPortIndex": 1,
                "portNumber": 1,
                "portType": "ETHERNET",
                "vnicMode": false
            }],
            "peerBay": 0,
            "physicalPortIndex": 2,
            "portNumber": 2,
            "portType": "ETHERNET",
            "speed": -1.0,
            "status": "Down"
        }]
    },
    "posID": "1657",
    "productName": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
    "slotName": "PCIe 13",
    "slotNumber": "13",
    "slotSupportsHotPlug": "false",
    "vpdID": "14e4"
}],    "physicalID": 0,
"ports": [{
    "ioModuleBay": 0,
    "portNumber": 3
},
...,
{
    "ioModuleBay": 0,
    "portNumber": 2
}],
"posID": "",
"powerAllocation": {
    "maximumAllocatedPower": 1100,
    "minimumAllocatedPower": 0
},
"powerCappingPolicy": {
    "cappingACorDCMode": "AC",
    "minimumHardCapLevel": 726000,
    "cappingPolicy": "OFF",
    "maxPowerCap": 1100000,
    "minimumPowerCappingHotPlugLevel": -1,
    "powerCappingAllocUnit": "watts*10^-3",
    "maximumPowerCappingHotPlugLevel": -1,
    "currentPowerCap": 0,
    "minPowerCap": 0
},
"powerStatus": 8,
"powerSupplies": [{
    "cmmDisplayName": "Power Supply 1",
```

```
    "cmmHealthState": "Unknown",
    "dataHandle": 0,
    "description": "Power Supply 1",
    "excludedHealthState": "Normal",
    "firmware": [{
        "build": null,
        "classifications": [10],
        "date": "",
        "name": "PSU1",
        "role": "OK",
        "softwareID": "PSUACBE8100",
        "status": "OK",
        "type": "Firmware",
        "version": "14.13"
    }],
    "FRU": "",
    "fruSerialNumber": "",
    "hardwareRevision": "",
    "healthState": "GOOD",
    "inputVoltageIsAC": true,
    "inputVoltageMax": -1,
    "inputVoltageMin": -1,
    "leds": [],
    "machineType": "",
    "manufactureDate": "",
    "manufacturer": "ACBE",
    "manufacturerId": "",
    "model": "",
    "name": "Power Supply 1",
    "overallHealthState": "Normal",
    "parent": {
        "uri": "chassis/",
        "uuid": ""
    },
    "partNumber": "SP57A88785",
    "posID": "",
    "powerAllocation": {
        "totalInputPower": 0,
        "totalOutputPower": 1100
    },
    "powerState": "Unknown",
    "productId": "",
    "productName": "",
    "serialNumber": "A1DB24110DX",
    "slots": [1],
    "type": "PowerSupply",
    "uri": "powerSupply/",
    "userDescription": "",
    "uuid": "",
    "vpdID": ""
}],    "primary": false,
"processorIntelSpeedSelect": {
    "currentValue": "Auto",
    "possibleValues": ["Auto","SST-PP V2","Config1","Config2","Base"]
},
"processors": [{
    "cores": 44,
    "displayName": "Intel(R) Xeon(R) Platinum 8458P",
    "family": "INTEL_R_XEON_TM",
    "healthState": "GOOD",
    "manufacturer": "Intel(R) Corporation",
```

```
    "maxSpeedMHZ": 3800,
    "partNumber": "",
    "present": false,
    "productVersion": "Intel(R) Xeon(R) Platinum 8458P",
    "serialNumber": "0x5583BC1F3716456E",
    "slot": 1,
    "socket": "CPU 1",
    "speed": 2.7,
    "tdpWatts": 350
}],
"processorSlots": 0,
"productId": "664A00",
"productName": "ThinkSystem SR650 V3 MB,EGS,DDR5,SH,2U",
"raidSettings": [{
    "batteryData": [],
    "description": "ThinkSystem RAID 940-16i 8GB Flash PCIe Gen4 12Gb Adapter",
    "diskDrives": [{
        "bay": 1,
        "blockSize": 512,
        "capacity": 300000000000,
        "description": "300GB 10K 6Gbps SAS HDD",
        "diskState": "Online",
        "encryptionStatus": "Unencrypted",
        "firmware": [{
            "build": "0",
            "classifications": [10],
            "date": "",
            "name": "ST9300603SS",
            "revision": "0",
            "role": "",
            "softwareID": "41Y8473",
            "status": "Active",
            "type": "Firmware",
            "version": "B53B"
        }],
        "FRU": "42D0628",
        "healthState": "OK",
        "hotSpareType": "None",
        "interfaceType": "SAS",
        "largestAvailableSize": 512,
        "m2Location": "",
        "manufacturer": "IBM-ESXS",
        "mediaType": "HDD",
        "model": "ST9300603SS",
        "name": "Disk.1",
        "numberOfBlocks": 585937500,
        "partNumber": "42D0631",
        "remainingLife": -1,
        "serialNumber": "6SE2SSGD",
        "temperature": 33,
        "uuid": ""
    }],
    "firmware": [{
        "classifications": [],
        "build": "0",
        "date": "",
        "name": "",
        "revision": "0",
        "role": "",
        "softwareID": "",
        "status": "",
```

```
    "type": "",
    "version": "52.22.0-4633"
}],
"isAddOnCard": true,
"model": "SAS3916",
"name": "ThinkSystem RAID 940-16i 8GB Flash PCIe Gen4 12Gb Adapter",
"pciFirmware": []
"slotNumber": "1",
"storagePools": [{
    "arrayStatus": "",
    "arrayUid": "0",
    "combinedRaidLevel": "0",
    "description": "The resource is used to represent a storage pool for a Redfish implementation.",
    "diskDrives": [{
        "bay": 1,
        "blockSize": 512,
        "capacity": 300000000000,
        "description": "300GB 10K 6Gbps SAS HDD",
        "diskState": "Online",
        "encryptionStatus": "Unencrypted",
        "firmware": [{
            "build": "0",
            "classifications": [10],
            "date": "",
            "name": "ST9300603SS",
            "revision": "0",
            "role": "",
            "status": "Active",
            "softwareID": "41Y8473",
            "type": "Firmware",
            "version": "B53B"
        }],
        "FRU": "42D0628",
        "healthState": "OK",
        "hotSpareType": "None",
        "interfaceType": "SAS",
        "largestAvailableSize": 512,
        "m2Location": "",
        "manufacturer": "IBM-ESXS",
        "mediaType": "HDD",
        "model": "ST9300603SS",
        "name": "Disk.1",
        "numberOfBlocks": 585937500,
        "partNumber": "42D0631",
        "remainingLife": -1,
        "serialNumber": "6SE2SSGD",
        "temperature": 33,
        "uuid": "",
    }],
    "name": "Pool_6_7",
    "raidLevel": 0,
    "remainingSpace": 0,
    "storageVolumes": [{
        "accessPermission": "READ_WRITE",
        "accessPolicy": "ReadWrite",
        "blockSize": 512,
        "bootable": true,
        "description": "This resource is used to represent a volume for a Redfish implementation.",
        "driveCachePolicy": "Unchanged",
        "driveIndex": 0,
        "health": "OK",
```

```
                "ioPolicy": "DirectIO",
                "isSDRAID": null,
                "LUN": -1,
                "name": "",
                "numberOfBlocks": 1167966208,
                "primaryPartition": 0,
                "raidType": "RAID 0",
                "readPolicy": "",
                "removable": false,
                "stripeSize": 262144,
                "targetType": null,
                "volumeID": "239",
                "volumeOwner": null,
                "volumeStatus": "",
                "volumeType": "RAID",
                "volumeUID": "0",
                "writePolicy": "WriteThrough"
            }],
            "totalManagedSpace": 597998698496
        }],
        "storageVolumes": [{
            "accessPermission": "READ_WRITE",
            "accessPolicy": "ReadWrite",
            "blockSize": 512,
            "bootable": true,
            "description": "This resource is used to represent a volume for a Redfish implementation.",
            "driveIndex": 0,
            "driveCachePolicy": "Unchanged",
            "health": "OK",
            "ioPolicy": "DirectIO",
            "isSDRAID": null,
            "LUN": -1,
            "name": "",
            "numberOfBlocks": 1167966208,
            "primaryPartition": 0,
            "raidType": "RAID 0",
            "readPolicy": "",
            "removable": false,
            "stripeSize": 262144,
            "targetType": null,
            "volumeID": "239",
            "volumeOwner": null,
            "volumeStatus": "",
            "volumeType": "RAID",
            "volumeUID": "0",
            "writePolicy": "WriteThrough"
        }],
        "uuid": "4BEF9CA0-830B-49F4-8589-1705132EF6F6"
    }],
    "releaseName": "egs_gp_ga",
    "secureBootMode": {
        "currentValue": "Disabled",
        "possibleValues": ["Enabled","Disabled"]
    },
    "securityDescriptor": {
        "identityManagementSystemEnabled": false,
        "managedAuthEnabled": true,
        "managedAuthSupported": true,
        "publicAccess": false,
        "roleGroups": ["lxc-supervisor"],
        "storedCredentials": {
```

```
            "description": "Passw0rd@01",
            "id": "1652",
            "userName": "USERID"
        },
        "uri": "nodes/40bdb5f8d609b801c183337c180d3f29"
    },
    "securityMode": "Compatibility  Security",
    "selLog": true,
    "serialNumber": "SR650R112",
    "slots": [],
    "ssoEnabled": true,
    "ssdWearThreshold": 8,
    "status": {
        "message": "managed",
        "name": "MANAGED"
    },
    "subSlots": [],
    "subType": "",
    "systemGuardSetting": {
        "lockDownPolicy": "PreventOSBooting",
        "osBootPreventing": false,
        "status": "Compliant",
        "systemGuardEnabled": false
    },
    "userDefinedName": "Shanghai-SR650V3",
    "tlsVersion": {
        "currentValue": "TLS_12",
        "possibleValues": ["unsupported","TLS_12","TLS_11","TLS_10"]
    },
    "type": "Rack-Tower  Server",
    "uri": "nodes/40BDB5F8D609B801C183337C180D3F29",
    "userDescription": "",
    "uuid": "40BDB5F8D609B801C183337C180D3F29",
    "vnicMode": "disabled",
    "vpdID": ""
}
```


PUT /nodes/*{uuid}*

Use this method to modify node properties or perform management actions on a specific the server or Flex System storage node.

The request body differs depending on the action that you want to perform. You can use this PUT method to perform the following management actions.

- Table 19 “Modify node properties” on page 316
- Table 20 “Modifying the power state” on page 319
- Table 21 “Configure device authentication” on page 319
- Table 22 “Refresh the inventory” on page 321
- Table 23 “Configure the boot order” on page 321
- Table 24 “Configure the TLS protocol and NIST compliance” on page 322
- Table 25 “Configure the encapsulation mode” on page 322
- Table 26 “Configure LED states” on page 323
- Table 27 “Clear the SEL log” on page 323
- Table 28 “Modify the asset tag” on page 324
- Table 29 “Enable or disable System Guard” on page 324

This method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform

this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/{uuid}`

where *{uuid}* is the UUID of the node to be retrieved. To obtain the node UUID, use the GET /nodes method.

Query parameters

Parameters	Required / Optional	Description
synchronous=*{Boolean}*	Optional	When modifying attributes, indicates when the job ID is returned • **true**. (default) Returns the job ID and job status after the job is complete. • **false**. Returns the job ID immediately. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If the **powerState=bootToF1** request attribute is specified, indicates when the job ID is returned. • **true**. (default) Returns the job ID and job status after the job is complete. • **false**. Returns the job ID immediately. **Note:** This query parameter applies only when a node-properties attribute or **powerState=bootToF1** attribute is specified in the request body.

The following example sets synchronous to true.

```
PUT https://192.0.2.0/nodes/6ED2CB368C594C66C2BB066D5A306138?synchronous=true
```

Request body

You can specify attributes from one of the following tables in each request.

Note: If you specify one or more request attributes in Table 19 “Modify node properties” on page 316 (to modify properties), Table 20 “Modifying the power state” on page 319 (to modify the power state), or Table 22 “Refresh the inventory” on page 321 (to refresh the inventory), this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, /tasks/12) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Table 19. Modify node properties

Attributes	Required / Optional	Type	Description
cmmDisplayName	Optional	String	Chassis name
contact	Optional	String	The chassis contact information

Table 19. Modify node properties (continued)

Attributes	Re-quired / Optional	Type	Description
hostname	Optional	String	Hostname
ipInterfaces	Optional	Array	Information about the CMM IP addresses
name	Required	String	IP Interface name
IPv4enabled	Optional	Boolean	Identifies whether IPv4 is enabled. This can be one of the following values. • **true**. IPv4 is enabled • **false**. IPv4 is disabled
IPv6enabled	Optional	Boolean	Identifies whether IPv6 is enabled. This can be one of the following values. • **true**. IPv6 is enabled • **false**. IPv6 is disabled
IPv4DHCPmode	Optional	String	IPv4 address assignment method. This can be one of the following values. • **STATIC_ONLY** • **DHCP_ONLY** • **DHCP_THEN_STATIC** • **UNKNOWN**
IPv6DHCPenabled	Optional	Boolean	Identifies whether IPv6 DHCP is enabled. This can be one of the following values. • **true**. IPv6 DHCP is enabled • **false**. IPv6 DHCP is disabled
IPv6statelessEnabled	Optional	Boolean	Identifies whether IPv6 stateless is enabled. This can be one of the following values. • **true**. IPv6 stateless is enabled • **false**. IPv6 stateless is disabled
IPv6staticEnabled	Optional	Boolean	Identifies whether IPv6 static is enabled. This can be one of the following values. • **true**. IPv6 static is enabled • **false**. IPv6 static is disabled
IPv4assignments	Optional	Array	Information about IPv4 assignments
id	Required	Integer	IPv4 assignment ID
subnet	Optional	String	IPv4 subnet mask
gateway	Optional	String	IPv4 gateway
address	Optional	String	IPv4 address
IPv6assignments	Optional	Array	Information about IPv6 assignments
id	Required	Integer	IPv6 assignment ID
prefix	Optional	Integer	IPv6 prefix
gateway	Optional	String	IPv6 gateway
address	Optional	String	IPv6 address
location	Optional	String	(Flex System compute nodes only) Location in the chassis **Important:** Changes made to the location of the server or storage device using this API method are not reflected in the rack view.

Table 19. Modify node properties (continued)

Attributes	Required / Optional	Type	Description
location	Optional	Object	(Rack and tower servers only) Information about the location in the rack **Important:** Changes made to the location of the server using this API method are not reflected in the rack view.
location	Optional	String	Location of the server
rack	Optional	String	Rack
room	Optional	String	Room
lowestRackUnit	Optional	Integer	LRU
name	Optional	String	Server name
userDescription	Optional	String	The server description

The following example modifies the hostname, location, and contact information for the target server.

```
{
   "contact": "new contact",
   "hostname":"",
   "location": {
      "location":"new location"
   }
}
```

Table 20. Modifying the power state

Attributes	Required / Optional	Type	Description
powerState	Optional	String	Performs a power operation on the device. This can be one of the following values: • **powerOn**. Powers on the server. • **powerOff**. Powers off the server immediately. • **powerCycleHard**. . • **powerCycleSoft**. Restarts the server immediately. • **powerCycleSoftGrace**. Restarts the server gracefully (shuts down the operating system where applicable). • **virtualReseat**. Calls the CMM function to simulate removing power from the bay. • **powerNMI**. Restarts the server with non-maskable interrupt (performs a diagnostic interrupt). • **bootToF1**. (Lenovo devices only) Restarts the server to BIOS/UEFI (F1) Setup. This is supported for non-ThinkServer servers that are supported without limitations • **PXEHard**. (Lenovo Flex System, System x, and ThinkSystem servers only) Restarts the server immediately, and boots the server to the Preboot Execution Environment (PXE) network. **Note:** PXE-boot related UEFI settings must be configured on the server. For edge devices, only **powerCycleSoft** and **powerCycleSoftGrace** are supported. If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

The following example restarts the target server:

```
{
   "powerState": "powerCycleSoft"
}
```

Table 21. Configure device authentication and access control

Note: Only users with **lxc-supervisor** or **lxc-security-admin** authority can modify the access-control settings.

Table 21. Configure device authentication and access control (continued)

Attributes	Required / Optional	Type	Description
securityDescriptor	Required	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Optional	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication
publicAccess	Optional	Boolean	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
roleGroups	Optional	Array of strings	List of role groups that are permitted to view and manage this device
storedCredentials	Required if **managedAuthEnabled** is set to `true`	Object	Information about the stored credential that is associated with this device, if applicable.
id	Required if **managedAuthEnabled** is set to `true`	String	ID of the stored credential to associated with the device

The following example enables managed authentication and associates a stored credential account with the device.

```
{
   "securityDescriptor" : {
      "managedAuthEnabled" : true,
      "storedCredential": {
         "id":"249721...",
      }
   }
}
```

The following example disables managed authentication to use local authentication instead.

```
{
   "securityDescriptor": {
      "managedAuthEnabled" : false,
   }
}
```

The following example restricts access to the managed device to members of the specified role groups:

```
{
   "securityDescriptor": {
```

```
      "publicAccess": false,
      "roleGroups": ["sales-os-admin","corp_fw_admin"]
   }
}
```

Table 22. Refresh the inventory

Attributes	Required / Optional	Type	Description
refreshInventory	Optional	String	Refreshes inventory for the device. If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

The following example refreshes inventory for the target server.

```
{
   "refreshInventory": "true"
}
```

Table 23. Configure the boot order

Attributes	Required / Optional	Type	Description
bootOrder	Optional	Array	Boot order settings
bootOrderList	Required	Array	
currentBootOrderDevices	Required	Array of strings	List of potential boot devices **Tip:** To obtain the boot-order device values, use in GET /nodes method.
bootType	Optional	String	Boot type of the boot order setting. This can be one of the following values. • **BootOrder** • **CDDVDROMBootOrder** • **HardDiskBootOrder** • **NetworkBootOrder** • **Permanent** • **SingleUse** • **USBBootOrder** • **WakeOnLan**

The following example changes the boot order.

```
{
   "bootOrder": {
      "bootOrderList": [{
         "currentBootOrderDevices": [
            "HardDrive 0",
```

```
            "CDROM 0",
            "Hard Drive 1"
         ],
         "bootType": "BootOrder"
      }]
   }
}
```

Table 24. Configure the TLS protocol and NIST compliance

Attributes	Required / Optional	Type	Description
nist	Optional	Object	Information about NIST
currentValue	Required	String	Cryptography mode that is set. This can be one of the following values. • **Unknown** • **Compatibility** • **Nist_800_131A_Strict** • **Nist_800_131A_Custom**
tlsVersion	Optional	Object	Information about the SSL or TLS protocol
currentValue	Required	String	SSL or TLS protocol and version that is set. This can be one of the following values. • **unsupported** • **TLS_12**. TLS v1.2 • **TLS_13**. TLS v1.3

The following example changes the cryptography settings:

```
{
    "nist": {
      "currentValue": "Compatibility"
    }
}
```

Table 25. Configure the encapsulation mode

Attributes	Required / Optional	Type	Description
encapsulationMode	Optional	String	Encapsulation mode. This can be one of the following values. • **normal**. Encapsulation is disabled for this node.The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process. • **encapsulationLite**. Encapsulation is enabled for this node.When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.

The following example updates the encapsulation mode:

```
{
   "encapsulationMode": "encapsulationLite
}
```

Table 26. Configure LED states

Attributes	Required / Optional	Type	Description
leds	Optional	Object	State of the location LED.
name	Required	String	Description of the LED (for example, “Fault” or “Power”. To obtain the names of LEDs for a specific server, use the GET /nodes/*{uuid_list}* method.
state	Required	String	State of LED. This can be one of the following values. • **off** • **on** • **blinking** To obtain the current state of the LED, use the GET /nodes/*{uuid_list}* method. **Note:** Location LED on ThinkServer servers can be on or off. Blinking is not supported.

The following example turns on the Information LED.

```
{
   "leds":[{
      "name":"Information",
      "state":"on"
   }]
}
```

Table 27. Clear the SEL log

Attributes	Required / Optional	Type	Description
selLog	Optional	String	Clears the SEL log for the device. This value is always **cleared**. If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Table 28. Modify the asset tag

Attributes	Required / Optional	Type	Description
assetTag	Required	String	(ThinkSystem rack servers only) Name or Tag that represents the server or other physical enclosure

The following example modifies the asset tag.

```
{
   "assetTag": "Server_1"
}
```

Table 29. Enable or disable System Guard

Attributes	Required / Optional	Type	Description
systemGuardEnabled	Required	Boolean	(ThinkSystem rack servers only) Indicates whether to enable System Guard. This can be one of the following values. • **true**. System Guard is enabled. A snapshot of hardware inventory is collected automatically for comparison purposes. • **false**. System Guard is disabled.

The following example modifies the asset tag.

```
{
   "systemGuardEnabled": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response body provides information about the success or failure of the request. The attributes in the response body differ depending on the specified request attributes.

Note: A response body is not returned for some requests.

The following example is returned when the **"refreshInventory": "true"** is specified in the request body to refresh the device inventory.

```
{
   "statusCode": 200,
   "statusDescription": "The request completed successfully.",
   "messages": [{
      "explanation": "refreshInventory request for target 6ED2CB368C594C66C2BB066D5A306138 has
                      completed successfully.",
      "id": "FQXDM0200",
      "recovery": "",
      "recoveryUrl": "",
      "text": "The request completed successfully."
   }]
}
```

/nodes/*{uuid}*/bmc

Use this REST API to restart the baseboard management controller for a specific managed server.

HTTP methods

PUT

PUT /nodes/*{uuid}*/bmc

Use this method to restart the baseboard management controller for a specific managed server.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/{uuid}/bmc`

where *{uuid}* is the UUID of the node to be retrieved. To obtain the node UUID, use the GET /nodes method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
powerState	Optional	String	Performs a power operation on the device. This can be one of the following values. • **restart**. Restarts the server immediately. If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

The following example restarts the target server:

```
{
   "powerState": "restart"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

No response is returned if the request is successful with a response code of 200. If the request is not successful, the following attributes are returned.

Attributes	Type	Description
statusCode	Integer	Response code
statusDescription	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	String	User actions that can be taken to recover from the event
recoveryUrl	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request fails.

```
{
   "statusCode": 409,
   "statusDescription": "The current state of the requested resources conflicts with this
                         request.",
   "messages": [{
      "explanation": "The RESTART action on endpoint AndroMeda failed.",
      "id": "FQXDM0409N",
      "recovery": "Verify the state of the requested resource and send this request again.",
      "recoveryUrl": "",
      "text": "The current state of the requested resources conflicts with this request.",
   }]
}
```

/nodes/*{uuid}*/bundleRepoAvailableSpaceInKB

Use this REST API to return the amount of space that is available in repository on the baseboard management controller for an ThinkSystem server with XCC2.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

GET

GET /nodes/*{uuid}*/bundleRepoAvailableSpaceInKB

Use this method to return the amount of space that is available in repository on the baseboard management controller for an ThinkSystem server with XCC2.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{uuid}/bundleRepoAvailableSpaceInKB`

where *{uuid}* is the UUID of the node to be retrieved. To obtain the node UUID, use the GET /nodes method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
BundleRepoAvailableSpaceInKB	Long	Amount of space, in KB, that is available in repository on the baseboard management controller

The following example is returned if the request is successful.

```
{
   "BundleRepoAvailableSpaceInKB": 300000
}
```

/nodes/*{uuid}*/isRAIDReady

Use this REST API to return the hardware RAID status for a specific server.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

HTTP methods

GET

GET /nodes/*{uuid}*/isRAIDReady

Use this method to return the hardware RAID status for a specific server.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{uuid}/isRAIDReady`

where *{uuid}* is the UUID of the server. To obtain the server UUIDs, use GET /nodes.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
isRAIDReady	Boolean	Indicates whether Hardware RAID is in the Ready state. This can be one of the following values. • **true**. Hardware RAID is in the Ready state. • **false**. Hardware RAID is in the Pending or Initializing state.

The following example is returned if the request is successful.

```
{
   "isRAIDReady": true
}
```

/nodes/*{uuid}*/maintenanceHistory

Use this REST API to return information about the maintenance history for a specific ThinkSystem or ThinkAgile device.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

HTTP methods

GET

GET /nodes/*{uuid}*/maintenanceHistory

Use this method to return information about the maintenance history for a specific ThinkSystem or ThinkAgile device.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{uuid}/maintenanceHistory`

where *{uuid}* is the UUID of the node to be retrieved. To obtain the node UUID, use the GET /nodes method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
results	Array of objects	Information about each maintenance activity If maintenance history is not available for the specified device, an empty array is returned
id	String	Maintenance activity ID
createdTimestamp	String	Timestamp when the maintenance activity occurred This timestamp is specified using ISO-8601 format (for example, 2019-05-02T19:28:14.000Z). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
messages	String	Message text that describes the maintenance activity
type	String	Maintenance type. This can be one of the following values. • **Hardware** • **Firmware**

The following example is returned if the request is successful.


```
{
   "results": [{
      "id": "1",
      "createdTimestamp": "2020-07-01T04:46:59Z",
      "message": "Primary XCC firmware is activated to TEI3A2C .",
      "type": "Firmware"
   },
   {
      "id": "2",
      "createdTimestamp": "2020-07-01T04:47:09Z",
      "message": "DIMM(SN: 125CE8A1) in slot 3 is added.",
      "type": "Hardware"
   },
   ...,
   {
      "id": "28",
      "createdTimestamp": "2020-10-15T15:25:12Z",
      "message": "Backup XCC firmware is updated to TEI3A8L by XCC Web.",
      "type": "Firmware"
   },
   {
```

```
      "id": "29",
      "createdTimestamp": "2020-10-21T09:50:14Z",
      "message": "Primary XCC firmware is activated to TEI3A8L.",
      "type": "Firmware"
   }]
}
```

/nodes/*{uuid}*/mediaMount

Use this REST API to retrieve information about all discovered media, mount media, unmount media that was previously mounted, or enable or disable support for mounting media.

HTTP methods

GET, PUT

GET /nodes/*{uuid}*/mediaMount

Use this method to return information about all discovered media.

Information about all discovered media is not included in node inventory using GET /nodes/*{uuid_list}*.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{uuid}/mediaMount`

where *{uuid}* is the UUID of a ThinkServer server. To obtain the node UUID, use the GET /nodes method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Table 30. ThinkServer servers

Attributes	Type	Description
mediaLocation	String	Location of the media that is mounted to the ThinkServer server, if the media is mounted
mediaServerAddress	String	IP address of the server on which media is located
mediaState	String	Indicates whether the media is mounted. This can be one of the following values. • **mount** • **unmount**
mediaType	String	Media type. This can be one of the following values. • **CD/DVD**. CD drive • **FD**. Flash drive • **HD**. Disk drive
mountMediaEnabled	String	Indicates whether the mounted media is enabled. This can be one of the following values. • **true**. The mounted media is enabled. • **false**. The mounted media is disabled.

The following example is returned for a ThinkServer server if the request is successful.

```
{
   "mediaLocation": "/path/to/someiso.iso",
   "mediaServerAddress": "10.243.5.21",
   "mediaState": "mount",
   "mediaType": "HD"
   "mountMediaEnabled": "true",
}
```

Table 31. All servers other than ThinkServer

Attributes		Type	Description
memberCount		Integer	(Servers other than ThinkServer only) Number of media members
members		Array of objects	(Servers other than ThinkServer only) Information about each media member
	domainName	String	(Samba only) Domain of the user name to access the file path
	filePath	String	File path of the map image
	options	String	(Samba and NFS only) The mount options to map the image of the file path
	shareType	String	Map type of the image. This can be one of the following values. • **ftp** • **http** • **https** • **nfs** • **samba** • **sftp**
	UID	String	Unique ID of the media member
	username	String	(Samba, NFS, HTTP, HTTPS, FTP, and SFTP only) User name that is used to access the file path

The following example is returned for a System x server if the request is successful.

```
{
   "memberCount": 2,
   "members": [{
      "domainName": "10.243.8.196",
      "filePath": "https://10.243.8.196/path/to/some.iso",
      "options": "ro",
      "shareType": "NFS",
      "UID": "28F0114D78",
      "username": "JOE"
   },
   {
      "domainName": "10.243.5.166",
      "filePath": "sftp://10.243.5.166/path/to/some.iso",
      "options": "ro",
      "shareType": "SFTP",
      "UID": "BB7CDCB184",
      "username": "JOE"
   }]
}
```


PUT /nodes/*{uuid}*/mediaMount

Use this method to mount media, unmount media that was previously mounted, or enable or disable support for mounting media on a specific ThinkServer or ThinkSystem server.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/{uuid}/mediaMount`

where *{uuid}* is the UUID of a ThinkServer server. To obtain the node UUID, use the GET /nodes method.

Query parameters

None

Request body

Table 32. Enable or disable support for mounting media

Attributes	Required / Optional	Type	Description
action	Required	String	(ThinkServer servers only) Enable or disabled servers to support mounting media. Specify one of the following values. • **enableMountMedia**. Enable a mounted image. • **disableMountMedia**. Disable a mounted image. • **reset**. (ThinkSystem only) Cleans the management console and removes mounted media.

This example enables support for mounting media on a ThinkServer server.


```
{
   "action": "enableMountMedia"
}
```

Table 33. Mount media

Attributes	Required / Optional	Type	Description
action	Required	String	Mounts an image that was previously mounted when **mount** is specified If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.
domainName	Required if **shareType** is Samba	String	Domain name of the server on which media is located If a value is not specified, the domain name is used.
mediaLocation	Required	String	Full path of the media ISO
mediaServerAddress	Required	String	IP address of the server on which media is located
mediaType	Required	String	(ThinkServer servers only) The media type. This can be one of the following values. • **CD/DVD**. CD drive • **FD**. Flash drive • **HD**. Disk drive
password	Required if **shareType** is Samba	String	Password to authenticate to the media
port	Optional	Integer	Port number to use if **mediaLocation** is on an external web server and **shareType** is **http** or **https**
shareType	Required	String	Share type. This can be one of the following values. • **ftp** • **http** • **https** • **nfs** • **samba** • **sftp**
username	Required if **shareType** is Samba	String	User name to authenticate to the media

This example mounts a hard disk drive on a Samba server.

```
{
   "action": "mount",
```

```
   "domainName":"192.0.2.146",
   "mediaLocation":"/path/to/someiso.iso",
   "mediaServerAddress": "192.0.2.146",
   "mediaType" : "HD",
   "password":"password",
   "shareType":"samba",
   "username":"JOE"
}
```

This example mounts an NFS server to a System x server

```
{
   "action": "mount",
   "domainName":"192.0.2.146",
   "mediaLocation":"/path/to/some.iso",
   "mediaServerAddress": "192.0.2.146",
   "password":"password",
   "shareType":"nfs",
   "username":"JOE"
}
```

This example mounts an HTTPS server to a server

```
{
   "action":"mount",
   "domainName":"",
   "mediaLocation":"/linux/SuSE/SLES15/SLE-15-SP2-Full-x86_64-GM-Media1.iso",
   "mediaServerAddress":"192.0.2.146",
   "mediaType":"CD",
   "password":"",
   "port":443,
   "shareType":"https",
   "username":""
}
```

Table 34. Unmount media

Attributes	Required / Optional	Type	Description
action	Required	String	Unmounts an image when **unmount** is specified If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.
mediaType	Required	String	(ThinkServer servers only) Media type. This can be one of the following values. • **CD/DVD**. CD drive • **FD**. Flash drive • **HD**. Disk drive
UID	Required	String	(Servers other than ThinkServer only) Unique ID of the mounted media to be unmounted. If not specified, all mounted media of the specified type is unmounted. To obtain the mount media ID, use the GET /tasks/*{job_list}* method.

The example unmounts a CD drive on a ThinkServer server.

```
{
   "action": "unmount",
   "mediaType" : "CD"
}
```

The example unmounts media with UID `597BDF427O` on a System x server.

```
{
   "action": "unmount",
   "UID" : "597BDF427O"
}
```

The example unmounts all media from a server.

```
{
   "action": "unmount",
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
statusCode		Integer	The return code
statusDescription		String	Description of the return code.
messages		Array of objects	Information about one or more messages.
	explanation	String	Additional information to clarify the reason for the message.
	id	String	The message identifier of a returned message.
	recovery	String	Recovery information
	recoveryURL	String	
	text	String	Message text associated with the message identifier.

The following example is returned if the request is successful.

```
{
   "statusCode": 403,
   "statusDescription": "The request is forbidden by server.",
   "messages": [{
      "explanation": "The mount media request to the device has been rejected..",
      "id": "FQXDM0403N",
      "recovery": "Verify the request and make sure it is allowed by server."
      "recoveryUrl": "",
      "text": "The request is forbidden by server.",
   }]
}
```

/nodes/*{uuid}*/mediaMount/*{UID}*

Use this REST API to retrieve information about members of media that was previously mounted and unmount specific media from a specific server.

HTTP methods

GET, PUT

GET /nodes/*{uuid}*/mediaMount/*{uid}*

Use this method to return information about members of specific media that was previously mounted to a specific server.

Note: This API is not supported for ThinkServer servers.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{uuid}/mediaMount/{uid}`

where

- *{uuid}* is the UUID of a server. To obtain the server UUID, use the GET /nodes method.
- *{uid}* is the UID of the mounted media. To obtain the mounted-media UID, use the GET /nodes/*{uuid}*/mediaMount method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
memberCount	Integer	Number of media members
members	Array of objects	Information about the media member
domainName	String	(Samba only) Domain of the user name to access the file path
filePath	String	File path of the map image
options	String	(Samba and NFS only) The mount options to map the image of the file path
readonly	String	Indicates whether the map image is read only. This can be one of the following values. • **true**. The map image has read-only permissions. • **false**. The map image has read/write permissions.

Attributes		Type	Description
	shareType	String	Map type of the image. This can be one of the following values. • **ftp** • **http** • **https** • **nfs** • **samba** • **sftp**
	username	String	User name that is used to access the file path

The following example is returned if the request is successful.

```
{
   "memberCount": 2,
   "members": [{
      "domainName": "10.244.9.146",
      "filePath": "https://10.244.9.146/tftpboot/nightbuild/current.iso",
      "options": "ro""shareType": "NFS",
      "UID": "42DDD3DA43",
      "username": "test",

   },
   {
      "domainName": "10.243.7.146",
      "filePath": "https://10.244.9.146/tftpboot/nightbuild/dummy.img",
      "options": "ro""shareType": "NFS",
      "UID": "60E7E61E82",
      "username": "test",

   }]
}
```

PUT /nodes/*{uuid}*/mediaMount/*{UID}*

Use this method to unmount specific media that was previously mounted to a specific server.

Note: This API is not supported for ThinkServer servers. To unmount media from a ThinkServer server, use the PUT /nodes/*{uuid}*/mediaMount method.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/{uuid}/mediaMount/{UID>`

where

- *{uuid}* is the UUID of a server. To obtain the server UUID, use the GET /nodes method.
- *{UID}* is the UID of the mounted media. To obtain the mounted-media UID, use the GET /nodes/*{uuid}*/mediaMount method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
action	Required	String	Unmounts an image when **unmount** is specified

This example unmounts the specified media from the specified server.

```
{
   "action": "unmount",
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
statusCode		Integer	Return code
statusDescription		String	Description of the return code
messages		Array of objects	Information about one or more messages
	explanation	String	Additional information to clarify the reason for the message
	id	String	Message identifier of a returned message
	recovery	String	Recovery information
	recoveryURL	String	Link to the help system for more information about how to recover, if available
	text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "statusCode": 403,
   "statusDescription": "The request is forbidden by server.",
   "messages": [{
      "explanation": "The mount media request to the endpoint has been rejected..",
      "id": "FQXDM0403N",
      "recovery": "Verify the request and make sure it is allowed by server."
      "recoveryUrl": "",
      "text": "The request is forbidden by server
```

```
    }]
}
```

/nodes/*{uuid}*/MPFAData

Use this REST API to collect or retrieve memory-failure-prediction analytics data for a specific ThinkSystem or ThinkAgile server.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

GET, POST

GET /nodes*{uuid}*/MPFAData

Use this method to return memory-failure-prediction analytics data for a specific ThinkSystem or ThinkAgile server.

Notes:

- This REST API is not supported for AMD-based ThinkSystem or ThinkAgile servers.
- This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{uuid}/MPFAData`

where *{uuid}* is the UUID of the server. To obtain the server UUIDs, use GET /nodes.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
MPFAData	String	Raw (binary) memory failure prediction analytics data

The following example is returned if the request is successful.

```
{
   "MPFAData": "{binary data}"
}
```

POST /nodes/{uuid}/MPFAData

Use this method to collect memory-failure-prediction analytics data for a specific ThinkSystem or ThinkAgile server.

Notes:

- This REST API is not supported for AMD-based ThinkSystem or ThinkAgile servers.
- This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

A job is created to complete this request.

A successful response code indicates that the job was successfully transmitted and accepted by the management server. It does not indicate that the operation that is associated with the job was successful. If a job was not successfully started, refer to the response code and response body for details.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/nodes/{uuid}/MPFAData
```

where *{uuid}* is the UUID of the server. To obtain the server UUIDs, use GET /nodes.

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
action	Required	String	This value is always **collectMPFAData**.

The following example collects memory failure prediction analytics data.

```
{
   "action": "collectMPFAData"
```

}

Response codes

Code	Description	Comments
202	Accepted	The request has been accepted for processing, but the processing has not yet completed. The request might or might not be acted upon, depending on the results of the processing.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

This method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

/nodes/*{uuid}*/MPFAHealthStatus

Use this REST API to return or modify the memory-failure-prediction analytics status for a specific ThinkSystem or ThinkAgile server.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

GET, PUT

GET /nodes/*{uuid}*/MPFAHealthStatus

Use this method to return the memory-failure-prediction analytics status for a specific ThinkSystem or ThinkAgile server.

Notes:

- This REST API is not supported for AMD-based ThinkSystem or ThinkAgile servers.
- This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{uuid}/MPFAHealthStatus`

where *{uuid}* is the UUID of the server. To obtain the server UUIDs, use GET /nodes.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.

Code	Description	Comments
405	Method Not Allowed	A specified resource is invalid. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
MPFAHealthStatusEnabled	Boolean	Indicates whether collecting memory failure prediction analytics data is enabled. This can be one of the following values. • **true**. Memory failure prediction analytics is enabled. • **false**. (default) Memory failure prediction analytics status is disabled

The following example is returned if the request is successful.

```
{
   "MPFAHealthStatusEnabled": true
}
```

PUT /nodes/*{uuid}*/MPFAHealthStatus

Use this method to enable or disable memory-failure-prediction analytics for a specific ThinkSystem or ThinkAgile server.

Notes:

- This REST API is not supported for AMD-based ThinkSystem or ThinkAgile servers.
- This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/{uuid}/MPFAHealthStatus`

where *{uuid}* is the UUID of the server. To obtain the server UUIDs, use GET /nodes.

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
MPFAHealthStatusEnabled	Required	Boolean	Indicates whether collecting memory failure prediction analytics data is enabled. This can be one of the following values. • **true**. Memory failure prediction analytics is enabled. • **false**. (default) Memory failure prediction analytics status is disabled

The following example enables collecting memory failure prediction analytics data.

```
{
   "MPFAHealthStatusEnabled": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/nodes/*{uuid}*/pfaConfigSettings

Use this REST API to retrieve information about and configure the predicted failure alerts (PFA) configuration settings.

HTTP methods

GET, PUT

GET /nodes/*{uuid}*/pfaConfigSettings

Use this method to return information about the predicted failure alerts (PFA) configuration settings from the baseboard management controller.

A 64-bit *category map* is used to identify hardware event categories and severities:
- **Bit 0**. RAS event VM movement support
- **Bit 1**. Processor subsystem
- **Bit 2**. Memory subsystem
- **Bit 3**. I/O subsystem
- **Bit 4**. Power
- **Bit 5**. Cooling
- **Bit 6**. Fans
- **Bit 7**. Storage
- **Bit 8**. CEC hardware (For System x servers, this bit is not supported and is set to 0.)
- **Bit 9**. Platform firmware
- **Bit 10**. Software
- **Bit 11**. External environment

- **Bit 12 – 25**. Reserved
- **Bit 26**. Redundancy degrade
- **Bit 27**. PFA
- **Bit 28**. Redundancy loss
- **Bit 29**. Info
- **Bit 30**. Warning
- **Bit 31**. Error

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/{uuid}/pfaConfigSettings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
categoryBitMap	Array of Objects	Bits definition
vmMoveCategoryBit	Integer	Bit number of the category
vmMoveCategoryName	String	Name of the category
vmMoveCategoryType	String	Type of the category
desiredCategories	Integer	Hardware event categories that are monitored. This value can be a bitmask value as per the category map.
supportedCategories	Integer	Hardware event categories that are supported by the platform. This value can be a bitmask value as per the category map.

The following example is returned if the request is successful.

```
{
   "categoryBitMap": [{
      "vmoveCategoryBit": 0,
```

```
      "vmMoveCategoryName": "RASeventVMmovementsupport",
      "vmMoveCategoryType": "VMEFlag"
   },
   {
      "vmMoveCategoryBit": 1,
      "vmMoveCategoryName": "Processorsubsystem",
      "vmMoveCategoryType": "EventCategory"
   },
   ...,
   {
      "vmMoveCategoryBit": 31,
      "vmMoveCategoryName": "partialcapacityloss",
      "vmMoveCategoryType": "Severity"
   }],
   "desiredCategoriesv": 2147483684,
   "supportedCategories": 3087007935
}
```

PUT /nodes/*{uuid}*/pfaConfigSettings

Use this method to modify the predicted failure alerts (PFA) configuration settings on the baseboard management controller.

A 64-bit *category map* is used to identify hardware event categories and severities:

- **Bit 0**. RAS event VM movement support
- **Bit 1**. Processor subsystem
- **Bit 2**. Memory subsystem
- **Bit 3**. I/O subsystem
- **Bit 4**. Power
- **Bit 5**. Cooling
- **Bit 6**. Fans
- **Bit 7**. Storage
- **Bit 8**. CEC hardware (For System x servers, this bit is not supported and is set to 0.)
- **Bit 9**. Platform firmware
- **Bit 10**. Software
- **Bit 11**. External environment
- **Bit 12 – 25**. Reserved
- **Bit 26**. Redundancy degrade
- **Bit 27**. PFA
- **Bit 28**. Redundancy loss
- **Bit 29**. Info
- **Bit 30**. Warning
- **Bit 31**. Error

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/{uuid}/pfaConfigSettings`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
desiredCategories	Required	Long integer	Hardware event categories to be monitored. This can be a bitmask value as per the category map.

The following example modifies PFA configuration settings.

```
{
   "desiredCategories": 2147483684
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/nodes/*{uuid}*/ssdWearThreshold

Use this REST API to modify the SSD remaining-life alert threshold for ThinkSystem and ThinkAgile servers.

Note: This REST API requires Lenovo XClarity Administrator v3.6.0 or later.

HTTP methods

PUT

PUT /nodes/*{uuid}*/ssdWearThreshold

Use this method to modify the SSD remaining-life alert threshold for ThinkSystem and ThinkAgile servers.

Note: This REST API requires Lenovo XClarity Administrator v3.6.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/{uuid}/ssdWearThreshold`

where *{uuid}* is the UUID of the ThinkSystem or ThinkAgile server. To obtain the server UUIDs, use GET /nodes.

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
ssdWearThreshold	Required	Integer	SSD remaining-life alert threshold, as a percentage of remaining life. This can be a value from **0** – **100**. The default is **8**. When this threshold is exceeded, an alert is generated.

The following example sets the SSD remaining-life alert threshold to 50%.

```
{
   "ssdWearThreshold": 50
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/nodes/*{uuid}*/singleSignOn

Use this REST API to return the single sign-on setting or enable or disable single sign-on for a specific ThinkSystem or ThinkAgile server.

Note: This API requires Lenovo XClarity Administrator v3.3.0 or later.

HTTP methods

GET, PUT

GET /nodes/*{uuid}*/singleSignOn

Use this method to return the single sign-on setting for the specified ThinkSystem or ThinkAgile server.

Note: This API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/nodes/{uuid}/singleSignOn
```

where *{uuid}* is the UUID of the ThinkSystem or ThinkAgile server. To obtain the server UUIDs, use GET /nodes.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
ssoEnabled	Boolean	Indicates whether single sign-on is enabled. This can be one of the following values. • **true**. Single sign-on is enabled. • **false**. Single sign-on is disabled. **Note:** Single sign-on is disabled automatically when using the CyberArk identity-management system for authentication.

The following example is returned if the request is successful.

```
{
   "ssoEnabled": true
}
```

PUT /nodes/*{uuid}*/singleSignOn

Use this method to enable or disable single sign-on for a specific ThinkSystem or ThinkAgile server.

Note: This API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
PUT https://{management_server_IP}/nodes/{uuid}/singleSignOn
```

where *{uuid}* is the UUID of the ThinkSystem or ThinkAgile server. To obtain the server UUIDs, use GET /nodes.

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
ssoEnabled	Required	Boolean	Indicates whether single sign-on is enabled. This can be one of the following values. • **true**. Single sign-on is enabled. • **false**. Single sign-on is disabled. **Note:** Single sign-on is disabled automatically when using the CyberArk identity-management system for authentication.

The following example clears a port-forwarding configuration.

```
{
   "ssoEnabled": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/nodes/*{uuid}*/systemGuardSetting

Use this REST API to return the System Guard settings for a specific managed servers with XCC2.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

GET

GET /nodes/*{uuid}*/systemGuardSetting

Use this method to return the System Guard settings for a specific managed servers with XCC2 only.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://<management_server_IP>/nodes/{uuid}/systemGuardSetting`

where *{uuid}* is the UUID of the server. To obtain the server UUIDs, use GET /nodes.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

The URI and ID of the root job are returned in the **Location** field, for example:

```
Location: /tasks/34
```

Response body

Attributes	Type	Description
lockDownPolicy	String	Indicates the behavior when System Guard is enabled. This can be one of the following values. • **GenerateEventOnly**. When any inventory change is detected, an event is raised, but no other action is taken. This is default behavior on devices. • **PreventOSBooting**. When a processor or memory inventory change is detected, an event is raised. If you attempt to boot into the OS, you are warned if System Guard detects configuration changes. In this case, you are prompted to log into the baseboard management controller if the changes are unexpected; otherwise, you can continue the boot or shutdown process.
osBootPreventing	Boolean	Indicates whether to prevent booting the OS when processor or memory deviations are detected between the snapshot and the current inventory (when the status is **noncompliant**). This can be one of the following values. • **true**. Rebooting the OS is prevented when processor or memory deviations are detected. • **false**. Rebooting the OS is allowed when processor or memory deviations are detected.
status	String	Compliance status. This can be one of the following values. • **Compliant**. The snapshot matches the current inventory for the device. • **Noncompliant**. The snapshot does not match the current inventory for the device.
systemGuardEnabled	Boolean	Indicates whether System Guard is enabled. This can be one of the following values. • **true**. System Guard is enabled. • **false**. System Guard is disabled.

The following example is returned if the request is successful.

```
{
   "lockDownPolicy": "PreventOSBooting",
   "osBootPreventing" : true,
   "status" : "Noncompliant",
   "systemGuardEnabled": true
}
```

/nodes/cryptoSettings

Use this REST API to modify the current cryptographic settings on one or more managed servers with XCC2.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

PUT

PUT /nodes/cryptoSettings

Use this method to modify the current cryptographic settings on one or more managed servers with XCC2.

This method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform

this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

To modify the current cryptographic setting for the management server, use PUT /cryptoSettings.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/cryptoSettings`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
uuid	Required	String	UUID of the managed device to configure
securityMode	Required	String	Security Mode. This can be one of the following values. • **NIST SP 800-131A** • **Compatibility Security** • **Standard Security** • **Enterprise Strict Security**

The following example set security mode for all target servers.

```
[{
   "uuid": "fbb43c13103511e785f2e4a2ced78753",
   "securityMode": "Standard Security"
},
{
   "uuid": "23abc13103511e785f2e4a2ced787de",
   "securityMode": "Standard Security"
}]
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

/nodes/globalConfigSettings

Use this REST API to retrieve and modify global inventory-configuration settings.

Note: This API requires Lenovo XClarity Administrator v3.0.0 or later.

HTTP methods

GET, PUT

GET /nodes/globalConfigSettings

Use this method to return global-configuration settings for ThinkAgile and ThinkSystem servers.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/nodes/globalConfigSettings
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
SMARTDataRetrievalPreference	Boolean	Indicates whether to enable the collection of SMART data. This can be one of the following values. • **true**. SMART data collection is enabled. • **false**. (default) SMART data collection is disabled.
secureEraseMaxServerLimit	Integer	Maximum number of servers on which the secure-erase operation can be performed at one time You can specify a value from **3 – 100**. The default value is **3**.

The following example is returned if the request is successful.

```
{

   "SMARTDataRetrievalPreference": false,
   "secureEraseMaxServerLimit": 5
}
```

PUT /nodes/globalConfigSettings

Use this method to modify global-configuration settings for ThinkAgile and ThinkSystem servers.

Note: You must have **lxc-supervisor** authority to update these settings.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/globalConfigSettings`

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
SMARTDataRetrievalPreference	Optional	Boolean	Indicates whether to enable the collection of SMART data. This can be one of the following values. • **true**. SMART data collection is enabled. • **false**. (default) SMART data collection is disabled.
secureEraseMaxServerLimit	Optional	Integer	Maximum number of servers on which the secure-erase operation can be performed at one time You can specify a value from **3 – 100**. The default value is **3**.

The following example enables collecting SMART data and limits the secure-erase operation to up to 5 servers.

```
{

   "SMARTDataRetrievalPreference": true,
   "secureEraseMaxServerLimit": 5
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/nodes/linkStatusPreference

Use this REST API to retrieve and modify the link-status preference.

HTTP methods

GET, PUT

GET /nodes/linkStatusPreference

Use this method to return the link-status preference.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/linkStatusPreference`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

Parameters	Type	Description
linkStatus	Boolean	Indicates whether an alert is raised when the link status of a port changes. This can be one of the following values. • **true**. Alerts are raised for link-status changes. • **false**. (default) Alerts are not raised for link-status changes.

The following example is returned if the request is successful.

```
{
   "linkStatus": true
}
```

PUT /nodes/linkStatusPreference

Use this method to modify the link-status preference.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/linkStatusPreference`

Query parameters

None

Request body

Parameter	Re-quired / Optional	Type	Description
linkStatus	Required	Boolean	Indicates whether an alert is raised when the link status of a port changes. This can be one of the following values. • **true**. Alerts are raised for link-status changes. • **false**. (default) Alerts are not raised for link-status changes.

The following example enables raising alerts when a link-status changes.

```
{
   "linkStatus": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/nodes/ssdRemainingLifeStatistics

Use this REST API to return remaining-life statistics for SSDs in all or specific managed servers.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

HTTP methods

POST

POST /nodes/ssdRemainingLifeStatistics

Use this method to return remaining-life statistics for SSDs in all or specific managed servers.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/nodes/ssdRemainingLifeStatistics
```

Query parameters

Parameter	Required / Optional	Description
lowRemainingLifeBoundary=*{integer}*	Optional	Low remaining-life threshold, as a percentage The default value is **10**.
highRemainingLifeBoundary=*{integer}*	Optional	High remaining-life threshold, as a percentage The default value is **50**.

The following example returns statistics for SSDs with a low threshold of 10% and a high threshold of 50%.

```
POST https://192.0.2.0/nodes/ssdRemainingLifeStatistics
```

The following example returns statistics for SSDs with a low threshold of 15% and a high threshold of 85%.

```
POST https://192.0.2.0/nodes/ssdRemainingLifeStatistics
?lowRemainingLifeBoundary=15&highRemainingLifeBoundary=85
```

Request body

Attributes	Required / Optional	Type	Description
uuids	Optional	Array of strings	Returns statistics for SSDs in one or more specific servers, specified by UUIDs separated by a comma If not specified, statistics are returned for SSDs in *all* managed servers.

The following example returns remaining-life statistics for two managed servers.

```
{
   "uuids": ["FBEF740B178F4EFAA846E7225EE256DC", "B1B549049DE811E00005000500050005"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
highRemainingLife	Integer	Number of SSDs for which the remaining life is greater than the **highRemainingLifeBoundary**
lowRemainingLife	Integer	Number of SSDs for which the remaining life is less than or equal to the **lowRemainingLifeBoundary**
midRemainingLife	Integer	Number of SSDs for which the remaining life is between the **lowRemainingLifeBoundary** and **highRemainingLifeBoundary**
unknownRemainingLife	Integer	Number of SSDs for which the remaining life is unknown **Note:** XCC cannot retrieve the SSD remaining life for onboard SATA drives.

The following example is returned if the request is successful.

```
{
   "highRemainingLife": 180,
   "lowRemainingLife": 1,
   "midRemainingLife": 20,
   "unknownRemainingLife": 0
}
```

/nodes/SMARTData

Use this REST API to retrieve the most recent SMART data that was collected for all managed ThinkAgile and ThinkSystem servers or to collect SMART data for all manage ThinkAgile and ThinkSystem servers.

Note: This API requires Lenovo XClarity Administrator v3.0.0 or later.

HTTP methods

GET, POST

GET /nodes/SMARTData

Use this method to return the most recent SMART data that was collected for all managed ThinkAgile and ThinkSystem servers.

Note: This API requires Lenovo XClarity Administrator v3.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/SMARTData`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
nodeList	Object	Information about SMART data for each server
uuid	String	Server UUID
timestamp	Long	Timestamp when SMART data was collected
controllerList	Array of objects	Information about each drive
uuid	String	Drive UUID
smartData	Array of objects	SMART data for each drive This value is an empty string if SMART data does not exist for the drive.
disk	String	Serial number of the drive
details	String	Base64b encoded SMART data

The following example is returned if the request is successful.

```
{
   "nodeList": [{
```

```
      "controllerList": [{
         "smartData":[{
            "details":"Byte array data of disk smartdata",
            "disk":"disk_id11"
         },
         {
            "details":"Byte array data of disk smartdata",
            "disk":"disk_id12"
         }],
         "uuid":"controlleruuid1"
      },
      {
         "smartData":[{
            "details":"Byte array data of disk smartdata",
            "disk":"disk_id21"
         },
         {
            "details":"Byte array data of disk smartdata",
            "disk":"disk_id22"
         }],
         "uuid":"controlleruuid2"
      }],
      "timestamp": 924239842347328743,
      "uuid":"AAAAABBBBBBCCCCCCDDDDDDEEEEEE"
}
```

POST /nodes/SMARTData

Use this method to collect Self-Monitoring, Analysis and Reporting Technology (SMART) data for all manage ThinkAgile and ThinkSystem servers.

Notes:

- Servers must be powered on to collect SMART data.
- A job is created to collect SMART data. The response header includes the job ID for this request, in the format jobIDs="*{job_id}*" (for example, jobIDs="12"). You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

  Attention: A successful response indicates that the request was successfully transmitted and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.
- This API requires Lenovo XClarity Administrator v3.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/nodes/SMARTData`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
action	Required	String	This value is always **collectSMARTData**. *SMART data* is collected from hard drives and solid-state drives and is used to analyze drive reliability and detect imminent hardware failures. If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response body returns a URI in the form /tasks/*{task_id}* (for example, /tasks/12) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully transmitted and accepted by the management server. It does not indicate that the operation that is associated with the job was successful. **Note:** SMART data collection must be enabled (see GET /nodes/globalConfigSettings).

The following example collects SMART data.

```
{
   "action": "collectSMARTData"
}
```

Response codes

Code	Description	Comments
202	Accepted	The request has been accepted for processing, but the processing has not yet completed. The request might or might not be acted upon, depending on the results of the processing.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/nodes/systemGuardSetting

Use this REST API to enable or disable System Guard on one or more managed servers with XCC2.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

PUT

PUT /nodes/systemGuardSetting

Use this method to enable or disable System Guard on one or more managed servers with XCC2 only.

This request starts a job that runs in the background to perform the operation. The response body returns the job URI for this request. Use GET /tasks/*{job_list}* to monitor the status and progress of the job.

A successful response code indicates that the job was successfully transmitted and accepted by the portal. It does not indicate that the operation that is associated with the job was successful. If a job was not successfully started, refer to the response code and response body for details.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/systemGuardSetting`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
lockDownPolicy	Optional	String	Indicates the behavior when **systemGuardEnable** is **true**, an inventory change is detected, and the server becomes non-compliant. This can be one of the following values. If not specified, the current setting on the device remains as is. • **GenerateEventOnly**. When any inventory change is detected, an event is raised, but no other action is taken. This is default behavior on devices. • **PreventOSBooting**. When a processor or memory inventory change is detected, an event is raised. If you attempt to boot into the OS, you are warned if System Guard detects configuration changes. In this case, you are prompted to log into the baseboard management controller if the changes are unexpected; otherwise, you can continue the boot or shutdown process.
systemGuardEnabled	Required	Boolean	Indicates whether to enable System Guard. This can be one of the following values. • **true**. Enables System Guard • **false**. Disables System Guard
uuids	Required	Array of strings	List of UUIDs of managed devices to configure

The following example enables System Guard and sets the non-compliant behavior to prevent OS booting on all target servers.

```
{
   "lockDownPolicy": "PreventOSBooting",
   "systemGuardEnabled": true,
   "uuids": ["FBB43C13103511E785f2E4A2CED78753", "23ABC13103511E785f2E4A2CED787DE"]
}
```

The following example disables System Guard on all target servers.

```
{
   "systemGuardEnabled": false,
   "uuids": ["FBB43C13103511E785f2E4A2CED78753", "23ABC13103511E785f2E4A2CED787DE"]
}
```

Response codes

Code	Description	Comments
202	Accepted	The request has been accepted for processing, but the processing has not yet completed. The request might or might not be acted upon, depending on the results of the processing.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

The URI the root job are returned in the **Location** field, for example:

```
Location: /tasks/34
```

Response body

Attributes	Type	Description
path	String	URI of the root job

The following example is returned if the request is successful.

```
{
   "path": "/tasks/34"
}
```

/nodes/tlsSettings

Use this REST API to modify the current TLS settings on one or more managed servers with XCC2.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

PUT

PUT /nodes/tlsSettings

Use this method to modify the current TLS settings on one or more managed devices.

This method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

To modify the current cryptographic setting for the management server, use PUT /cryptoSettings.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

You can change the security settings for the following devices.
- Lenovo ThinkSystem servers with Intel or AMD processors (except SR635 / SR655)
- Lenovo ThinkSystem V2 servers
- Lenovo ThinkSystem V3 servers with Intel or AMD processors
- Lenovo ThinkEdge SE350 / SE450 servers
- Lenovo System x servers

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/nodes/tlsSettings`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
minTlsVersionClient	Required	String	Minimum TLS protocol version to use for client connections to other servers (such as the LDAP client). This can be one of the following values. • **TLS1.2**. Enforces TLS v1.2 cryptography protocols. • **TLS1.3**. Enforces TLS v1.3 cryptography protocols. **Notes:** • For CMMs, this value is used for client connections (such as an LDAP client). • System x and CMM devices support only TLS v1.2.
minTlsVersionServer	Required	String	Minimum TLS protocol version to use for server connections (such as the web server). This can be the following value. • **TLSv1.2**. Enforces TLS v1.2 or later cryptography protocols. **Note:** This attribute is supported only for CMMs.
uuidList	Required	String Should this be an array of strings?	List of device UUIDs, separated by a comma

The following example modifies the TLS settings on two ThinkSystem servers with XCC2.

```
{
   "minTlsVersionClient": "TLSv1.2",
   "minTlsVersionServer": "TLSv1.2",
   "uuidList": "8923abcfa78e232,23423424bcde895864"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/powerSupplies

Use this REST API to retrieve properties for power supplies in all Flex System chassis.

HTTP methods

GET

GET /powerSupplies

Use this method to return properties for power supplies in all Flex System chassis.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/powerSupplies`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
powerSupplyList	Array of objects	List of all power supplies in all chassis
See GET /powerSupplies/*{uuid}*	Object	Detailed information about each power supply

The following example is returned if the request is successful.


```
{
"powerSupplyList": [{
   "cmmDisplayName": "Power Supply 01",
   "cmmHealthState": "Non-Critical",
   "dataHandle": 0,
   "description": "Power Supply",
   "firmware": [{
      "build": "",
      "date": "",
      "name": "Power Supply Firmware",
      "role": "",
      "status": "",
      "type": "Power Supply Firmware",
      "version": "0"
   }],
   "FRU": "69Y5817",
   "fruSerialNumber": "ZK125116E0KK",
   "hardwareRevision": "5.0",
   "inputVoltageIsAC": true,
   "inputVoltageMax": 208,
   "inputVoltageMin": 200,
   "leds": [{
      "color": "Green",
      "location": "Planar",
      "name": "IN",
      "state": "On"
   },
   ...,
   {
      "color": "Amber",
      "location": "Planar",
      "name": "FAULT",
      "state": "Off"
   }],
   "machineType": "",
   "manufacturer": "IBM",
   "manufactureDate": "2411",
   "manufacturerId": "20301",
   "model": "",
   "name": "Power Supply 01",
   "parent": {
      "uri": "chassis/FBEF740B178F4EFAA846E7225EE256DC",
```

```
      "uuid": "FBEF740B178F4EFAA846E7225EE256DC"
   },
   "partNumber": "69Y5801",
   "posID": "128",
   "powerAllocation": {
      "totalInputPower": 0,
      "totalOutputPower": 0
   },
   "powerState": "Unknown",
   "productId": "303",
   "productName": "IBM 2500 W Power Supply",
   "serialNumber": "",
   "slots": [1],
   "type": "PowerSupply",
   "uri": "powerSupply/B1B549049DE811E00005000500050005",
   "userDescription": "",
   "uuid": "B1B549049DE811E00005000500050005",
   "vpdID": "60"
}]
}
```


/powerSupplies/*{uuid}*

Use this REST API to retrieve the properties for a specific power supply in a Flex System chassis.

HTTP methods

GET

GET /powerSupplies/*{uuid}*

Use this method to return properties for a specific power supply in a Flex System chassis.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/powerSupplies/{uuid}`

where *{uuid}* is the UUID of the power supply to be retrieved. To obtain the power supply UUID, use the GET /powerSupplies method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=*<attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
cmmDisplayName	String	Display name provided by the CMM
cmmHealthState	String	Health summary that corresponds to the highest event severity of all the devices in the chassis. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
dataHandle	Long	Time stamp of the last status update
description	String	Description that was provided by the CMM.
firmware	Array of objects	Power-supply firmware details
build	String	Firmware build
date	String	Firmware date
name	String	Firmware name
role	String	Firmware role
status	String	Firmware status
type	String	Firmware type
version	String	Firmware version
FRU	String	FRU part number
fruSerialNumber	String	FRU serial number
hardwareRevision	String	Hardware revision
inputVoltageIsAC	Boolean	Identifies whether the input voltage is AC or DC. This can be one of the following values. The value is valid only if **inputVoltageMin** and **inputVoltageMax** are valid. • **true**. AC • **false**. DC
inputVoltageMax	Long	Maximum input voltage. A value of **-1** mean it has not been set yet.
inputVoltageMin	Long	Minimum input voltage. A value of **-1** means it has not been set yet.
LEDs	Array of objects	Information about power-supply LEDs
color	String	LED color. This can be one of the following values. • **Red** • **Amber** • **Yellow** • **Green** • **Blue** • **Unknown**

Attributes	Type	Description
location	String	LED location. This can be one of the following values. • **Front panel** • **Lightpath Card** • **Planar** • **FRU** • **Rear Panel** • **Unknown**
name	String	LED name
state	String	LED state This can be one of the following values. • **Off** • **On** • **Blinking** • **Unknown**
machineType	String	Machine type
manufacturer	String	Manufacturer
manufactureDate	String	Manufacture date
manufacturerID	String	Manufacturer ID
model	String	Power-supply model
name	String	Name that is displayed in the user interface for this device
parent	Object	
uri	String	Parent URI
uuid	String	Parent UUID
partNumber	String	Part number
posID	String	Position ID
powerAllocation	Object	
totalInputPower	Long	Total input power
totalOutputPower	Long	Total output power
powerState	String	Current power state of the power supply. This can be one of the following values. • **Off** • **On** • **ShuttingDown** • **Standby** • **Hibernate** • **Unknown**
productID	String	Product ID
productName		Product name
serialNumber	String	Serial number
slots	Integer	Power-supply primary slot
type	String	Resource type. This value is always “PowerSupply.”
uri	String	URI
userDescription	String	User description

Attributes	Type	Description
uuid	String	UUID
vpdID	String	VPD ID

The following example is returned if the request is successful.


```
{
   "cmmDisplayName": "Power Supply 01",
   "cmmHealthState": "Non-Critical",
   "dataHandle": 0,
   "description": "Power Supply",
   "firmware": [{
      "build": "",
      "date": "",
      "name": "Power Supply Firmware",
      "role": "",
      "status": "",
      "type": "Power Supply Firmware",
      "version": "0"
   }],
   "FRU": "69Y5817",
   "fruSerialNumber": "ZK125116E0KK",
   "hardwareRevision": "5.0",
   "inputVoltageIsAC": true,
   "inputVoltageMax": 208,
   "inputVoltageMin": 200,
   "leds": [{
      "color": "Green",
      "location": "Planar",
      "name": "IN",
      "state": "On"
   },
   ...,
   {
      "color": "Amber",
      "location": "Planar",
      "name": "FAULT",
      "state": "Off"
   }],
   "machineType": "",
   "manufacturer": "IBM",
   "manufactureDate": "2411",
   "manufacturerId": "20301",
   "model": "",
   "name": "Power Supply 01",
   "parent": {
      "uri": "chassis/FBEF740B178F4EFAA846E7225EE256DC",
      "uuid": "FBEF740B178F4EFAA846E7225EE256DC"
   },
   "partNumber": "69Y5801",
   "posID": "128",
   "powerAllocation": {
      "totalInputPower": 0,
      "totalOutputPower": 0
   },
   "powerState": "Unknown",
   "productId": "303",
   "productName": "IBM 2500 W Power Supply",
   "serialNumber": "",
   "slots": [1],
```

```
   "type": "PowerSupply",
   "uri": "powerSupply/B1B549049DE811E00005000500050005",
   "userDescription": "",
   "uuid": "B1B549049DE811E00005000500050005",
   "vpdID": "60"
}
```

/scalableComplex

Use this REST API to retrieve properties for all scalable complexes. A *scalable complex* is a portfolio comprised of rack servers or Flex compute nodes that can be scaled to two, four, or eight sockets, depending on workload needs.

HTTP methods

GET

GET /scalableComplex

Use this method to return properties for all scalable complexes.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/scalableComplex`

Query parameters

Attributes	Required / Optional	Description
complexType=*{type}*	Optional	Returns a JSON response that includes only compute nodes or rack servers. This can be one of the following values. • **flex**. Flex System compute nodes • **rackserver**. System x rack servers
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
complex	Array	List of scalable complexes.
See GET /scalableComplex/*{uuid}*	Object	Detailed information about each scalable complex.

The following example is returned if the request is successful.


```
{
"complex": [{
   "complexID": "C29379AA380E11E39DF3000AF7256714",
   "location": {
      "location": "here",
      "lowestRackUnit": 35,
      "rack": "ZD123",
      "room": "here"
   },
   "nodeCount": 1,
   "orphanNodes": [],
  "partition": [{
     "nodes": [{
         "FRU": "None",
         "accessState": "Online",
         "activationKeys": [{
            "description": "IBM Integrated Management Module Advanced Upgrade",
            "keyExpirationDate": "",
            "keyFeatureType": 1,
            "keyIdentiferList": [{
               "keyIdentifier": "5463KVD0153",
               "keyIdentifierType": "MT"
            }],
            "keyStatus": "VALID",
            "keyUseCount": 0,
            "keyUseLimit": 0,
            "uuid": "8f0f1789295e78f9"
         }],
         "addinCardSlots": 0,
         "addinCards": [{
            "FRU": "N/A",
            "firmware": [{
               "build": "0",
```

```
            "classifications": [13],
            "date": "2015-04-06T00:00:00Z",
            "name": "LSI MegaRAID Adapter Firmware",
            "revision": "0",
            "role": "Primary",
            "softwareID": "10140454",
            "status": "Active",
            "type": "Software Bundle",
            "version": "24.7.0-0052"
         }],
         "fodUniqueID": "N/A",
         "fruSerialNumber": "SV42100396",
         "isAddOnCard": true,
         "isAgentless": true,
         "manufacturer": "IBM",
         "name": "ServeRAID M5210",
         "partNumber": "N/A",
         "pciBusNumber": "1",
         "pciDeviceNumber": "0",
         "pciFunctionNumber": "0",
         "pciRevision": "2",
         "pciSubID": "454",
         "pciSubVendorID": "1014",
         "portInfo": {,
         "posID": "5d",
         "productName": "ServeRAID M5210",
         "slotName": "SlotDesig4_Slot 4",
         "slotNumber": "4",
         "slotSupportsHotPlug": "false",
         "vpdID": "1000"
      }],
      "arch": "x86",
      "backedBy": "real",
      "bladeState": 0,
      "bootMode": {
         "currentValue": "UEFI Mode",
         "possibleValues": [
            "UEFI Mode",
            "Legacy Mode"
      ]},
      "bootOrder": {
         "bootOrderList": [{
            "bootType": "SingleUse",
            "currentBootOrderDevices": ["None"],
            "possibleBootOrderDevices": [
               "None",
               "PXE Network",
               "Disk Drive 0",
               "Diagnostics",
               "CD/DVD Rom",
               "Boot To F1",
               "Hypervisor",
               "Floppy Disk"
            ]
         },
         {
            "bootType": "Permanent",
            "currentBootOrderDevices": [
               "CD/DVD Rom",
               "Disk Drive 0",
               "PXE Network"
```

```
    ],
    "possibleBootOrderDevices": [
       "CD/DVD Rom",
       "Hard Disk 0",
       "PXE Network",
       "Floppy Disk",
       "Disk Drive 1",
       "Disk Drive 2",
       "Disk Drive 3",
       "Disk Drive 4",
       "USB Storage",
       "Diagnostics",
       "iSCSI",
       "iSCSI Critical",
       "Embedded Hypervisor",
       "Legacy Only",
       "IMM1",
       "IMM2",
       "USB1",
       "USB2",
       "USB3",
       "USB4",
       "USB5",
       "USB6",
       "SdRaid",
       "USB8",
       "Slot4",
       "Slot1",
       "Slot2",
       "Slot2",
       "Slot3",
       "NIC1",
       "NIC2",
       "NIC3",
       "NIC4",
       "CD/DVD",
       "SATA Port 0",
       "SATA Port 1",
       "SATA Port 2",
       "SATA Port 3",
       "sSATA Port 0",
       "sSATA Port 1",
       "sSATA Port 2",
       "sSATA Port 3",
       "DSA"
]},
{
    "bootType": "WakeOnLAN",
    "currentBootOrderDevices": [
       "PXE Network",
       "CD/DVD Rom",
       "Disk Drive 0"
    ],
    "possibleBootOrderDevices": [
       "PXE Network",
       "CD/DVD Rom",
       "Disk Drive 0",
       "Floppy Disk",
       ...,
       "sSATA Port 2",
       "sSATA Port 3",
```

```
            "DSA"
         ]
      }],
      "uri": "node/425AF828DF7D11D4B0F8E76767BBBBBB/bootOrder"
   },
   "cmmDisplayName": "Management Controller UUID-425AF828DF7D11D4B0F8E76767BBBBBB",
   "cmmHealthState": "Normal",
   "complexID": -1,
   "contact": "",
   "dataHandle": 1440525606363,
   "description": "Chassis",
   "dnsHostnames": [
      "10.243.6.69",
      "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:1585"
   ],
   "domainName": "",
   "driveBays": 0,
   "drives": [],
   "embeddedHypervisorPresence": false,
   "errorFields": [{
      "ChassisMounted": "NO_CONNECTOR"
   }],
   "excludedHealthState": "Normal",
   "expansionCardSlots": 0,
         "expansionCards": [],
   "expansionProductType": "",
   "expansionProducts": [],
   "firmware": [{
      "build": "TBE105KUS",
      "date": "2015-04-17T00:00:00Z",
      "name": "UEFI Firmware/BIOS",
      "role": "Primary",
      "status": "Active",
      "type": "UEFI",
      "version": "1.10"
   },
   ...,
   {
      "build": "TCOOO9D",
      "date": "2015-04-17T00:00:00Z",
      "name": "IMM2 Backup Firmware",
      "role": "Backup",
      "status": "Inactive",
      "type": "IMM2-Backup",
      "version": "1.71"
   }],
   "flashStorage": [],
   "fruSerialNumber": "None",
   "hasOS": false,
   "height": 1,
   "hostMacAddresses": "40:F2:E9:B8:15:80,40:F2:E9:B8:15:81,40:F2:E9:B8:15:82,40:F2:E9:B8:15:83",
   "hostname": "IMM2-40f2e9b81585",
   "ipInterfaces": [{
      "IPv4DHCPmode": "STATIC_ONLY",
      "IPv4assignments": [{
         "address": "10.243.6.69",
         "gateway": "0.0.0.0",
         "id": 0,
         "subnet": "255.255.240.0",
         "type": "INUSE"
      }],
```

```
            "IPv4enabled": true,
            "IPv6DHCPenabled": true,
            "IPv6assignments": [{
               "address": "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:1585",
               "gateway": "0:0:0:0:0:0:0:0",
               "id": 0,
               "prefix": 64,
               "scope": "Global",
               "source": "Stateless",
               "type": "INUSE"
            },
            {
               "address": "fe80:0:0:0:42f2:e9ff:feb8:1585",
               "gateway": "0:0:0:0:0:0:0:0",
               "id": 0,
               "prefix": 64,
               "scope": "LinkLocal",
               "source": "Other",
               "type": "INUSE"
            }],
            "IPv6enabled": true,
            "IPv6statelessEnabled": true,
            "IPv6staticEnabled": false,
            "label": "unknown",
            "name": "eth0"
         }],
          "ipv4Addresses": [
             "10.243.6.69",
             "169.254.95.118"
          ],
          "ipv6Addresses": [
             "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:1585",
             "fe80::42f2:e9ff:feb8:1585"
          ],
          "isConnectionTrusted": "true",
          "isITME": false,
          "isRemotePresenceEnabled": true,
          "isScalable": false,
          "lanOverUsb": "enabled",
         "leds": [{
             "color": "Yellow",
             "location": "Unknown",
             "name": "Fault",
             "state": "Off"
          },
...,
          {
            "color": "Yellow",
             "location": "Planar",
             "name": "SDRAID Error",
             "state": "Off"
          }],
          "location": {
             "location": "",
             "lowestRackUnit": 0,
             "rack": "",
             "room": ""
          },
          "macAddress": "40:F2:E9:B8:15:85,40:F2:E9:B8:15:86",
          "machineType": "5463",
          "manufacturer": " IBM(WIST)",
```

```
"manufacturerId": " IBM(WIST)",
"memoryModules": [{
   "capacity": 4,
   "displayName": "DIMM 1",
   "manufacturer": "Unknown",
   "model": "DDR4",
   "partNumber": "HMA451R7MFR8N-TFTD ",
   "serialNumber": "103D4F44",
   "slot": 1,
   "speed": 2133,
   "type": "DDR4"
}],
"memorySlots": 0,
"mgmtProcIPaddress": "10.243.6.69",
"model": "45Z",
"name": "DaAn5",
"nist": {
   "currentValue": "Compatibility",
   "possibleValues": ["Compatibility",
   "Nist_800_131A_Strict"]
},
"onboardPciDevices": [{
   "firmware": [{
      "build": "0",
      "classifications": [0],
      "date": "",
      "name": "PCIFirmware",
      "revision": "0",
      "role": "Primary",
      "softwareID": "1014:405",
      "status": "Active",
      "type": "",
      "version": ""
   }],
   "fodUniqueID": "",
   "isAddOnCard": false,
   "isAgentless": false,
   "name": "",
   "pciBusNumber": "25",
   "pciDeviceNumber": "0",
   "pciFunctionNumber": "0",
   "pciRevision": "1",
   "pciSubID": "405",
   "pciSubVendorID": "1014",
   "portInfo": {},
   "posID": "534",
   "vpdID": "102b"
},
...,
{
   "firmware": [{
      "build": "0",
      "classifications": [33024],
      "date": "",
      "name": "17.0.4.4a",
      "revision": "0",
      "role": "Primary",
      "softwareID": "101404D1",
      "status": "Active",
      "type": "VPD-V0",
     "version": "17.0.4.4a"
```

```
            }],
            "fodUniqueID": "11SBCM957190123456789",
            "isAddOnCard": false,
            "isAgentless": true,
            "name": "Broadcom NetXtreme Gigabit Ethernet Adapter",
            "pciBusNumber": "27",
            "pciDeviceNumber": "0",
            "pciFunctionNumber": "3",
            "pciRevision": "1",
            "pciSubID": "4d1",
            "pciSubVendorID": "1014",
            "portInfo": {
               "logicalPorts": [{
                  "addresses": "40F2E9B81583",
                  "portNumber": 1,
                  "portType": "ETHERNET",
                  "vnicMode": false
               }],
               "peerBay": 0,
               "portNumber": 4,
               "portType": "ETHERNET"
            },
            "posID": "1657",
            "vpdID": "14e4"
         }],
         "overallHealthState": "Normal",
         "partNumber": "00KC903",
         "partitionID": -1,
         "pciCapabilities": [
    "Raid Link",
"OOB PCIe",
"Raid Link Config",
"Raid Link Alert",
"OOB PCIe Config"
],
         "pciDevices": [{
            "FRU": "N/A",
            "firmware": [{
               "build": "0",
               "classifications": [13],
               "date": "2015-04-06T00:00:00Z",
               "name": "LSI MegaRAID Adapter Firmware",
               "revision": "0",
               "role": "Primary",
               "softwareID": "10140454",
               "status": "Active",
               "type": "Software Bundle",
               "version": "24.7.0-0052"
            }],
            "fodUniqueID": "N/A",
            "fruSerialNumber": "SV42100396",
            "isAddOnCard": true,
            "isAgentless": true,
            "manufacturer": "IBM",
            "name": "ServeRAID M5210",
            "partNumber": "N/A",
            "pciBusNumber": "1",
            "pciDeviceNumber": "0",
            "pciFunctionNumber": "0",
            "pciRevision": "2",
            "pciSubID": "454",
```

```
      "pciSubVendorID": "1014",
      "portInfo": {},
      "posID": "5d",
      "productName": "ServeRAID M5210",
      "slotName": "SlotDesig4_Slot 4",
      "slotNumber": "4",
      "slotSupportsHotPlug": "false",
      "vpdID": "1000"
   },
   ...,
   {
      "firmware": [{
         "build": "0",
         "classifications": [33024],
         "date": "",
         "name": "17.0.4.4a",
         "revision": "0",
         "role": "Primary",
         "softwareID": "101404D1",
         "status": "Active",
         "type": "VPD-V0",
         "version": "17.0.4.4a"
      }],
      "fodUniqueID": "11SBCM957190123456789",
      "isAddOnCard": false,
      "isAgentless": true,
      "name": "Broadcom NetXtreme Gigabit Ethernet Adapter",
      "pciBusNumber": "27",
      "pciDeviceNumber": "0",
      "pciFunctionNumber": "3",
      "pciRevision": "1",
      "pciSubID": "4d1",
      "pciSubVendorID": "1014",
      "portInfo": {
         "logicalPorts": [{
            "addresses": "40F2E9B81583",
            "portNumber": 1,
           "portType": "ETHERNET",
            "vnicMode": false
         }],
         "peerBay": 0,
         "portNumber": 4,
         "portType": "ETHERNET"
      },
      "posID": "1657",
      "vpdID": "14e4"
   }],
  "ports": [{
      "ioModuleBay": 0,
      "portNumber": 1
   },
  ...,
   {
      "ioModuleBay": 0,
      "portNumber": 4
   }],
   "posID": "",
   "powerAllocation": {
      "maximumAllocatedPower": 660,
      "minimumAllocatedPower": 26
   },
```

```
"powerCappingPolicy": {
   "cappingACorDCMode": "DC",
   "cappingPolicy": "OFF",
   "currentPowerCap": 0,
   "maxPowerCap": 319000,
   "maximumPowerCappingHotPlugLevel": 367000,
   "minPowerCap": 85300,
   "minimumHardCapLevel": 246200,
   "minimumPowerCappingHotPlugLevel": 268000,
   "powerCappingAllocUnit": "watts*10^-3"
},
"powerStatus": 5,
"powerSupplies": [{
   "FRU": "",
   "cmmDisplayName": "Power Supply 1",
   "dataHandle": 0,
   "description": "",
   "firmware": [],
   "fruSerialNumber": "",
   "hardwareRevision": "",
   "healthState": "CRITICAL",
   "inputVoltageIsAC": true,
   "inputVoltageMax": -1,
   "inputVoltageMin": -1,
   "leds": [],
   "machineType": "",
   "manufactureDate": "",
   "manufacturer": "EMER",
   "manufacturerId": "",
   "model": "",
   "name": "Power Supply 1",
   "partNumber": "94Y8136",
   "posID": "",
   "powerAllocation": {
      "totalInputPower": 0,
      "totalOutputPower": 550000
   },
   "powerState": "Unknown",
   "productId": "",
   "productName": "",
   "serialNumber": "K118146600A",
   "slots": [1],
  "type": "PowerSupply",
   "uri": "powerSupply/",
   "userDescription": "",
   "uuid": "",
   "vpdID": ""
},
{
   "FRU": "",
   "cmmDisplayName": "Power Supply 2",
  "dataHandle": 0,
   "description": "",
   "firmware": [],
   "fruSerialNumber": "",
   "hardwareRevision": "",
   "healthState": "CRITICAL",
   "inputVoltageIsAC": true,
   "inputVoltageMax": -1,
   "inputVoltageMin": -1,
   "leds": [],
```

```
      "machineType": "",
      "manufactureDate": "",
      "manufacturer": "EMER",
      "manufacturerId": "",
      "model": "",
      "name": "Power Supply 2",
      "partNumber": "94Y8136",
      "posID": "",
      "powerAllocation": {
         "totalInputPower": 0,
         "totalOutputPower": 550000
      },
      "powerState": "Unknown",
      "productId": "",
      "productName": "",
      "serialNumber": "K1181466087",
      "slots": [2],
      "type": "PowerSupply",
      "uri": "powerSupply/",
      "userDescription": "",
      "uuid": "",
      "vpdID": ""
   }],
   "processorSlots": 0,
   "processors": [{
      "cores": 10,
      "displayName": "Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz",
     "family": "INTEL_R_XEON_TM",
      "manufacturer": "Intel(R) Corporation",
      "productVersion": "Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz",
      "slot": 1,
      "speed": 2.2999999999999998
   }],
   "productId": "4D4F00",
   "productName": "Lenovo System x3550 M5",
   "raidSettings": [{
      "description": "ServeRAID M5210",
      "diskDrives": [{
         "FRU": "42D0631",
         "bay": 0,
         "blockSize": 512,
         "description": "AL13SEB300",
         "diskState": "System",
         "healthState": "Normal",
         "interfaceType": "SAS",
         "manufacturer": "IBM-ESXS",
         "mediaType": "Rotational",
         "model": "AL13SEB300",
         "name": "Disk 0_0",
         "numberOfBlocks": 585937500,
         "partNumber": "42D0628",
         "serialNumber": "44P012H5",
         "uuid": ""
      },
      ...,
      {
         "FRU": "81Y3810",
         "bay": 1,
         "blockSize": 512,
         "description": "ST9300653SS",
         "diskState": "System",
```

```
                "healthState": "Normal",
                "interfaceType": "SAS",
                "manufacturer": "IBM-ESXS",
                "mediaType": "Rotational",
                "model": "ST9300653SS",
                "name": "Disk 2_2",
                "numberOfBlocks": 585937500,
                "partNumber": "81Y9667",
                "serialNumber": "6XN3J9M9",
                "uuid": ""
             }],
            "firmware": [{
                "build": "0",
                "classifications": [],
                "date": "2015-04-06T00:00:00Z",
                "name": "LSI MegaRAID Adapter Firmware",
                "revision": "0",
                "role": "Primary",
                "softwareID": "10140454",
                "status": "Active",
                "type": "",
                "version": "24.7.0-0052"
             }],
             "name": "ServeRAID M5210",
            "uuid": "00000000000000000500605B008E4828O"
          }],
          "secureBootMode": {
             "currentValue": "Disabled",
            "possibleValues": ["Disabled",
             "Enabled"]
          },
          "serialNumber": "KVD0153",
          "slots": [1],
          "status": {
             "message": "managed",
             "name": "MANAGED"
          },
          "subSlots": [],
          "subType": "",
          "tlsVersion": {
             "currentValue": "TLS_10",
            "possibleValues": ["TLS_10",
             "TLS_11",
             "TLS_12"]
          },
          "type": "Rack-Tower Server",
          "uri": "node/425AF828DF7D11D4B0F8E76767BBBBBB",
          "userDescription": "",
          "uuid": "425AF828DF7D11D4B0F8E76767BBBBBB",
          "vnicMode": "disabled",
          "vpdID": ""
       }],
       "partitionID": 1,
       "uuid": "C29379AA380E11E39DF3000AF7256714"
    }],
    "partitionCount": 1,
    "uuid": "C29379AA380E11E39DF3000AF7256714"
}]
}
```

/scalableComplex/*{uuid}*

Use this REST API to retrieve properties for a specific scalable complexes. A *scalable complex* is a portfolio comprised of rack servers or Flex compute nodes that can be scaled to two, four, or eight sockets, depending on workload needs.

HTTP methods

GET

GET /scalableComplex/*{uuid}*

Use this method to return properties for a specific scalable complex.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/scalableComplex/{uuid}`

where *{uuid}* is the UUID of the scalable complex to be retrieved. To obtain the scalable complex UUID, use the GET /scalableComplex method.

Query parameters

Attributes	Required / Optional	Description
complexType=*{type}*	Optional	Returns a JSON response that includes only compute nodes or rack servers. This can be one of the following values. • **flex**. Flex System compute nodes • **rackserver**. System x rack servers
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
complexID	String	Scalable complex ID
location	Object	
location	String	
lowestRackUnit	String	
rack	String	
room	String	
nodeCount	Integer	Number of nodes in the scalable complex.
orphanNodes	Array of node objects	Information about orphan compute nodes and/or rack servers in the complex. For a list of response attributes, see GET /nodes.
partition	Array	Information about partitions in the scalable complex.
nodes	Array of node objects	Information about compute nodes and/or rack servers in the complex. For a list of response attribute, see GET /nodes.
partitionID	Integer	Partition ID
uuid	String	UUID
partitionCount	Integer	Partition count in complex
uuid	String	UUID

The following example is returned if the request is successful.


```
{
   "complexID": "C29379AA380E11E39DF3000AF7256714",
   "location": {
      "location": "here",
      "lowestRackUnit": 35,
      "rack": "ZD123",
      "room": "here"
   },
   "nodeCount": 1,
   "orphanNodes": [],
```

```
"partition": [{
   "nodes": [{
       "FRU": "None",
       "accessState": "Online",
       "activationKeys": [{
          "description": "IBM Integrated Management Module Advanced Upgrade",
          "keyExpirationDate": "",
          "keyFeatureType": 1,
          "keyIdentifierList": [{
             "keyIdentifier": "5463KVD0153",
             "keyIdentifierType": "MT"
          }],
          "keyStatus": "VALID",
          "keyUseCount": 0,
          "keyUseLimit": 0,
          "uuid": "8f0f1789295e78f9"
       }],
       "addinCardSlots": 0,
       "addinCards": [{
          "FRU": "N/A",
          "firmware": [{
             "build": "0",
             "classifications": [13],
             "date": "2015-04-06T00:00:00Z",
             "name": "LSI MegaRAID Adapter Firmware",
             "revision": "0",
             "role": "Primary",
             "softwareID": "10140454",
             "status": "Active",
             "type": "Software Bundle",
             "version": "24.7.0-0052"
          }],
          "fodUniqueID": "N/A",
          "fruSerialNumber": "SV42100396",
          "isAddOnCard": true,
          "isAgentless": true,
          "manufacturer": "IBM",
          "name": "ServeRAID M5210",
          "partNumber": "N/A",
          "pciBusNumber": "1",
          "pciDeviceNumber": "0",
          "pciFunctionNumber": "0",
          "pciRevision": "2",
          "pciSubID": "454",
          "pciSubVendorID": "1014",
          "portInfo": {,
          "posID": "5d",
          "productName": "ServeRAID M5210",
          "slotName": "SlotDesig4_Slot 4",
          "slotNumber": "4",
          "slotSupportsHotPlug": "false",
          "vpdID": "1000"
       }],
       "arch": "x86",
       "backedBy": "real",
       "bladeState": 0,
       "bootMode": {
          "currentValue": "UEFI Mode",
          "possibleValues": [
             "UEFI Mode",
             "Legacy Mode"
```

```
]},
"bootOrder": {
   "bootOrderList": [{
      "bootType": "SingleUse",
      "currentBootOrderDevices": ["None"],
      "possibleBootOrderDevices": [
         "None",
         "PXE Network",
         "Disk Drive 0",
         "Diagnostics",
         "CD/DVD Rom",
         "Boot To F1",
         "Hypervisor",
         "Floppy Disk"
      ]
   },
   {
      "bootType": "Permanent",
      "currentBootOrderDevices": [
         "CD/DVD Rom",
         "Disk Drive 0",
         "PXE Network"
      ],
      "possibleBootOrderDevices": [
         "CD/DVD Rom",
         "Disk Drive 0",
         "PXE Network",
         "Floppy Disk",
         "Disk Drive 1",
         "Disk Drive 2",
         "Disk Drive 3",
         "Disk Drive 4",
         "USB Storage",
         "Diagnostics",
         "iSCSI",
         "iSCSI Critical",
         "Embedded Hypervisor",
         "Legacy Only",
         "IMM1",
         "IMM2",
         "USB1",
         "USB2",
         "USB3",
         "USB4",
         "USB5",
         "USB6",
         "SdRaid",
         "USB8",
         "Slot4",
         "Slot1",
         "Slot2",
         "Slot2",
         "Slot3",
         "NIC1",
         "NIC2",
         "NIC3",
         "NIC4",
         "CD/DVD",
         "SATA Port 0",
         "SATA Port 1",
         "SATA Port 2",
```

```
            "SATA Port 3",
            "sSATA Port 0",
            "sSATA Port 1",
            "sSATA Port 2",
            "sSATA Port 3",
            "DSA"
      ]},
      {
         "bootType": "WakeOnLAN",
         "currentBootOrderDevices": [
            "PXE Network",
            "CD/DVD Rom",
            "Disk Drive 0"
         ],
         "possibleBootOrderDevices": [
            "PXE Network",
            "CD/DVD Rom",
            "Disk Drive 0",
            "Floppy Disk",
            ...,
            "sSATA Port 2",
            "sSATA Port 3",
            "DSA"
         ]
      }],
      "uri": "node/425AF828DF7D11D4B0F8E76767BBBBBB/bootOrder"
   },
   "cmmDisplayName": "Management Adapter UUID-425AF828DF7D11D4B0F8E76767BBBBBB",
   "cmmHealthState": "Normal",
   "complexID": -1,
   "contact": "",
   "dataHandle": 1440525606363,
   "description": "Chassis",
   "dnsHostnames": [
      "10.243.6.69",
      "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:1585"
   ],
   "domainName": "",
   "driveBays": 0,
   "drives": [],
   "embeddedHypervisorPresence": false,
   "errorFields": [{
      "ChassisMounted": "NO_CONNECTOR"
   }],
   "excludedHealthState": "Normal",
   "expansionCardSlots": 0,
         "expansionCards": [],
   "expansionProductType": "",
   "expansionProducts": [],
   "firmware": [{
      "build": "TBE105KUS",
      "date": "2015-04-17T00:00:00Z",
      "name": "UEFI Firmware/BIOS",
      "role": "Primary",
      "status": "Active",
      "type": "UEFI",
      "version": "1.10"
   },
   ...,
   {
      "build": "TCO009D",
```

```
      "date": "2015-04-17T00:00:00Z",
      "name": "IMM2 Backup Firmware",
      "role": "Backup",
      "status": "Inactive",
      "type": "IMM2-Backup",
      "version": "1.71"
   }],
   "flashStorage": [],
   "fruSerialNumber": "None",
   "hasOS": false,
   "height": 1,
   "hostMacAddresses": "40:F2:E9:B8:15:80,40:F2:E9:B8:15:81,40:F2:E9:B8:15:82,
                        40:F2:E9:B8:15:83",
   "hostname": "IMM2-40f2e9b81585",
   "ipInterfaces": [{
      "IPv4DHCPmode": "STATIC_ONLY",
      "IPv4assignments": [{
         "address": "10.243.6.69",
         "gateway": "0.0.0.0",
         "id": 0,
         "subnet": "255.255.240.0",
         "type": "INUSE"
      }],
      "IPv4enabled": true,
      "IPv6DHCPenabled": true,
      "IPv6assignments": [{
         "address": "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:1585",
         "gateway": "0:0:0:0:0:0:0:0",
         "id": 0,
         "prefix": 64,
         "scope": "Global",
         "source": "Stateless",
         "type": "INUSE"
      },
      {
         "address": "fe80:0:0:0:42f2:e9ff:feb8:1585",
         "gateway": "0:0:0:0:0:0:0:0",
         "id": 0,
         "prefix": 64,
         "scope": "LinkLocal",
         "source": "Other",
         "type": "INUSE"
      }],
      "IPv6enabled": true,
      "IPv6statelessEnabled": true,
      "IPv6staticEnabled": false,
      "label": "unknown",
      "name": "eth0"
   }],
   "ipv4Addresses": [
      "10.243.6.69",
      "169.254.95.118"
   ],
   "ipv6Addresses": [
      "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:1585",
      "fe80::42f2:e9ff:feb8:1585"
   ],
   "isConnectionTrusted": "true",
   "isITME": false,
   "isRemotePresenceEnabled": true,
   "isScalable": false,
```

```
          "lanOverUsb": "enabled",
         "leds": [{
             "color": "Yellow",
             "location": "Unknown",
             "name": "Fault",
             "state": "Off"
          },
...,
          {
            "color": "Yellow",
             "location": "Planar",
             "name": "SDRAID Error",
             "state": "Off"
          }],
          "location": {
             "location": "",
             "lowestRackUnit": 0,
             "rack": "",
             "room": ""
          },
          "macAddress": "40:F2:E9:B8:15:85,40:F2:E9:B8:15:86",
          "machineType": "5463",
          "manufacturer": " IBM(WIST)",
          "manufacturerId": " IBM(WIST)",
          "memoryModules": [{
             "capacity": 4,
             "displayName": "DIMM 1",
             "manufacturer": "Unknown",
             "model": "DDR4",
             "partNumber": "HMA451R7MFR8N-TFTD ",
             "serialNumber": "103D4F44",
             "slot": 1,
             "speed": 2133,
             "type": "DDR4"
          }],
          "memorySlots": 0,
          "mgmtProcIPaddress": "10.243.6.69",
          "model": "45Z",
          "name": "DaAn5",
          "nist": {
             "currentValue": "Compatibility",
             "possibleValues": ["Compatibility",
             "Nist_800_131A_Strict"]
          },
          "onboardPciDevices": [{
             "firmware": [{
                "build": "0",
                "classifications": [0],
                "date": "",
                "name": "PCIFirmware",
                "revision": "0",
                "role": "Primary",
                "softwareID": "1014:405",
                "status": "Active",
                "type": "",
                "version": ""
             }],
             "fodUniqueID": "",
             "isAddOnCard": false,
             "isAgentless": false,
             "name": "",
```

```
      "pciBusNumber": "25",
      "pciDeviceNumber": "0",
      "pciFunctionNumber": "0",
      "pciRevision": "1",
      "pciSubID": "405",
      "pciSubVendorID": "1014",
      "portInfo": {},
      "posID": "534",
      "vpdID": "102b"
   },
   ...,
   {
      "firmware": [{
         "build": "0",
         "classifications": [33024],
         "date": "",
         "name": "17.0.4.4a",
         "revision": "0",
         "role": "Primary",
         "softwareID": "101404D1",
         "status": "Active",
         "type": "VPD-V0",
        "version": "17.0.4.4a"
      }],
      "fodUniqueID": "11SBCM957190123456789",
      "isAddOnCard": false,
      "isAgentless": true,
      "name": "Broadcom NetXtreme Gigabit Ethernet Adapter",
      "pciBusNumber": "27",
      "pciDeviceNumber": "0",
      "pciFunctionNumber": "3",
      "pciRevision": "1",
      "pciSubID": "4d1",
      "pciSubVendorID": "1014",
      "portInfo": {
         "logicalPorts": [{
            "addresses": "40F2E9B81583",
            "portNumber": 1,
            "portType": "ETHERNET",
            "vnicMode": false
         }],
         "peerBay": 0,
         "portNumber": 4,
         "portType": "ETHERNET"
      },
      "posID": "1657",
      "vpdID": "14e4"
   }],
   "overallHealthState": "Normal",
   "partNumber": "00KC903",
   "partitionID": -1,
   "pciCapabilities": ["Raid Link","OOB PCIe","Raid Link Config","Raid Link Alert",
                       "OOB PCIe Config"],
   "pciDevices": [{
      "FRU": "N/A",
      "firmware": [{
         "build": "0",
         "classifications": [13],
         "date": "2015-04-06T00:00:00Z",
         "name": "LSI MegaRAID Adapter Firmware",
         "revision": "0",
```

```
            "role": "Primary",
            "softwareID": "10140454",
            "status": "Active",
            "type": "Software Bundle",
            "version": "24.7.0-0052"
        }],
        "fodUniqueID": "N/A",
        "fruSerialNumber": "SV42100396",
        "isAddOnCard": true,
        "isAgentless": true,
        "manufacturer": "IBM",
        "name": "ServeRAID M5210",
        "partNumber": "N/A",
        "pciBusNumber": "1",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "0",
        "pciRevision": "2",
        "pciSubID": "454",
        "pciSubVendorID": "1014",
        "portInfo": {},
        "posID": "5d",
        "productName": "ServeRAID M5210",
        "slotName": "SlotDesig4_Slot 4",
        "slotNumber": "4",
        "slotSupportsHotPlug": "false",
        "vpdID": "1000"
    },
    ...,
    {
        "firmware": [{
            "build": "0",
            "classifications": [33024],
            "date": "",
            "name": "17.0.4.4a",
            "revision": "0",
            "role": "Primary",
            "softwareID": "101404D1",
            "status": "Active",
            "type": "VPD-V0",
            "version": "17.0.4.4a"
        }],
        "fodUniqueID": "11SBCM957190123456789",
        "isAddOnCard": false,
        "isAgentless": true,
        "name": "Broadcom NetXtreme Gigabit Ethernet Adapter",
        "pciBusNumber": "27",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "3",
        "pciRevision": "1",
        "pciSubID": "4d1",
        "pciSubVendorID": "1014",
        "portInfo": {
            "logicalPorts": [{
                "addresses": "40F2E9B81583",
                "portNumber": 1,
              "portType": "ETHERNET",
                "vnicMode": false
            }],
            "peerBay": 0,
            "portNumber": 4,
            "portType": "ETHERNET"
```

```
      },
      "posID": "1657",
      "vpdID": "14e4"
   }],
  "ports": [{
      "ioModuleBay": 0,
      "portNumber": 1
   },
  ...,
   {
      "ioModuleBay": 0,
      "portNumber": 4
   }],
   "posID": "",
   "powerAllocation": {
      "maximumAllocatedPower": 660,
      "minimumAllocatedPower": 26
   },
   "powerCappingPolicy": {
      "cappingACorDCMode": "DC",
      "cappingPolicy": "OFF",
      "currentPowerCap": 0,
      "maxPowerCap": 319000,
      "maximumPowerCappingHotPlugLevel": 367000,
      "minPowerCap": 85300,
      "minimumHardCapLevel": 246200,
      "minimumPowerCappingHotPlugLevel": 268000,
      "powerCappingAllocUnit": "watts*10^-3"
   },
   "powerStatus": 5,
   "powerSupplies": [{
      "FRU": "",
      "cmmDisplayName": "Power Supply 1",
      "dataHandle": 0,
      "description": "",
      "firmware": [],
      "fruSerialNumber": "",
      "hardwareRevision": "",
      "healthState": "CRITICAL",
      "inputVoltageIsAC": true,
      "inputVoltageMax": -1,
      "inputVoltageMin": -1,
      "leds": [],
      "machineType": "",
      "manufactureDate": "",
      "manufacturer": "EMER",
      "manufacturerId": "",
      "model": "",
      "name": "Power Supply 1",
      "partNumber": "94Y8136",
      "posID": "",
      "powerAllocation": {
         "totalInputPower": 0,
         "totalOutputPower": 550000
      },
      "powerState": "Unknown",
      "productId": "",
      "productName": "",
      "serialNumber": "K118146600A",
      "slots": [1],
     "type": "PowerSupply",
```

```
      "uri": "powerSupply/",
      "userDescription": "",
      "uuid": "",
      "vpdID": ""
   },
   {
      "FRU": "",
      "cmmDisplayName": "Power Supply 2",
     "dataHandle": 0,
      "description": "",
      "firmware": [],
      "fruSerialNumber": "",
      "hardwareRevision": "",
      "healthState": "CRITICAL",
      "inputVoltageIsAC": true,
      "inputVoltageMax": -1,
      "inputVoltageMin": -1,
      "leds": [],
      "machineType": "",
      "manufactureDate": "",
      "manufacturer": "EMER",
      "manufacturerId": "",
      "model": "",
      "name": "Power Supply 2",
      "partNumber": "94Y8136",
      "posID": "",
      "powerAllocation": {
         "totalInputPower": 0,
         "totalOutputPower": 550000
      },
      "powerState": "Unknown",
      "productId": "",
      "productName": "",
      "serialNumber": "K1181466087",
      "slots": [2],
      "type": "PowerSupply",
      "uri": "powerSupply/",
      "userDescription": "",
      "uuid": "",
      "vpdID": ""
   }],
   "processorSlots": 0,
   "processors": [{
      "cores": 10,
      "displayName": "Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz",
     "family": "INTEL_R_XEON_TM",
      "manufacturer": "Intel(R) Corporation",
      "productVersion": "Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz",
      "slot": 1,
      "speed": 2.2999999999999998
   }],
   "productId": "4D4F00",
   "productName": "Lenovo System x3550 M5",
   "raidSettings": [{
      "description": "ServeRAID M5210",
      "diskDrives": [{
         "FRU": "42D0631",
         "bay": 0,
         "blockSize": 512,
         "description": "AL13SEB300",
         "diskState": "System",
```

```
      "healthState": "Normal",
      "interfaceType": "SAS",
      "manufacturer": "IBM-ESXS",
      "mediaType": "Rotational",
      "model": "AL13SEB300",
      "name": "Disk 0_0",
      "numberOfBlocks": 585937500,
      "partNumber": "42D0628",
      "serialNumber": "44P012H5",
      "uuid": ""
   },
   ...,
   {
      "FRU": "81Y3810",
      "bay": 1,
      "blockSize": 512,
      "description": "ST9300653SS",
      "diskState": "System",
      "healthState": "Normal",
      "interfaceType": "SAS",
      "manufacturer": "IBM-ESXS",
      "mediaType": "Rotational",
      "model": "ST9300653SS",
      "name": "Disk 2_2",
      "numberOfBlocks": 585937500,
      "partNumber": "81Y9667",
      "serialNumber": "6XN3J9M9",
      "uuid": ""
   }],
  "firmware": [{
      "build": "0",
      "classifications": [],
      "date": "2015-04-06T00:00:00Z",
      "name": "LSI MegaRAID Adapter Firmware",
      "revision": "0",
      "role": "Primary",
      "softwareID": "10140454",
      "status": "Active",
      "type": "",
      "version": "24.7.0-0052"
   }],
   "name": "ServeRAID M5210",
  "uuid": "0000000000000000500605B008E48280"
}],
"secureBootMode": {
   "currentValue": "Disabled",
  "possibleValues": ["Disabled",
   "Enabled"]
},
"serialNumber": "KVD0153",
"slots": [1],
"status": {
   "message": "managed",
   "name": "MANAGED"
},
"subSlots": [],
"subType": "",
"tlsVersion": {
   "currentValue": "TLS_10",
  "possibleValues": ["TLS_10",
   "TLS_11",
```

```
            "TLS_12"]
         },
         "type": "Rack-Tower Server",
         "uri": "node/425AF828DF7D11D4B0F8E76767BBBBBB",
         "userDescription": "",
         "uuid": "425AF828DF7D11D4B0F8E76767BBBBBB",
         "vnicMode": "disabled",
         "vpdID": ""
      }],
      "partitionID": 1,
      "uuid": "C29379AA380E11E39DF3000AF7256714"
   }],
   "partitionCount": 1,
   "uuid": "C29379AA380E11E39DF3000AF7256714"
}
```


/storage

Use this REST API to retrieve properties for all storage devices.

HTTP methods

GET, POST

GET /storage

Use this method to return properties for all storage devices and tape libraries.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/storage
```

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
formatType=*{type}*	Optional	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv** If the format type is not specified, JSON format is returned. **Note:** To retrieve properties for a large number of devices, use POST /storage.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

The following example returns a CSV file that contains information about all storage devices.

```
GET https://192.0.2.0 /storage?formatType=csv
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
storageList	Array	List of all storage devices and tape libraries.
See GET /storage/*{uuid_list}*	Object	Detailed information about the individual storage device and and tape library.

Response example

The following example is returned if the request is successful.


```
{
    "storageList": [{
        "accessState": Online",
        "canisterSlots": 2,
        "cmmHealthState": "Normal",
        "contact": "F",
        "description": "F",
        "diskGroups": 2,
        "driveBays": 12,
        "enclosureCount": 1,
        "enclosures": [{
            "canisters": [{
                "cmmDisplayName": "controller_a",
                "controllerId": "A",
                "controllerRedundancyMode": "Active-ActiveULP",
                "controllerRedundancyStatus": "Redundant",
                "disks": 9,
                "diskBusType": "SAS",
                "diskChannels": 2,
                "energyMetrics": {
                    "diskControllerTemperature": [],
                    "inletAirTemperature": [],
                    "memoryTemperature": []
                },
                "expansionPorts": [{
                    "health": "N/A",
                    "healthReason": "No drive enclosure is connected to this expansion port. This is normal if this
                                     is the last (or only) enclosure in the cabling sequence of the system.",
                    "healthRecommendation": "-Noactionisrequired.",
                    "name": "OutPort",
                    "status": "Disconnected"
                }],
                "failOverReason": "Notapplicable",
                "failedOverToThisController": "No",
                "firmware": {
                    "backplaneType": "7",
                    "bundleVersion": "GL221R020-14",
                    "buildDate": "ThuJun2909: 26: 26MDT2017",
                    "capiVersion": "3.19",
                    "cpldCodeVersion": "56",
                    "diskInterfaceHardwareVersion": "3",
                    "expanderControllerCodeVersion": "3206",
                    "hardwareVersion": "5.2",
                    "hostInterfaceHardwareVersion": "2",
                   "hostInterfaceModuleModel": "6",
                    "hostInterfaceModuleVersion": "11",
                    "managementControllerCodeVersion": "GLM221R037-02",
                  "managementControllerLoaderCodeVersion": "6.27.25440",
                    "scBootMemoryReferenceCodeVersion": "1.2.1.10",
```

```
   "storageControllerCodeBaselevel": "GLS221R13-01",
    "storageControllerCodeVersion": "GLS221R13-01",
    "storageControllerCpuType": "Gladden1300MHz",
    "storageControllerLoaderCodeVersion": "27.016",
    "version": "5.6",
    "versionType": "nonencrypted"
},
"hardwareVersion": "5.2",
"health": "Normal",
"healthReason": "",
"healthRecommendation": "",
"hostPorts": 4,
"networkPorts": {
    "addressingMode": "Manual",
    "gateway": "10.243.0.1",
    "health": "OK",
   "healthReason": "",
    "healthRecommendation": "",
    "ipAddress": "10.243.9.148",
    "ipVersion": 4,
    "macAddress": "00: c0: ff: 28: 03: c7",
    "name": "mgmtport_a",
    "networkMask": "255.255.240.0"
},
"phyIsolation": "Enabled",
"ports": [{
    "action": "- If this host port is intentionally unused, no actionis required.\n
                - Otherwise, use an appropriate interface cable to connect this host
                  port to a switch o rhost.\n
                - If a cable is connected, check the cable and the switch or host for
                  problems.",
    "actualSpeed": "",
    "configSpeed": "Auto",
    "health": "N/A",
    "media": "FC(-)",
    "port": "A2",
    "reason": "There is no active connection to this host port.",
    "status": "Disconnected",
    "targetId": "227000c0ff280e8b",
    "topology": "PTP"
},
...,
{
    "action": "- If this host port is intentionally unused, no actionis required.\n
                - Otherwise, use an appropriate interface cable to connect this host
                  port to a switch o rhost.\n
                - If a cable is connected, check the cable and the switch or host for
                  problems.",
    "actualSpeed": "",
    "configSpeed": "Auto",
    "health": "N/A",
    "media": "FC(-)",
    "port": "A3",
    "reason": "There is no active connection to this host port.",
    "status": "Disconnected",
    "targetId": "237000c0ff280e8b",
    "topology": "PTP"
}]
"position": "Top",
"powerState": "On",
"revision": "0",
```

```
    "serialNumber": "11S00WC050Y010DH677180",
    "status": "Operational",
    "systemCacheMemory": 6144,
}],
"drives": [{
    "firmwareVersion": null",
    "health": "OK",
    "healthReason": "",
    "healthRecommendation": "",
    "location": "0.9",
    "model": "ST2000NM0034X",
    "serialNumber": "Z4H02R730000R538RM68",
    "size": "2000.3TiB",
    "status": "Up",
    "type": "SASMDL",
    "vendorName": "LENOVO-X"
},
...,
{
    "firmwareVersion": null,
    "health": "OK",
    "healthReason": "",
    "healthRecommendation": "",
    "location": "0.4",
    "model": "ST2000NM0034X",
    "serialNumber": "Z4H07S8L0000R628K52C",
    "size": "2000.3TiB",
    "status": "Up",
    "type": "SASMDL",
  "vendorName": "LENOVO-X"
}],
"enclosureInfo": {
    "diskCount": 9,
    "driveBays": 12,
    "enclosureId": 0,
    "health": "OK",
    "model": "S3200",
    "midplaneSerialNumber": "11S00WC065Y010DH67C0RF",
    "status": "Up",
    "vendorName": "Lenovo",
    "wwn": "500C0FF0280E8B3C"
},
"energyMetrics": {
    "enclosurePower": []
},
"frus": [{
    "description": "SPSMemoryCard",
    "fruLocation": "LOWERIOMMEMORYCARDSLOT",
    "fruStatus": "OK",
    "partNumber": "40-00000053",
    "serialNumber": "",
    "shortName": "MemoryCard"
},
...,
{
    "description": "48X44xCNCRIOM-LX6GBLENOVO",
    "fruLocation": "LOWERIOMSLOT",
    "fruStatus": "OK",
  "partNumber": "00WC050",
    "serialNumber": "11S00WC050Y010DH677182",
    "shortName": "RAIDIOM"
```

```
    }],
     "location": {
          "lowestRackUnit": 0,
          "location": "",
          "rack": "",
          "room": ""
     },
     "powerSupplies": [{
          "health": "OK",
          "healthReason": "",
          "healthRecommendation": "",
          "model": "00WC067",
          "position": "Right",
          "status": "Up",
          "vendorName": ""
     },
     {
          "health": "OK",
          "healthReason": "",
          "healthRecommendation": "",
          "model": "00WC067",
          "position": "Left",
          "status": "Up",
          "vendorName": ""
     }],
     "slots": ["0", "1", "2", "4", "5", "6", "8", "9", "10"]
}],
"excludedHealthState": "Normal",
"healthReason": "",
"ipv4Addresses": ["10.243.9.148", "10.243.9.149"],
"isConnectionTrusted": "true",
"location": {
     "location": "",
     "lowestRackUnit": 0,
     "rack": "",
     "room": ""
     },
"machineType": "6411",
"mgmtProcIPaddress": "192.0.2.0",
"model": "S3200",
"name": "S3200",
"otherMcStatus": "Operational",
"overallHealthState": "Normal",
"parent": {
     "uri": "",
     "uuid": ""
},
"pfu": "Idle",
"productBrand": "Storage",
"productName": "S3200",
"scsiProductId": "S3200",
"scsiVendorId": "Lenovo",
"securityDescriptor": {
     "managedAuthEnabled": true
     "managedAuthSupported": true,
     "publicAccess": true,
     "roleGroups": ["lxc-admin","lxc-security-admin"],
     "storedCredentials": null,
     "uri": "storage/0069030ADC5F453E9EE49CA4B44DB8DC"
},
"serialNumber": "280E8B",
```

```
        "storageNodeCapacityList": [{
            "blockStorage": {
                "available": "6.66 TiB",
                "fullThresholdPercent": "96",
                "size": "6.83 TiB",
                "used": "168 GiB"
            },
            "nodeName": "PerfDM7100F-02"
        }, {
            "blockStorage": {
                "available": "6.66 TiB",
                "fullThresholdPercent": "96",
                "size": "6.83 TiB",
                "used": "168 GiB"
            },
            "nodeName": "PerfDM7100F-01"
        }],
        "supportedLocales": "English(English), Arabic(ةيبرعلا), Portuguese(português), Spanish(español),
                             French(français), German(Deutsch), Italian(italiano), Japanese(日本語),
                             Korean(한국어), Dutch(Nederlands), Russian(русский),
                             Chinese-Simplified(简体中文), Chinese-Traditional(繁體中文)",
        "systemLocation": "LXCA_empty_field, LXCA_empty_field, LXCA_empty_field",
        "type": "LenovoStorage",
        "userDefinedName": "Storage1",
        "userDescription": "F",
        "uri": "storage/208000C0FF280E8B",
        "uuid": "208000C0FF280E8B",
        "vendorName": "Lenovo",
        "virtualPools": 2,
        "wwnn": "208000C0FF280E8B",
    }]
}
```


POST /storage

Use this method to return properties for a large number of specific storage devices.

Note: If you choose **formatType=csv**, this request creates a file in CSV format and returns the filename in the request header. You can use to download the file using GET /storage/*{file_name}*.csv.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/storage`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
formatType	Optional	String	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv**
uuids	Required	String	List of device UUIDs, separated by a comma

The following example returns properties for two storage devices.

```
{
   "formatType": "csv",
   "uuids": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully. This is returned when **formatType** is “json.”
201	Created	One or more new resources were successfully created. This is returned when **formatType** is “csv.”
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

If **formatType=csv** is specified, the response header includes the URI of the downloaded file. If data for a single storage device is requested, the file name includes the storage UUID. If multiple storage devices are requested, the file name is `allStorage_`*{unique_ID}*`.csv`. For example:

```
Status Code: 201 Created
Location: /chassis/EF6D424FAACA4E539771B812AAEE0F73.csv
```

Response body

If the **formatType=csv** request attribute is specified, no response body is returned.

If the **formatType=json** request attribute is specified, the following JSON object is returned.

Attributes	Type	Description
storageList	Array	List of all storage devices.
See GET /storage/*{uuid_list}*	Object	Detailed information about each storage device.

The following example is returned if the request is successful.


```
{
"storageList": {
    "storageList": [{
        "accessState": Online",
        "canisterSlots": 2,
        "cmmHealthState": "Normal",
        "contact": "F",
        "description": "F",
        "diskGroups": 2,
        "driveBays": 12,
        "enclosureCount": 1,
        "enclosures": [{
            "canisters": [{
                "cmmDisplayName": "controller_a",
                "controllerId": "A",
                "controllerRedundancyMode": "Active-ActiveULP",
                "controllerRedundancyStatus": "Redundant",
                "disks": 9,
                "diskBusType": "SAS",
                "diskChannels": 2,
                "energyMetrics": {
                    "diskControllerTemperature": [],
                    "inletAirTemperature": [],
                    "memoryTemperature": []
                },
                "expansionPorts": [{
                    "health": "N/A",
                    "healthReason": "No drive enclosure is connected to this expansion port. This is normal if this
                                    is the last (or only) enclosure in the cabling sequence of the system.",
                    "healthRecommendation": "-Noactionisrequired.",
                    "name": "OutPort",
                    "status": "Disconnected"
                }],
                "failOverReason": "Notapplicable",
                "failedOverToThisController": "No",
                "firmware": {
                    "backplaneType": "7",
                    "bundleVersion": "GL221R020-14",
                    "buildDate": "ThuJun2909: 26: 26MDT2017",
                    "capiVersion": "3.19",
                    "cpldCodeVersion": "56",
                    "diskInterfaceHardwareVersion": "3",
                    "expanderControllerCodeVersion": "3206",
                    "hardwareVersion": "5.2",
                    "hostInterfaceHardwareVersion": "2",
                   "hostInterfaceModuleModel": "6",
                    "hostInterfaceModuleVersion": "11",
                    "managementControllerCodeVersion": "GLM221R037-02",
                  "managementControllerLoaderCodeVersion": "6.27.25440",
                    "scBootMemoryReferenceCodeVersion": "1.2.1.10",
                  "storageControllerCodeBaselevel": "GLS221R13-01",
                    "storageControllerCodeVersion": "GLS221R13-01",
                    "storageControllerCpuType": "Gladden1300MHz",
                    "storageControllerLoaderCodeVersion": "27.016",
                    "version": "5.6",
                    "versionType": "nonencrypted"
                },
                "hardwareVersion": "5.2",
                "health": "Normal",
                "healthReason": "",
```

```
    "healthRecommendation": "",
    "hostPorts": 4,
    "networkPorts": {
        "addressingMode": "Manual",
        "gateway": "10.243.0.1",
        "health": "OK",
       "healthReason": "",
        "healthRecommendation": "",
        "ipAddress": "10.243.9.148",
        "ipVersion": 4,
        "macAddress": "00: c0: ff: 28: 03: c7",
        "name": "mgmtport_a",
        "networkMask": "255.255.240.0"
    },
    "phyIsolation": "Enabled",
    "ports": [{
        "action": "- If this host port is intentionally unused, no actionis required.\n
                   - Otherwise, use an appropriate interface cable to connect this host
                     port to a switch o rhost.\n
                   - If a cable is connected, check the cable and the switch or host for
                     problems.",
        "actualSpeed": "",
        "configSpeed": "Auto",
        "health": "N/A",
        "media": "FC(-)",
        "port": "A2",
        "reason": "There is no active connection to this host port.",
        "status": "Disconnected",
        "targetId": "227000c0ff280e8b",
        "topology": "PTP"
    },
    ...,
    {
        "action": "- If this host port is intentionally unused, no actionis required.\n
                   - Otherwise, use an appropriate interface cable to connect this host
                     port to a switch o rhost.\n
                   - If a cable is connected, check the cable and the switch or host for
                     problems.",
        "actualSpeed": "",
        "configSpeed": "Auto",
        "health": "N/A",
        "media": "FC(-)",
        "port": "A3",
        "reason": "There is no active connection to this host port.",
        "status": "Disconnected",
        "targetId": "237000c0ff280e8b",
        "topology": "PTP"
    }]
    "position": "Top",
    "powerState": "On",
    "revision": "0",
    "serialNumber": "11S00WC050Y010DH677180",
    "status": "Operational",
    "systemCacheMemory": 6144,
}],
"drives": [{
    "firmwareVersion": null",
    "health": "OK",
    "healthReason": "",
    "healthRecommendation": "",
    "location": "0.9",
```

```
      "model": "ST2000NM0034X",
      "serialNumber": "Z4H02R730000R538RM68",
      "size": "2000.3TiB",
      "status": "Up",
      "type": "SASMDL",
      "vendorName": "LENOVO-X"
   },
   ...,
   {
      "firmwareVersion": null,
      "health": "OK",
      "healthReason": "",
      "healthRecommendation": "",
      "location": "0.4",
      "model": "ST2000NM0034X",
      "serialNumber": "Z4H07S8L0000R628K52C",
      "size": "2000.3TiB",
      "status": "Up",
      "type": "SASMDL",
     "vendorName": "LENOVO-X"
   }],
   "enclosureInfo": {
      "diskCount": 9,
      "driveBays": 12,
      "enclosureId": 0,
      "health": "OK",
      "model": "S3200",
      "midplaneSerialNumber": "11S00WC065Y010DH67C0RF",
      "status": "Up",
      "vendorName": "Lenovo",
      "wwn": "500C0FF0280E8B3C"
   },
   "energyMetrics": {
      "enclosurePower": []
   },
   "frus": [{
      "description": "SPSMemoryCard",
      "fruLocation": "LOWERIOMMEMORYCARDSLOT",
      "fruStatus": "OK",
      "partNumber": "40-00000053",
      "serialNumber": "",
      "shortName": "MemoryCard"
   },
   ...,
   {
      "description": "48X44xCNCRIOM-LX6GBLENOVO",
      "fruLocation": "LOWERIOMSLOT",
      "fruStatus": "OK",
     "partNumber": "00WC050",
      "serialNumber": "11S00WC050Y010DH677182",
      "shortName": "RAIDIOM"
  }],
   "location": {
      "lowestRackUnit": 0,
      "location": "",
      "rack": "",
      "room": ""
   },
   "powerSupplies": [{
      "health": "OK",
      "healthReason": "",
```

```
            "healthRecommendation": "",
            "model": "00WC067",
            "position": "Right",
            "status": "Up",
            "vendorName": ""
        },
        {
            "health": "OK",
            "healthReason": "",
            "healthRecommendation": "",
            "model": "00WC067",
            "position": "Left",
            "status": "Up",
            "vendorName": ""
        }],
        "slots": ["0", "1", "2", "4", "5", "6", "8", "9", "10"]
}],
"excludedHealthState": "Normal",
"healthReason": "",
"ipv4Addresses": ["10.243.9.148", "10.243.9.149"],
"isConnectionTrusted": "true",
"location": {
    "location": "",
    "lowestRackUnit": 0,
    "rack": "",
    "room": ""
    },
"machineType": "6411",
"mgmtProcIPaddress": "192.0.2.0",
"model": "S3200",
"name": "S3200",
"otherMcStatus": "Operational",
"overallHealthState": "Normal",
"parent": {
    "uri": "",
    "uuid": ""
},
"pfu": "Idle",
"productBrand": "Storage",
"productName": "S3200",
"scsiProductId": "S3200",
"scsiVendorId": "Lenovo",
"securityDescriptor": {
    "managedAuthEnabled": true
    "managedAuthSupported": true,
    "publicAccess": true,
    "roleGroups": ["lxc-admin","lxc-security-admin"],
    "storedCredentials": null,
    "uri": "storage/0069030ADC5F453E9EE49CA4B44DB8DC"
},
"serialNumber": "280E8B",
"storageNodeCapacityList": [{
    "blockStorage": {
        "available": "6.66 TiB",
        "fullThresholdPercent": "96",
        "size": "6.83 TiB",
        "used": "168 GiB"
    },
    "nodeName": "PerfDM7100F-02"
}, {
    "blockStorage": {
```

```
                "available": "6.66 TiB",
                "fullThresholdPercent": "96",
                "size": "6.83 TiB",
                "used": "168 GiB"
            },
            "nodeName": "PerfDM7100F-01"
        }],
        "supportedLocales": "English(English), Arabic(ةيبرعلا), Portuguese(português), Spanish(español),
                             French(français), German(Deutsch), Italian(italiano), Japanese(日本語),
                             Korean(한국어), Dutch(Nederlands), Russian(русский),
                             Chinese-Simplified(简体中文), Chinese-Traditional(繁體中文)",
        "systemLocation": "LXCA_empty_field, LXCA_empty_field, LXCA_empty_field",
        "type": "LenovoStorage",
        "userDefinedName": "Storage1",
        "userDescription": "F",
        "uri": "storage/208000C0FF280E8B",
        "uuid": "208000C0FF280E8B",
        "vendorName": "Lenovo",
        "virtualPools": 2,
        "wwnn": "208000C0FF280E8B",
    }]
}
}
```

/storage/*{file_name}*.csv

Use this REST API to download inventory for a large number of specific storage devices in CSV format to the local system.

HTTP methods

GET

GET /storage/*{file_name}*.csv

Use this method to download inventory for a large number of specific storage devices in CSV format to the local system.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/storage/{file_name}.csv`

where *{file_name}*.csv is the file name of the CSV file that contains inventory data. Use the POST /storage method to with the **formatType=csv** request parameter to create the CSV file. The POST /storage method returns the file name in the request header.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/storage/*{uuid}*

Use this REST API to retrieve properties for a specific storage device.

HTTP methods

GET

GET /storage/*{uuid_list}*

Use this method to return properties for one or more storage devices and tape libraries.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/storage/{uuid_list}`

where *{uuid_list}* is a list of one or more UUIDs, separated by a comma, of the storage devices and tape libraries to be retrieved. To obtain the storage UUIDs, use the GET /storage method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
formatType=*{type}*	Optional	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv** If the format type is not specified, JSON format is returned.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

The following example returns a CSV file that contains information about two storage devices.

```
GET https://192.0.2.0/storage/0E7D8E1CDF7D11D4ABB0D5D5D5313131,0E7D8E1CDF7D11D4ABB0D5D5E7533456
?formatType=csv
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The returned attributes vary, depending on the type of device.

Attributes	Type	Description
accessState	String	Access state of the server. This can be one of the following values. • **Online** • **Offline** • **Partial** • **Pending** • **Unknown**
baseFWRevision	String	(Tape library only) Base firmware revision
baseFWBuildDate	String	(Tape library only) Base firmware build date
canisterSlots	Integer	Canister slots
cmmHealthState	String	Health summary that corresponds to the highest event severity of all storage devices. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
contact	String	(Storage devices only) Contact
description	String	(Storage devices only) Description
diskGroups	Integer	(Storage devices only)
driveBays	Integer	Drive bays
enclosureCount	Integer	Number of enclosures
enclosures	Array of objects	Information about each enclosure
batteries	Array of objects	(Storage devices only)
age	String	
daysUntilReplacement	String	
position	String	
serialNumber	String	
status	String	
vendorName	String	
canisters	Array of objects	(Storage devices only) Information about storage controllers (canisters)
cmmDisplayName	String	(Flex System storage devices only) The display name provided by the CMM
controllerId	String	

Attributes	Type	Description
controllerRedundancyMode	String	
controllerRedundancyStatus	String	
disks	Integer	Number of disks
diskBusType	String	
diskChannels	Integer	
energyMetrics	Object	Energy metrics for the storage controller Each energy metric contains one or more arrays that include when the sample was taken (timeStamp) and the value of the sample (metricValue).
diskControllerTemperature	Array of objects	Disk-controller temperature samples
inletAirTemperature		Inlet air temperature samples
memoryTemperature		Memory temperature samples
ethPorts	Array of objects	(DM storage only) Information about Ethernet ports
broadcastDomain	String	
enabled	Boolean	Indicates whether the port is enabled. This can be one of the following values. • **true** • **false**
macAddress	String	Port MAC address
metric	Array of objects	Port metrics
duration	String	
status	String	
throughput	String	Port throughput. This can be one of the following values. • **read** • **write** • **total**
timestamp	String	
mtu	String	Maximum transmission unit
name	String	Port name
node	String	
speed	String	Port speed
state	String	Port state
type	String	Port type
uuid	String	Port UUID
fcPorts	Array of objects	(DM storage only) Information about Fibre Channel ports
description	String	Port description

Attributes	Type	Description
enabled	Boolean	Indicates whether the port is enabled. This can be one of the following values. • **true** • **false**
fabric	String	
metric	Array of objects	Port metrics
duration	String	
status	String	
throughput	String	Port throughput. This can be one of the following values. • **read** • **write** • **total**
timestamp	String	
name	String	Port name
node	String	
physicalProtocol	String	
speed	String	Port speed
state	String	Port state
supportedProtocols	Array of strings	
uuid	String	Port UUID
wwnn	String	Port world-wide node name
wwpn	String	Port world-wide port name
expansionPorts	Array of objects	
health	String	
healthReason	String	
healthRecommendation	String	
media	String	
name	String	
status	String	
failOverReason	String	
failedOverToThisController	String	
firmware	Object	
backplaneType	String	
bundleVersion	String	
buildDate	String	

Attributes	Type	Description
capiVersion	String	
cpldCodeVersion	String	
diskInterfaceHardwareVersion	String	
expanderControllerCodeVersion	String	
hardwareVersion	String	
hostInterfaceHardwareVersion	String	
hostInterfaceModuleModel	String	
hostInterfaceModuleVersion	String	
managementControllerCodeVersion	String	
managementControllerLoaderCodeVersion	String	
scBootMemoryReferenceCodeVersion	String	
storageControllerCodeBaselevel	String	
storageControllerCodeVersion	String	
storageControllerCpuType	String	
storageControllerLoaderCodeVersion	String	
version	String	Firmware version in the format *<major}.{minor}*P*{patch>*, where P*{patch}* is optional in case there is no patch applied (for example, 9.7 or 9.7P3)
versionType	String	Firmware type. This can be one of the following values. • **encrypted** • **nonencrypted**
hardwareVersion	String	
health	String	
healthReason	String	
healthRecommendation	String	
drawers	Array of objects	(Tape library only) Information about drawer in the storage enclosure
drives	Array of objects	Information about drives in the storage enclosure
available	String	
health	String	
healthReason	String	
healthRecommendation	String	
firmwareVersion	String	Firmware version
location	String	
media	String	

Attributes	Type	Description
model	String	
serialNumber	String	
size	String	Drive capacity, in TiB
status	String	
type	String	
vendorName	String	
enclosureInfo	Object	
diskCount	Integer	
driveBays	Integer	
enclosureId	Integer	
generatedUUID	String	(Storage devices only) Unique identifier for an individual storage enclosure. This attribute is present only when the **wwn** attribute is not available for the enclosure
health	String	
height	String	(Storage devices only)
location	String	(Storage devices only)
midplaneSerialNumber	String	
model	String	
physicalNumber	Integer	(Tape library only) Number of physical enclosures
status	Integer	(Tape library only) Drive status. This can be one of the following values. • **Optimal**
vendorName	String	
wwn	String	
energyMetrics	Object	Energy metrics for the enclosure Each energy metric contains one or more arrays that include when the sample was taken (timeStamp) and the value of the sample (metricValue).
enclosurePower	Array of objects	Enclosure power samples
fans	Array of objects	(Storage devices only)
description	String	
status	String	
frus	Array of objects	
description	String	
fruLocation	String	

Attributes	Type	Description
fruStatus	String	
partNumber	String	FRU part number
serialNumber	String	FRU serial number
shortName	String	
hostAdapters	Array of objects	(Storage devices only)
model	String	
serialNumber	String	
status	String	
type	String	
hostPorts	Integer	
networkPorts	Object	
addressingMode	String	
gateway	String	
health	String	
healthReason	String	
healthRecommendation	String	
ipAddress	String	
ipVersion	Integer	
media	String	
macAddress	String	
name	String	
networkMask	String	
role	String	
phyIsolation	String	
ports	Array of objects	
action	String	
actualSpeed	String	
configSpeed	String	
health	String	
media	String	
port	String	
reason	String	
status	String	

Attributes	Type	Description
targetId	String	
topology	String	
position	String	
powerState	String	
revision	String	
serialNumber	String	
status	String	
systemCacheMemory	Long	
drawers	Array of objects	
name	String	
model	String	
opened	String	
serialNumber	String	
status	String	
ioModules	Array of objects	(Storage devices only)
fwVersion	String	
model	String	
location	Object	
location	String	
lowestRackUnit	String	
rack	String	
room	String	
powerSupplies	Array of objects	Information about power supplies in the enclosure
fwVersion	String	
health	String	
healthReason	String	
healthRecommendation	String	
model	String	Power-supply model.
position	String	
serialNumber	String	
status	String	
vendorName	String	

Attributes	Type	Description
slots	Array of strings	Information about storage slots
tapeDrives	Array of objects	(Tape library only) Information about each tape drive that is not in a partition
adtMode	String	
barcode	String	
cartridge	Boolean	
errorState	Boolean	
fwRevision	String	
generation	String	
interfaceType	String	
logicalNumber	String	
mfgSerialNumber	String	
module	String	
partition	String	
physicalNumber	String	
power	Boolean	
presence	Boolean	
product	String	
serialNumber	String	
vendor	String	
wwnodeName	String	
tapePartitions	Array of objects	(Tape library only) Information about each tape slot that is in a partition
autoClean	String	
barcodeAlign	String	
barcodeLength	String	
encryptionMode	String	
lunMasterDrive	String	
lunMasterDriveArr	String	
lunMasterDrivePhys	String	
lunMasterDrivePhysArr	String	
micw	String	
name	String	
numDrives	String	
numIOSlots	String	

Attributes	Type	Description
NumSlots	String	
partitionInventory	Object	(Tape library only) Inventory information about each tape partition
tapeDrives	Array of objects	(Tape library only) Information about each tape drive that is in a partition
fwRevision	String	
logicalNumber	String	
module	String	
partition	String	
physicalNumber	String	
product	String	
serialNumber	String	
vendor	String	
tapeSlots	Array of objects	(Tape library only) Information about each tape slot that is in a partition
access	String	
blocked	String	
cartridge	String	
cartridgeEncrypted	String	
cartridgeType	String	
logicalNumber	String	
mailslot	String	
module	String	
partition	String	
physicalNumber	String	
partitionNumber	String	
serialSumber	String	
wwNode	String	
tapeSlots	Array of objects	(Tape library only) Information about each tape slot that is in a partition
access	String	
blocked	String	
cartridge	String	
cartridgeEncrypted	String	
cartridgeType	String	
logicalNumber	String	

Attributes	Type	Description
mailslot	String	
module	String	
partition	String	
physicalNumber	String	
excludedHealthState	String	Highest severity alert with exclusions. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
expansionFWRevision	String	(Tape library only) Expansion firmware revision
healthReason	String	(Storage devices only)
ipv4Addresses	Array of strings	IPv4 address
isConnectionTrusted		
lastOfflineTimestamp	String	(Tape library only) Timestamp when the tape library was last offline
libHealth	String	(Tape library only) Library overall health
libraryType	String	(Tape library only) Library type
location	object	(Storage devices only) Information about the location of the storage device
location	String	Location
lowestRackUnit	String	Lowest rack unit
rack	String	Rack
room	String	Room
macAddress_1	String	(Tape library only) MAC address 1
macAddress_2	String	(Tape library only) MAC address 2
machineType	String	Storage-device machine type
mgmtProcIPaddress	String	Management IP address
model	String	Storage-device model
name	String	Name that is displayed in the user interface for this device The value of this attribute is determined by **preferredDisplayName** attribute in the GET /aicc method. For example, if the **preferredDisplayName** attribute is set to “hostname,” then the value for this **name** attribute is the same as the **hostname** attribute in the GET /aicc method.
otherMcStatus	String	(Storage devices only)

Attributes	Type	Description
overallHealthState	String	Highest severity of all alerts. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
parent	Object	Information about the parent of the storage device, if applicable
uri	String	Parent UUID
uuid	String	Parent URI
pfu	String	
productBrand	String	
productName	String	Product name
roboticFWRevision	String	(Tape library only) Robotic hardware revision
roboticHWRevision	String	(Tape library only) Robotic firmware revision
roboticSerialNumber	String	(Tape library only) Robotic serial number
scsiProductId	String	(Storage devices only)
scsiVendorId	String	(Storage devices only)
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
identityManagementSystemEnabled	Boolean	Indicates whether to use an identity-management system for authentication. This can be one of the following values. • **true**. An identity-management system is to authenticate this device. • **false**. An identity-management system is not used to authenticate this device. In this case, either manually entered credentials or stored credentials must be used. **Note:** Identity management systems can be used to authenticate only ThinkSystem and ThinkAgile servers.
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports the ability to choose managed authentication • **false**. This device does not support the ability to choose managed authentication.

Attributes	Type	Description
publicAccess	Boolean	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is accessible by all role group. • **false**. The resource is restricted to specific role groups.
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device
storedCredentials	Array of objects	Information about the stored credential that is associated with this device, if applicable.
id	String	ID of the stored credential
description	String	Description of the stored credential
userName	String	Name of the stored credential
uri	String	URI of the device
serialNumber	String	
slots	Array of integers	(Storage devices only)
storageNodeCapacityList	Array of objects	Information about storage capacity for each node
blockStorage	Object	Information about storage capacity
available	String	Amount of available (unused) capacity, in TiB
fullThresholdPercent	String	Full capacity threshold, as a percentage This can be a value from **0** – **100**.
size	String	Total amount of capacity, in TiB
used	String	Amount of used capacity, in TiB
nodeName	String	Node name
status	Array of strings	(Storage devices only)
message	String	
name	String	
subSlots	Array of strings	(Storage devices only)
subType	String	(Storage devices only)
supportedLocales	String	(Storage devices only)
systemLocation	String	(Storage devices only)
tlsVersion	Object	(Storage devices only) Information about the SSL or TLS protocol and version
currentValue	String	SSL or TLS protocol and version to be used. This can be one of the following values. • **unsupported** • **TLS_12**. TLS v1.2 • **TLS_13**. TLS v1.3

Attributes	Type	Description
possibleValues	Array of strings	List of possible values
type	String	Resource type. This can be one of the following values. • **LenovoStorage** • **TapeLibrary**
uri	String	URI
userDefinedName	String	User-defined name for the device
userDescription	String	(Storage devices only) User description
uuid	String	UUID
vendorName	String	
virtualPools	Integer	(Storage devices only)
vnicMode	String	(Storage devices only)
vpid	String	(Storage devices only)
wwnn	String	

The following example is returned if the request is successful for a storage device.


```
{
    "storageList": [{
        "accessState": Online",
        "canisterSlots": 2,
        "cmmHealthState": "Normal",
        "contact": "F",
        "description": "F",
        "diskGroups": 2,
        "driveBays": 12,
        "enclosureCount": 1,
        "enclosures": [{
            "canisters": [{
                "cmmDisplayName": "controller_a",
                "controllerId": "A",
                "controllerRedundancyMode": "Active-ActiveULP",
                "controllerRedundancyStatus": "Redundant",
                "disks": 9,
                "diskBusType": "SAS",
                "diskChannels": 2,
                "energyMetrics": {
                    "diskControllerTemperature": [],
                    "inletAirTemperature": [],
                    "memoryTemperature": []
                },
                "expansionPorts": [{
                    "health": "N/A",
                    "healthReason": "No drive enclosure is connected to this expansion port. This is normal if this
                                    is the last (or only) enclosure in the cabling sequence of the system.",
                    "healthRecommendation": "-Noactionisrequired.",
                    "name": "OutPort",
                    "status": "Disconnected"
                }],
                "failOverReason": "Notapplicable",
                "failedOverToThisController": "No",
```

```
"firmware": {
    "backplaneType": "7",
    "bundleVersion": "GL221R020-14",
    "buildDate": "ThuJun2909: 26: 26MDT2017",
    "capiVersion": "3.19",
    "cpldCodeVersion": "56",
    "diskInterfaceHardwareVersion": "3",
    "expanderControllerCodeVersion": "3206",
    "hardwareVersion": "5.2",
    "hostInterfaceHardwareVersion": "2",
   "hostInterfaceModuleModel": "6",
    "hostInterfaceModuleVersion": "11",
    "managementControllerCodeVersion": "GLM221R037-02",
   "managementControllerLoaderCodeVersion": "6.27.25440",
    "scBootMemoryReferenceCodeVersion": "1.2.1.10",
   "storageControllerCodeBaselevel": "GLS221R13-01",
    "storageControllerCodeVersion": "GLS221R13-01",
    "storageControllerCpuType": "Gladden1300MHz",
    "storageControllerLoaderCodeVersion": "27.016",
    "version": "5.6",
    "versionType": "nonencrypted"
},
"hardwareVersion": "5.2",
"health": "Normal",
"healthReason": "",
"healthRecommendation": "",
"hostPorts": 4,
"networkPorts": {
    "addressingMode": "Manual",
    "gateway": "10.243.0.1",
    "health": "OK",
   "healthReason": "",
    "healthRecommendation": "",
    "ipAddress": "10.243.9.148",
    "ipVersion": 4,
    "macAddress": "00: c0: ff: 28: 03: c7",
    "name": "mgmtport_a",
    "networkMask": "255.255.240.0"
},
"phyIsolation": "Enabled",
"ports": [{
    "action": "- If this host port is intentionally unused, no actionis required.\n
                - Otherwise, use an appropriate interface cable to connect this host
                  port to a switch o rhost.\n
                - If a cable is connected, check the cable and the switch or host for
                  problems.",
    "actualSpeed": "",
    "configSpeed": "Auto",
    "health": "N/A",
    "media": "FC(-)",
    "port": "A2",
    "reason": "There is no active connection to this host port.",
    "status": "Disconnected",
    "targetId": "227000c0ff280e8b",
    "topology": "PTP"
},
...,
{
    "action": "- If this host port is intentionally unused, no actionis required.\n
                - Otherwise, use an appropriate interface cable to connect this host
                  port to a switch o rhost.\n
```

```
                    - If a cable is connected, check the cable and the switch or host for
                      problems.",
          "actualSpeed": "",
          "configSpeed": "Auto",
          "health": "N/A",
          "media": "FC(-)",
          "port": "A3",
          "reason": "There is no active connection to this host port.",
          "status": "Disconnected",
          "targetId": "237000c0ff280e8b",
          "topology": "PTP"
      }]
      "position": "Top",
      "powerState": "On",
      "revision": "0",
      "serialNumber": "11S00WC050Y010DH677180",
      "status": "Operational",
      "systemCacheMemory": 6144,
  }],
  "drives": [{
      "firmwareVersion": null",
      "health": "OK",
      "healthReason": "",
      "healthRecommendation": "",
      "location": "0.9",
      "model": "ST2000NM0034X",
      "serialNumber": "Z4H02R730000R538RM68",
      "size": "2000.3TiB",
      "status": "Up",
      "type": "SASMDL",
      "vendorName": "LENOVO-X"
  },
  ...,
  {
      "firmwareVersion": null,
      "health": "OK",
      "healthReason": "",
      "healthRecommendation": "",
      "location": "0.4",
      "model": "ST2000NM0034X",
      "serialNumber": "Z4H07S8L0000R628K52C",
      "size": "2000.3TiB",
      "status": "Up",
      "type": "SASMDL",
     "vendorName": "LENOVO-X"
  }],
  "enclosureInfo": {
      "diskCount": 9,
      "driveBays": 12,
      "enclosureId": 0,
      "health": "OK",
      "model": "S3200",
      "midplaneSerialNumber": "11S00WC065Y010DH67C0RF",
      "status": "Up",
      "vendorName": "Lenovo",
      "wwn": "500C0FF0280E8B3C"
  },
  "energyMetrics": {
      "enclosurePower": []
  },
  "frus": [{
```

```
            "description": "SPSMemoryCard",
            "fruLocation": "LOWERIOMMEMORYCARDSLOT",
            "fruStatus": "OK",
            "partNumber": "40-00000053",
            "serialNumber": "",
            "shortName": "MemoryCard"
        },
        ...,
        {
            "description": "48X44xCNCRIOM-LX6GBLENOVO",
            "fruLocation": "LOWERIOMSLOT",
            "fruStatus": "OK",
           "partNumber": "00WC050",
            "serialNumber": "11S00WC050Y010DH677182",
            "shortName": "RAIDIOM"
      }],
        "location": {
            "lowestRackUnit": 0,
            "location": "",
            "rack": "",
            "room": ""
        },
        "powerSupplies": [{
            "health": "OK",
            "healthReason": "",
            "healthRecommendation": "",
            "model": "00WC067",
            "position": "Right",
            "status": "Up",
            "vendorName": ""
        },
        {
            "health": "OK",
            "healthReason": "",
            "healthRecommendation": "",
            "model": "00WC067",
            "position": "Left",
            "status": "Up",
            "vendorName": ""
        }],
        "slots": ["0", "1", "2", "4", "5", "6", "8", "9", "10"]
}],
"excludedHealthState": "Normal",
"healthReason": "",
"ipv4Addresses": ["10.243.9.148", "10.243.9.149"],
"isConnectionTrusted": "true",
"location": {
    "location": "",
    "lowestRackUnit": 0,
    "rack": "",
    "room": ""
    },
"machineType": "6411",
"mgmtProcIPaddress": "192.0.2.0",
"model": "S3200",
"name": "S3200",
"otherMcStatus": "Operational",
"overallHealthState": "Normal",
"parent": {
    "uri": "",
    "uuid": ""
```

```
        },
        "pfu": "Idle",
        "productBrand": "Storage",
        "productName": "S3200",
        "scsiProductId": "S3200",
        "scsiVendorId": "Lenovo",
        "securityDescriptor": {
            "managedAuthEnabled": true
            "managedAuthSupported": true,
            "publicAccess": true,
            "roleGroups": ["lxc-admin","lxc-security-admin"],
            "storedCredentials": null,
            "uri": "storage/0069030ADC5F453E9EE49CA4B44DB8DC"
        },
        "serialNumber": "280E8B",
        "storageNodeCapacityList": [{
            "blockStorage": {
                "available": "6.66 TiB",
                "fullThresholdPercent": "96",
                "size": "6.83 TiB",
                "used": "168 GiB"
            },
            "nodeName": "PerfDM7100F-02"
        }, {
            "blockStorage": {
                "available": "6.66 TiB",
                "fullThresholdPercent": "96",
                "size": "6.83 TiB",
                "used": "168 GiB"
            },
            "nodeName": "PerfDM7100F-01"
        }],
        "supportedLocales": "English(English), Arabic(العربية), Portuguese(português), Spanish(español),
                             French(français), German(Deutsch), Italian(italiano), Japanese(日本語),
                             Korean(한국어), Dutch(Nederlands), Russian(русский),
                             Chinese-Simplified(简体中文), Chinese-Traditional(繁體中文)",
        "systemLocation": "LXCA_empty_field, LXCA_empty_field, LXCA_empty_field",
        "type": "LenovoStorage",
        "userDefinedName": "Storage1",
        "userDescription": "F",
        "uri": "storage/208000C0FF280E8B",
        "uuid": "208000C0FF280E8B",
        "vendorName": "Lenovo",
        "virtualPools": 2,
        "wwnn": "208000C0FF280E8B",
    }]
}
```


The following example is returned if the request is successful for a tape library.


```
{
        "accessState": "OFFLINE",
        "baseFWBuildDate": "08-23-2019",
        "baseFWRevision": "1.3.0.1-A00",
        "canisterSlots": 0,
        "cmmHealthState": "Normal",
        "driveBays": 0,
        "enclosureCount": 1,
        "enclosures": [{
            "drawers": [],
            "drives": [],
            "enclosureInfo": {
```

```
    "diskCount": null,
    "driveBays": null,
    "enclosureId": 1,
    "generatedUUID": null,
    "health": "OK",
    "height": 3,
    "midplaneSerialNumber": "6741L1U78003LH",
    "model": "TS4300",
    "physicalNumber": 4,
    "status": "Optimal",
    "vendorName": "IBM",
    "wwn": "5000E1116763A000"
},
"energyMetrics": {
    "enclosurePower": []
},
"frus": [],
"location": null,
"powerSupplies": [],
"slots": [],
"tapeDrives": [{
    "adtmode": "IADT",
    "barcode": "440AACL8",
    "cartridge": "TRUE",
    "errorState": "FALSE",
    "fwrevision": "KAH0",
    "generation": "8",
    "interface": "FC",
    "logicalNumber": "1",
    "mfgserialNumber": "10WT000635",
    "module": "1",
    "partition": "1",
    "physicalNumber": "10",
    "power": "TRUE",
    "presence": "TRUE",
    "product": "ULT3580-TD8",
    "serialNumber": "116763A05B",
    "vendor": "IBM",
    "wwnodeName": "5000E1116763A05B"
},
{
    "adtmode": "IADT",
    "cartridge": "FALSE",
    "errorState": "FALSE",
    "fwrevision": "KAH1",
    "generation": "8",
    "interface": "SAS",
    "logicalNumber": "2",
    "mfgserialNumber": "10WT001111",
    "module": "1",
    "partition": "1",
    "physicalNumber": "12",
    "power": "TRUE",
    "presence": "TRUE",
    "product": "ULT3580-HH8",
    "serialNumber": "116763A06F",
    "vendor": "IBM",
    "wwnodeName": "5000E1116763A06F"
}],
"tapePartitions": [{
    "autoClean": "TRUE",
```

```
"barcodeAlign": "left",
"barcodeLength": "8",
"encryptionMode": "ISV",
"lunMasterDrive": "1",
"lunMasterDriveArr": ["1","2"],
"lunMasterDrivePhys": "10",
"lunMasterDrivePhysArr": ["12","10"],
"micw": "FALSE",
"name": "LogicalLib",
"numDrives": "2",
"numIOSlots": "4",
"numSlots": "28",
"partitionInventory": {
    "tapeDrives": [{
        "fwrevision": "KAH1",
        "logicalNumber": "2",
        "module": "1",
        "partition": "1",
        "physicalNumber": "12",
        "product": "ULT3580-HH8         ",
        "serialNumber": "10WT001111",
        "vendor": "IBM         "
    },
    {
        "barcode": "440AACL8",
        "fwrevision": "KAH0",
        "logicalNumber": "1",
        "module": "1",
        "partition": "1",
        "physicalNumber": "10",
        "product": "ULT3580-TD8         ",
        "serialNumber": "10WT000635",
        "vendor": "IBM         "
    }],
    "tapeSlots": [{
        "access": "TRUE",
        "blocked": "FALSE",
        "cartridge": "FALSE",
        "cartridgeEncrypted": "Unknown",
        "cartridgeType": "N/A",
        "logicalNumber": "1.23",
        "mailslot": "FALSE",
        "module": "1",
        "partition": "1",
        "physicalNumber": "143"
    },
    ...,
    {
        "access": "TRUE",
        "blocked": "FALSE",
        "cartridge": "FALSE",
        "cartridgeEncrypted": "Unknown",
        "cartridgeType": "N/A",
        "logicalNumber": "1.37",
        "mailslot": "TRUE",
        "module": "1",
        "partition": "1",
        "physicalNumber": "157"
    }]
},
"partitionNumber": "1",
```

```
            "serialNumber": "41L1U78003LH_LL01",
            "wwnode": "5000E1116763A05E"
        }],
        "tapeSlots": [{
            "access": "TRUE",
            "blocked": "TRUE",
            "cartridge": "FALSE",
            "cartridgeEncrypted": "Unknown",
            "cartridgeType": "N/A",
            "logicalNumber": "1.1",
            "mailslot": "FALSE",
            "module": "1",
            "partition": "0",
            "physicalNumber": "121"
        },
        ...,
        {
            "access": "TRUE",
            "blocked": "FALSE",
            "cartridge": "FALSE",
            "cartridgeEncrypted": "Unknown",
            "cartridgeType": "N/A",
            "logicalNumber": "1.37",
            "mailslot": "TRUE",
            "module": "1",
            "partition": "1",
            "physicalNumber": "157"
        }]
    }],
    "excludedHealthState": "Normal",
    "expansionFWRevision": "0.30",
    "ipv4Addresses": ["10.241.73.170"],
    "isConnectionTrusted": "true",
    "lastOfflineTimestamp": 1636545369437,
    "libHealth": "OK",
    "libraryType": "32",
    "macAddress_1": "00:0e:11:16:76:3a",
    "macAddress_2": "00:0e:11:16:76:3b",
    "machineType": "6741",
    "mgmtProcIPaddress": "10.241.73.170",
    "model": "TS4300",
    "name": "5000E1116763A000",
    "overallHealthState": "Normal",
    "parent": {
        "uri": "storage/5000E1116763A000",
        "uuid": "5000E1116763A000"
    },
    "productBrand": "IBM TS4300 Tape Library for Lenovo",
    "productName": "IBM TS4300 Tape Library for Lenovo",
    "roboticFWRevision": "0.13",
    "roboticHWRevision": "4",
    "roboticSerialNumber": "564EA002594",
    "securityDescriptor": {
        "identityManagementSystemEnabled": false,
        "managedAuthEnabled": false,
        "managedAuthSupported": true,
        "publicAccess": false,
        "roleGroups": [],
        "storedCredentials": {
            "id": "12002",
            "description": "Neptune Credentials for: 5000E1116763A000",
```

```
            "userName": "administrator"
        },
        "uri": "storage/5000e1116763a000"
    },
    "serialNumber": "6741L1U78003LH",
    "type": "TapeLibrary",
    "uri": "storage/5000E1116763A000",
    "userDefinedName": "5000E1116763A000",
    "uuid": "5000E1116763A000",
    "vendorName": "IBM",
    "wwnn": "5000E1116763A000"
}
```


PUT /storage/*{uuid}*

Use this method to modify properties or perform management actions on a specific storage devices.

The request body differs depending on the action that you want to perform. You can use this PUT method to perform the following management actions.

- Table 35 “Modify storage properties” on page 436
- Table 36 “Collect and export service data” on page 436
- Table 37 “Configure device authentication” on page 436

Note: To power on or off canisters in the storage device, use PUT /storage/*{uuid}*/*{controller}*

If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/storage/{uuid}`

where *{uuid}* is the UUID of the storage device to be retrieved. To obtain the node UUID, use the GET /storage method.

Query parameters

Attributes	Required / Optional	Description
synchronous=*{value}*	Optional	When modifying attributes, indicates when the job ID is returned • **true**. (default) Returns the job ID and job status after the job is complete. • **false**. Returns the job ID immediately. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. **Note:** This query parameter applies only when one or more property parameters are specified in the request body.

Request body

Table 35. Modify storage properties

Attributes	Required / Optional	Type	Description
contact	Optional	String	The contact information
name	Optional	String	Storage-device name
userDescription	Optional	String	The storage-device description

The following example modifies the hostname, location, and contact information for the target storage device:

```
{
   "contact":"new contact",
   "name":"new name",
   "userDescription":"new userDescription"
}
```

Table 36. Collect and export service data

Attributes	Required / Optional	Type	Description
sftpURI	Required	String	Collects and exports service data to the specified Secure FTP site.

The following example collects and exports an FFDC archive to `sftp://SYSMGR:JhdJshf922nms@10.241.53.50`.

```
{
   "sftpURI":"sftp://SYSMGR:JhdJshf922nms@10.241.53.50"
}
```

Table 37. Configure device authentication and access control

Note: Only users with **lxc-supervisor** or **lxc-security-admin** authority can modify the access-control settings.

Attributes	Required / Optional	Type	Description
securityDescriptor	Required	Object	Information about the authentication enablement and support the associated stored credentials for a managed device.
managedAuthEnabled	Optional	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication
publicAccess	Optional	Boolean	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
roleGroups	Optional	Array of strings	List of role groups that are permitted to view and manage this device.

Table 37. Configure device authentication and access control (continued)

Attributes	Required / Optional	Type	Description
storedCredentials	Required if **managedAuthEnabled** is set to `true`	Object	Information about the stored credential that is associated with this device, if applicable.
id	Required if **managedAuthEnabled** is set to `true`	String	ID of the stored credential to associated with the device

The following example restricts access to the managed device to members of the specified role groups:

```
{
   "securityDescriptor" : {
      "publicAccess": false,
      "roleGroups": ["sales-os-admin","corp_fw_admin"]
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/storage/*{uuid}*/*{controller}*

Use this REST API to modify properties or perform management actions on a specific storage device.

HTTP methods

PUT

PUT /storage/*{uuid}*/*{controller}*

Use this method to power on or off a specific storage controller.

This method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://`*{management_server_IP}*`/storage/`*{uuid}*`/`*{controller}*

where:

- *{uuid}* is the UUID of the storage device to be retrieved. To obtain the node UUID, use the GET /storage method.
- *{controller}* is `A` for the top controller or `B` for the bottom controller.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
powerState	Required	String	Performs a power operation on the device. This can be one of the following values: • **powerOn**. Powers on the storage. • **powerOff**. Powers off the storage device immediately. • **powerCycleSoft**. Restarts the storage device immediately. If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

The following example restarts the target storage device:

```
{
   "powerState": "powerCycleSoft"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/switches

Use this REST API to retrieve properties for all Flex and RackSwitch switches.

HTTP methods

GET, POST

GET /switches

Use this method to return the properties for all Flex and RackSwitch switches.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/switches`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
formatType=*{type}*	Optional	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv** If the format type is not specified, JSON format is returned. **Note:** To retrieve properties for a large number of devices, use POST /switches.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

The following example returns a CSV file that contains information about all switches.

```
GET https://192.0.2.0/switches?formatType=csv
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
switchList	Array	List of switches
See GET /switches/*{uuid_list}*	Object	Detailed information about each switch

The following example is returned if the request is successful when the **formatType=json** query parameter is specified.


```
{
"switchList": [{
   "switchList": [{
   "accessState": "Online",
   "accessStateRecords": [{
       "health": "SUCESS",
       "ipAddress": "10.243.6.68",
       "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
       "messageDisplay": "Connection is successful",
       "messageID": "1180_SHORT",
       "messageParameters": [],
       "protocol": "CIM",
       "timestamp": 1565785907453,
       "username": "USERID"
   },
   {
       "health": "SUCESS",
       "ipAddress": "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:163d",
       "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
       "messageDisplay": "Connection is successful",
       "messageID": "1180_SHORT",
       "messageParameters": [],
       "protocol": "CIM",
       "timestamp": 1565785907465,
       "username": "USERID"
   }],
   "applyPending": "No",
   "backedBy": "real",
   "badCredentials": false,
   "cmmDisplayName": "NE1072T",
   "cmmHealthState": "Critical",
   "contact": "John Smith",
   "cpuUtilization": "N/A",
   "dataHandle": 1559245736963,
   "description": "48*10 GbE(RJ-45), 6*40 GbE QSFP+",
   "dnsHostnames": [],
   "domainName": "",
   "elapsedTimeMillisecs": "291128",
   "entitleSerialNumber": "MM28753",
   "errorFields": [],
   "excludedHealthState": "Critical",
   "expiredCredentials": false,
   "fans": [{
       "fanName": "Fan 1",
       "fanSpeed": "1782 RPM (23 PWM)",
       "fanState": "Front-to-Back"
   },
   ...],
   "firmware": [{
       "build": "",
       "classifications": [],
```

```
    "date": "",
    "name": "Uboot",
    "role": "",
    "status": "N/A",
    "type": "Boot ROM",
    "version": "10.9.3.0"
},
...],
"FRU": "00YK768         ",
"fruSerialNumber": "",
"globalVlagState": "Disabled",
"height": 1,
"hostname": "NE1072T",
"httpsEnabled": true,
"ipInterfaces": [{
    "IPv4assignments": [{
        "id": 0,
        "subnet": "255.255.252.0",
        "gateway": "0.0.0.0",
        "address": "10.240.196.83",
        "type": "UNKNOWN"
    }],
    "IPv4DHCPmode": "UNKNOWN",
    "IPv4enabled": true,
    "IPv6assignments": [{
        "id": 0,
        "scope": "Global",
        "gateway": "0:0:0:0:0:0:0:0",
        "source": "Static",
        "address": "fe80:0:0:0:a68c:dbff:fe96:dd00",
        "prefix": 10,
        "type": "UNKNOWN"
    }],
    "IPv6DHCPenabled": false,
    "IPv6enabled": true,
    "IPv6statelessEnabled": false,
    "IPv6staticEnabled": false,
    "label": "unknown",
    "name": "mgmt0"
}...
],
"ipv4Addresses": ["10.240.196.83"],
"ipv6Addresses": ["fe80::200:ff:fe00:0","fe80::a68c:dbff:fe96:dd00"],
"isConnectionTrusted": "true",
"leds": [],
"location": {
    "location": "Santa Clara",
    "lowestRackUnit": 5,
    "rack": "Core 1",
    "room": "Core lab"
},
"macAddresses": ["A4:8C:DB:96:DD:00"],
"machineType": "7159",
"manufacturer": "LNVO",
"manufacturerId": "",
"manufacturingDate": "3117 (WWYY)",
"memoryUtilization": "",
"mgmtProcIPaddress": "10.240.196.83",
"model": "HD6",
"name": "NE1072T",
"ntpPushEnabled": false,
```

```
"ntpPushFrequency": 0,
"operationalVlagState": "Disabled",
"OS": "CNOS"
"overallHealthState": "Critical",
"panicDump": "No",
"parent": {
    "uri": null,
    "uuid": null
},
"partNumber": "00YL919        ",
"portDataSetTimestamp": "03:48:56",
"ports": [{
    "configuredStatus": "up",
    "interfaceIndex": "410001",
    "operationalStatus": "down",
    "mtu": 1500,
    "peerMacAddress": "",
    "portName": "",
    "portSpeed": "auto",
    "portState": "down",
    "tagPVID": "",
    "vLAN": "untagged",
    "port": "Ethernet1/1",
    "PVID": "1"
},
...],
"posID": "",
"powerState": "On",
"powerSupply": "Power Supply 1: Off;Power Supply 2: On.",
"productId": "",
"productName": "Lenovo ThinkSystem NE1072T RackSwitch",
"protectedMode": "Unknown",
"resetReason": "1",
"savePending": "No",
"securityDescriptor": {
    "managedAuthEnabled": false,
    "managedAuthSupported": false,
    "publicAccess": false,
    "roleGroups": ["WIRELESS"],
    "storedCredentials": [{
        "description": "",
        "id": "2417",
        "userName": "admin"
    }],
    "uri": "switches/0000000000010008000a48cdb96dd00"
},
"serialNumber": "Y055DH77R016",
"stackMode": "none",
"stackRole": "none",
"sysObjectID": "1.3.6.1.4.1.19046.1.7.34",
"temperatureSensors": [{
    "sensorName": "Inlet Temp",
    "sensorState": "38 °C"
},
...],
"type": "Rackswitch",
"upTime": "46 days, 06:37:12",
"userDescription": "",
"userDefinedName": "NE1072T",
"uri": "switches/0000000000010008000A48CDB96DD00",
"uuid": "0000000000010008000A48CDB96DD00",
```

```
    "vpdID": ""
}]
}
```

POST /switches

Use this method to return the properties for a large number of specific Flex and RackSwitch switches.

Note: If you choose **formatType=csv**, this request creates a file in CSV format and returns the filename in the request header. You can use to download the file using GET /switches/*{file_name}*.csv.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/switches
```

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
formatType	Optional	String	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv**
uuids	Required	String	List of device UUIDs, separated by a comma

Request example

```
{
   "formatType": "csv",
   "uuids": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

If **formatType=csv** is specified, the response header includes the URI of the downloaded file. If data for a single switch is requested, the file name includes the switch UUID. If multiple switches are requested, the file name is `allSwitches_{unique_ID}.csv`. For example:

```
Status Code: 201 Created
Location: /chassis/EF6D424FAACA4E539771B812AAEE0F73.csv
```

Response body

If the **formatType=csv** request attribute is specified, no response body is returned.

If the **formatType=json** request attribute is specified, the following JSON object is returned.

Attributes	Type	Description
switchList	Array	List of switches
See GET /switches/*{uuid_list}*	Object	Detailed information about each switch.

The following example is returned if the request is successful when the **formatType=json** query parameter is specified.


```
{
"switchList": [{
    "switchList": [{
    "accessState": "Online",
    "accessStateRecords": [{
        "health": "SUCESS",
        "ipAddress": "10.243.6.68",
        "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
        "messageDisplay": "Connection is successful",
        "messageID": "1180_SHORT",
        "messageParameters": [],
        "protocol": "CIM",
        "timestamp": 1565785907453,
        "username": "USERID"
    },
    {
        "health": "SUCESS",
        "ipAddress": "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:163d",
        "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
        "messageDisplay": "Connection is successful",
        "messageID": "1180_SHORT",
        "messageParameters": [],
        "protocol": "CIM",
        "timestamp": 1565785907465,
        "username": "USERID"
    }],
    "applyPending": "No",
    "backedBy": "real",
    "badCredentials": false,
    "cmmDisplayName": "NE1072T",
    "cmmHealthState": "Critical",
    "contact": "John Smith",
    "cpuUtilization": "N/A",
    "dataHandle": 1559245736963,
    "description": "48*10 GbE(RJ-45), 6*40 GbE QSFP+",
    "dnsHostnames": [],
    "domainName": "",
```

```
"elapsedTimeMillisecs": "291128",
"entitleSerialNumber": "MM28753",
"errorFields": [],
"excludedHealthState": "Critical",
"expiredCredentials": false,
"fans": [{
    "fanName": "Fan 1",
    "fanSpeed": "1782 RPM (23 PWM)",
    "fanState": "Front-to-Back"
},
...],
"firmware": [{
    "build": "",
    "classifications": [],
    "date": "",
    "name": "Uboot",
    "role": "",
    "status": "N/A",
    "type": "Boot ROM",
    "version": "10.9.3.0"
},
...],
"FRU": "00YK768         ",
"fruSerialNumber": "",
"globalVlagState": "Disabled",
"height": 1,
"hostname": "NE1072T",
"httpsEnabled": true,
"ipInterfaces": [{
    "IPv4assignments": [{
        "id": 0,
        "subnet": "255.255.252.0",
        "gateway": "0.0.0.0",
        "address": "10.240.196.83",
        "type": "UNKNOWN"
    }],
    "IPv4DHCPmode": "UNKNOWN",
    "IPv4enabled": true,
    "IPv6assignments": [{
        "id": 0,
        "scope": "Global",
        "gateway": "0:0:0:0:0:0:0:0",
        "source": "Static",
        "address": "fe80:0:0:0:a68c:dbff:fe96:dd00",
        "prefix": 10,
        "type": "UNKNOWN"
    }],
    "IPv6DHCPenabled": false,
    "IPv6enabled": true,
    "IPv6statelessEnabled": false,
    "IPv6staticEnabled": false,
    "label": "unknown",
    "name": "mgmt0"
}...
],
"ipv4Addresses": ["10.240.196.83"],
"ipv6Addresses": ["fe80::200:ff:fe00:0","fe80::a68c:dbff:fe96:dd00"],
"isConnectionTrusted": "true",
"leds": [],
"location": {
    "location": "Santa Clara",
```

```
    "lowestRackUnit": 5,
    "rack": "Core 1",
    "room": "Core lab"
},
"macAddresses": ["A4:8C:DB:96:DD:00"],
"machineType": "7159",
"manufacturer": "LNVO",
"manufacturerId": "",
"manufacturingDate": "3117 (WWYY)",
"memoryUtilization": "",
"mgmtProcIPaddress": "10.240.196.83",
"model": "HD6",
"name": "NE1072T",
"ntpPushEnabled": false,
"ntpPushFrequency": 0,
"operationalVlagState": "Disabled",
"OS": "CNOS"
"overallHealthState": "Critical",
"panicDump": "No",
"parent": {
    "uri": null,
    "uuid": null
},
"partNumber": "00YL919        ",
"portDataSetTimestamp": "03:48:56",
"ports": [{
    "configuredStatus": "up",
    "interfaceIndex": "410001",
    "operationalStatus": "down",
    "mtu": 1500,
    "peerMacAddress": "",
    "portName": "",
    "portSpeed": "auto",
    "portState": "down",
    "tagPVID": "",
    "vLAN": "untagged",
    "port": "Ethernet1/1",
    "PVID": "1"
},
...],
"posID": "",
"powerState": "On",
"powerSupply": "Power Supply 1: Off;Power Supply 2: On.",
"productId": "",
"productName": "Lenovo ThinkSystem NE1072T RackSwitch",
"protectedMode": "Unknown",
"resetReason": "1",
"savePending": "No",
"securityDescriptor": {
    "managedAuthEnabled": false,
    "managedAuthSupported": false,
    "publicAccess": false,
    "roleGroups": ["WIRELESS"],
    "storedCredentials": [{
        "description": "",
        "id": "2417",
        "userName": "admin"
    }],
    "uri": "switches/00000000000010008000a48cdb96dd00"
},
"serialNumber": "Y055DH77R016",
```

```
    "stackMode": "none",
    "stackRole": "none",
    "sysObjectID": "1.3.6.1.4.1.19046.1.7.34",
    "temperatureSensors": [{
        "sensorName": "Inlet Temp",
        "sensorState": "38 °C"
    },
    ...],
    "type": "Rackswitch",
    "upTime": "46 days, 06:37:12",
    "userDescription": "",
    "userDefinedName": "NE1072T",
    "uri": "switches/00000000000010008000A48CDB96DD00",
    "uuid": "00000000000010008000A48CDB96DD00",
    "vpdID": ""
}]
}
```


/switches/*{file_name}*.csv

Use this REST API to download inventory for a large number of specific Flex and RackSwitch switches in CSV format to the local system.

HTTP methods

GET

GET /switches/*{file_name}*.csv

Use this method to download inventory for a large number of specific Flex and RackSwitch switches in CSV format to the local system.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/switches/{file_name}.csv`

where *{file_name}*.csv is the file name of the CSV file that contains inventory data. Use the POST /switches method to with the **formatType=csv** request parameter to create the CSV file. The POST /switches method returns the file name in the request header.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/switches/*{uuid}*

Use this REST API to retrieve and modify properties for a specific Flex and RackSwitch switch and or to perform a power operation on a specific switch. This REST API is available only for Lenovo XClarity Administrator v1.0.1 and later.

HTTP methods

GET, PUT

GET /switches/*{uuid_list}*

Use this method to return properties for one or more specific Flex and RackSwitch switches. This REST API is available only for Lenovo XClarity Administrator v1.0.1 and later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/switches/{uuid_list}`

where *{uuid_list}* is a list of one or more UUIDs, separated by a comma, of the switches to be retrieved. To obtain the switch UUIDs, use the GET /switches method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
formatType=*{type}*	Optional	Returns information in the specified format. This can be one of the following values. • **json** (default) • **csv** If the format type is not specified, JSON format is returned. **Note:** To retrieve properties for a large number of devices, use POST /switches.
includeAttributes=*<attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

The following example returns a CSV file that contains information about two specific switches.

```
GET https://192.0.2.0/switches/0E7D8E1CDF7D11D4ABB0D5D5D5313131,
409583E0BD27B7019F3758946B036818?formatType=csv
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
413	Request Entity Too Large	Clients might impose limitations on the length of the request URI, and the request URI is too long to be handled. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
accessState	String	State of the switch. This can be one of the following values. • **Online** • **Offline** • **Partial** • **Pending** • **Unknown**
accessStateRecords	Array of objects	Information about the access-state record for each network interface and protocol that is available for the device **Note:** This attribute is present only for devices that are offline due to connectivity issues.
health	String	Connection health state of the device. This can be one of the following values. • **OFFLINE** • **PARTIAL** • **FAIL**
ipAddress	String	IP address that was used to check the network connectivity
isTrusted	Boolean	Indicates whether the connection to the device is trusted. This can be one of the following values. • **true**. The connection is trusted. • **false**. The connection is not trusted.
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle
messageDisplay	String	Translated label that corresponds to the message ID or to the pre-translated backup string if no message ID is specified
messageID	String	Message ID for the translatable connection error states
messageParameters	Array of strings	Attributes for the message if the translated message requires input. A JSON object that points to translated messages.
protocol	String	Type of the protocol to check connectivity. This can be one of the following values. • **CIM** • **CLI** • **DCS** • **REDFISH**
timestamp	Long	Timestamp when connectivity was last checked and when this record was created
username	String	User name that was used to check connectivity
applyPending	Integer	Indicates whether an apply action is needed and that the configuration has been changed by the user actions.
attachedNodes	Array	List of nodes with one or more ports attached to the switch.
badCredentials	Boolean	Indicates whether stored credentials are valid to login. This can be one of the following values. • **true**. Stored credentials are not valid for login. • **false**. Stored credentials are valid for login.
cmmDisplayName	String	Switch name provided by the CMM

Attributes	Type	Description
cmmHealthState	String	Health summary that corresponds to the highest event severity of all the devices. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
contact	String	Contact name for the switch
cpuUtilization	Long	Processor usage for the switch.
dataHandle	Long	Time stamp of the last status update
description	String	Description provided by the CMM
dnsHostnames	Array of strings	List of DNS hostnames
domainName	String	User defined domain name
elapsedTimeMillisecs	String	Elapsed time, in milliseconds
entitleSerialNumber	String	Wwitch serial number
errorFields	Array of objects that contain {*String*, *Error Code*}	Error codes. This can be one of the following values. • **FETCH_SUCCESS** • **FETCH_FAILED** • **NO_CONNECTOR** • **FATAL_EXCEPTION** • **NETWORK_FAIL**
excludedHealthState	String	Highest severity alert with exclusions. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
expiredCredentials	Boolean	Indicates whether stored credentials are accepted by the switch but not authorized for login. This can be one of the following values. • **true**. Stored credentials are accepted by the switch but not authorized for login. • **false**. Stored credentials are accepted by the switch and authorized for login.
fans	Array	Information about each fan in the switch
fanName	String	Fan name
fanSpeed	String	Fan speed
fanState	String	Fan status
firmware	Array	Firmware details

Attributes	Type	Description
build	String	Firmware build
date	String	Firmware date
name	String	Firmware name
status	String	Firmware status
role	String	
type	String	Firmware type
version	String	Firmware version
FRU	String	FRU part number
fruSerialNumber	String	FRU serial number
globalVlagState	String	Configured state of VLAG. This can be one of the following values. • **Enabled** • **Disabled** • **N/A**
hostname	String	User defined hostname
httpsEnabled	Boolean	(Rack switches running ENOS only) Indicates whether to enable HTTPS on the switch. This can be one of the following values. • **true**. HTTPS is enabled. • **false**. HTTPS is not enabled.
ipInterfaces	Array	Information about the switch IP addresses
IPv4assignments	Array	Information about IPv4 assignments
address	String	IPv4 address
gateway	String	IPv4 gateway
id	Integer	IPv4 assignment ID
subnet	String	Subnet mask
type	String	Type of IPv4 assignment. This can be one of the following values. • **INUSE** • **CONFIGURED** • **ALIAS** • **UNKNOWN**
IPv4DHCPmode	String	IP address assignment method. This can be one of the following values. • **STATIC_ONLY** • **DHCP_ONLY** • **DHCP_THEN_STATIC** • **UNKNOWN**
IPv4enabled	Boolean	Identifies whether IPv4 is enabled. This can be one of the following values. • **true**. IPv4 is enabled. • **false**. IPv4 is disabled.
IPv6assignments	Array	Information about IPv6 assignments
address	String	IPv6 address
gateway	String	IPv6 gateway

Attributes	Type	Description
id	Integer	IPv6 assignment ID
prefix	Integer	IPv6 prefix
scope	String	Scope of the IPv6 assignment. This can be one of the following values. • **Global** • **LinkLocal** • **Unknown**
source	String	Source of the IPv6 assignment. This can be one of the following values. • **DHCP** • **Statelesss** • **Static** • **Other** • **Unknown**
type	String	Type of IPv6 assignment. This can be one of the following values. • **INUSE** • **CONFIGURED** • **ALIAS** • **UNKNOWN**
IPv6DHCPenabled	Boolean	Identifies whether IPv6 DHCP is enabled. This can be one of the following values. • **true**. IPv6 DHCP is enabled. • **false**. IPv6 DHCP is disabled.
IPv6enabled	Boolean	Identifies whether IPv6 is enabled. This can be one of the following values. • **true**. IPv6 is enabled • **false**. IPv6 is disabled
IPv6statelessEnabled	Boolean	Identifies whether IPv6 stateless is enabled. This can be one of the following values. • **true**. IPv6 stateless is enabled. • **false**. IPv6 stateless is disabled.
IPv6staticEnabled	Boolean	Identifies whether IPv6 static is enabled. This can be one of the following values. • **true**. IPv6 static is enabled. • **false**. IPv6 static is disabled.
label	String	Label
name	String	Name
ipv4Addresses	Array of strings	List of IPv4 addresses
ipv6Addresses	Array of strings	List of IPv6 addresses
leds	Array	Information about switch LEDs.
color	String	LED color. This can be one of the following values. • **Red** • **Amber** • **Yellow** • **Green** • **Blue** • **Unknown**

Attributes	Type	Description
location	String	LED location. This can be one of the following values. • **Front panel** • **Lightpath Card** • **Planar** • **FRU** • **Rear Panel** • **Unknown**
name	String	LED name.
state	String	LED state. This can be one of the following values. • **Off** • **On** • **Blinking** • **Unknown**
location	Array of objects	Information about the switch location
location	String	Location description
lowestRackUnit	Integer	Lowest unit that is occupied by the device in the rack
rack	String	Rack
room	String	Room
macAddresses	Array of strings	List of MAC addresses
machineType	String	Machine type
manufacturer	String	Manufacturer
manufacturerID	String	Manufacturer ID
manufacturingDate	String	Manufacturing date
memoryUtilization	String	Amount of used and free memory
mgmtProcIPaddress	String	IP address that is used by XClarity Administrator to manage this resource
model	String	Switch model
name	String	Name that is displayed in the user interface for this device The value of this attribute is determined by **preferredDisplayName** attribute in the GET /aicc method. For example, if the **preferredDisplayName** attribute is set to “hostname,” then the value for this **name** attribute is the same as the **hostname** attribute in the GET /aicc method.
NTPPushEnabled	Boolean	Indicates whether pushing NTP settings to the CMM is enabled. This can be one of the following values. • **true**. Push is enabled. • **false**. Push is disabled.
NTPPushFrequency	Integer	Frequency for pushing NTP settings to the CMM. This can be a number from `0 – 44640`.
operationalVlagState	String	Operational state of VLAG. This can be one of the following values. • **Enabled** • **Disabled** • **N/A**

Attributes	Type	Description
OS	String	(Rack switches only) Firmware type. This can be one of the following values. • **CNOS** • **ENOS**
overallHealthState	String	Highest severity of all alerts. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
parent	Object	(Flex switches only) Information about the chassis in which the switch resides
uri	String	URI of the chassis (for example, chassis/3A8B7173-0D66-4FA1-93B4-9213A74DE9F5)
uuid	String	UUID of the chassis (for example, 3A8B7173-0D66-4FA1-93B4-9213A74DE9F5)
partNumber	String	Part number for the switch
portDataSetTimestamp	String	
panicDump	String	Presence of a panic dump in the flash memory. This can be one of the following values. • **Yes**. A panic dump is in the flash memory. • **No**. A panic dump is not in the flash memory.
ports	Array of objects	Information about fan ports
configuredStatus	String	Configuration of the port. This can be one of the following values. • **enabled**. The port is enabled. • **disabled**. The port is disabled.
interfaceIndex	String	
mtu	Integer	Maximum transmission unit for the port
operationalStatus	String	Rreal-time status of the port. This can be one of the following values. • **up** • **down** • **notPresent**. The cable is unplugged
peerMacAddress	String	Port MAC address
port	String	Port index
portName	String	Port name
portSpeed	String	Port speed
portState	String	Current operational link status of the port. This can be one of the following values. • **up** • **down**
PVID	Integer	Default VLAN ID for the port

Attributes	Type	Description
tagPVID	String	PVID tag state of the port. This can be one of the following values. • **tagged** • **untagged**
vLAN	String	VLAN tag state of the port. This can be one of the following values. • **tagged**. VLAN tagging is enabled. • **untagged**. VLAN tagging is diaabled.
posID	String	Position ID
powerState	String	Current power state of the switch. This can be one of the following values. • **Off** • **On** • **ShuttingDown** • **Standby** • **Hibernate** • **Unknown**
powerSupply	String	Information about the state of each power supply, separated by a colon and ending with a period (for example, `Power Supply 1: Off;Power Supply 2: on.`)
productID	String	Product ID
productName	String	Model of the switch
protectedMode	Boolean	Identifies whether the switch is in protected mode. This can be one of the following values. • **true**. The switch is in protected mode • **false**. The switch is not in protected mode
resetReason	String	Reason for the switch reset.
savePending	String	Indicates whether an save action is needed and that the configuration has been applied but not saved to the flash. • **yes**. The save action is needed. • **no**. The save action is not needed.
securityDescriptor	Object	Information about the authentication enablement and support the associated stored credentials for a managed device.
managedAuthEnabled	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication.
managedAuthSupported	Boolean	Indicates whether the device supports the ability to choose whether managed authentication is to be used. This can be one of the following values. • **true**. This device supports the ability to choose managed authentication. • **false**. This device does not support the ability to choose managed authentication.
publicAccess	Boolean	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
roleGroups	Array of strings	List of role groups that are permitted to view and manage this device

Attributes	Type	Description
storedCredentials	Array of objects	Information about the stored credential that is associated with this device, if applicable
description	String	Description of the stored credential
id	String	ID of the stored credential
userName	String	Name of the stored credential
uri	String	URI of the device
serialNumber	String	Serial number
slots	Integer	Primary slot
stackedMode	Boolean	Identifies whether the switch is in stacked mode. This can be one of the following values. • **true**. The switch is in stacked mode • **false**. The switch is not in stacked mode
stackRole	String	Role of the switch in the stack
sysObjectID	String	System-object identifier of the switch.
temperatureSensors	Array of objects	Information about temperature sensors
sensorName	String	Temperature sensor name
sensorState	String	Temperature sensor state
type	String	Resource type. This value is always “Switch.”
upTime	String	Time (in hundredths of a second) since the network management portion of the system was last re-initialized
uri	String	URI
userDefinedName	String	User-defined name for the device
userDescription	String	User description
uuid	String	UUID
vpdID	String	VPD ID

The following example is returned if the request is successful when the **formatType=json** query parameter is specified.


```
{
    "switchList": [{
    "accessState": "Online",
    "accessStateRecords": [{
        "health": "SUCESS",
        "ipAddress": "10.243.6.68",
        "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
        "messageDisplay": "Connection is successful",
        "messageID": "1180_SHORT",
        "messageParameters": [],
        "protocol": "CIM",
        "timestamp": 1565785907453,
        "username": "USERID"
    },
    {
        "health": "SUCESS",
```

```
    "ipAddress": "fd55:faaf:e1ab:2021:42f2:e9ff:feb8:163d",
    "messageBundle": "com.lenovo.lxca.discovery.bundle.tasks.messages",
    "messageDisplay": "Connection is successful",
    "messageID": "1180_SHORT",
    "messageParameters": [],
    "protocol": "CIM",
    "timestamp": 1565785907465,
    "username": "USERID"
}],
"applyPending": "No",
"backedBy": "real",
"badCredentials": false,
"cmmDisplayName": "NE1072T",
"cmmHealthState": "Critical",
"contact": "John Smith",
"cpuUtilization": "N/A",
"dataHandle": 1559245736963,
"description": "48*10 GbE(RJ-45), 6*40 GbE QSFP+",
"dnsHostnames": [],
"domainName": "",
"elapsedTimeMillisecs": "291128",
"entitleSerialNumber": "MM28753",
"errorFields": [],
"excludedHealthState": "Critical",
"expiredCredentials": false,
"fans": [{
    "fanName": "Fan 1",
    "fanSpeed": "1782 RPM (23 PWM)",
    "fanState": "Front-to-Back"
},
...],
"firmware": [{
    "build": "",
    "classifications": [],
    "date": "",
    "name": "Uboot",
    "role": "",
    "status": "N/A",
    "type": "Boot ROM",
    "version": "10.9.3.0"
},
...],
"FRU": "00YK768        ",
"fruSerialNumber": "",
"globalVlagState": "Disabled",
"height": 1,
"hostname": "NE1072T",
"httpsEnabled": true,
"ipInterfaces": [{
    "IPv4assignments": [{
        "id": 0,
        "subnet": "255.255.252.0",
        "gateway": "0.0.0.0",
        "address": "10.240.196.83",
        "type": "UNKNOWN"
    }],
    "IPv4DHCPmode": "UNKNOWN",
    "IPv4enabled": true,
    "IPv6assignments": [{
        "id": 0,
        "scope": "Global",
```

```
            "gateway": "0:0:0:0:0:0:0:0",
            "source": "Static",
            "address": "fe80:0:0:0:a68c:dbff:fe96:dd00",
            "prefix": 10,
            "type": "UNKNOWN"
        }],
        "IPv6DHCPenabled": false,
        "IPv6enabled": true,
        "IPv6statelessEnabled": false,
        "IPv6staticEnabled": false,
        "label": "unknown",
        "name": "mgmt0"
    }...
    ],
    "ipv4Addresses": ["10.240.196.83"],
    "ipv6Addresses": ["fe80::200:ff:fe00:0","fe80::a68c:dbff:fe96:dd00"],
    "isConnectionTrusted": "true",
    "leds": [],
    "location": {
        "location": "Santa Clara",
        "lowestRackUnit": 5,
        "rack": "Core 1",
        "room": "Core lab"
    },
    "macAddresses": ["A4:8C:DB:96:DD:00"],
    "machineType": "7159",
    "manufacturer": "LNVO",
    "manufacturerId": "",
    "manufacturingDate": "3117 (WWYY)",
    "memoryUtilization": "",
    "mgmtProcIPaddress": "10.240.196.83",
    "model": "HD6",
    "name": "NE1072T",
    "ntpPushEnabled": false,
    "ntpPushFrequency": 0,
    "operationalVlagState": "Disabled",
    "OS": "CNOS"
    "overallHealthState": "Critical",
    "panicDump": "No",
    "parent": {
        "uri": null,
        "uuid": null
    },
    "partNumber": "00YL919         ",
    "portDataSetTimestamp": "03:48:56",
    "ports": [{
        "configuredStatus": "up",
        "interfaceIndex": "410001",
        "operationalStatus": "down",
        "mtu": 1500,
        "peerMacAddress": "",
        "portName": "",
        "portSpeed": "auto",
        "portState": "down",
        "tagPVID": "",
        "vLAN": "untagged",
        "port": "Ethernet1/1",
        "PVID": "1"
    },
    ...],
    "posID": "",
```

```
    "powerState": "On",
    "powerSupply": "Power Supply 1: Off;Power Supply 2: On.",
    "productId": "",
    "productName": "Lenovo ThinkSystem NE1072T RackSwitch",
    "protectedMode": "Unknown",
    "resetReason": "1",
    "savePending": "No",
    "securityDescriptor": {
        "managedAuthEnabled": false,
        "managedAuthSupported": false,
        "publicAccess": false,
        "roleGroups": ["WIRELESS"],
        "storedCredentials": [{
            "description": "",
            "id": "2417",
            "userName": "admin"
        }],
        "uri": "switches/00000000000010008000a48cdb96dd00"
    },
    "serialNumber": "Y055DH77R016",
    "stackMode": "none",
    "stackRole": "none",
    "sysObjectID": "1.3.6.1.4.1.19046.1.7.34",
    "temperatureSensors": [{
        "sensorName": "Inlet Temp",
        "sensorState": "38 °C"
    },
    ...],
    "type": "Rackswitch",
    "upTime": "46 days, 06:37:12",
    "userDescription": "",
    "userDefinedName": "NE1072T",
    "uri": "switches/00000000000010008000A48CDB96DD00",
    "uuid": "00000000000010008000A48CDB96DD00",
    "vpdID": ""
}
```


PUT /switches/*{uuid}*

Use this method to modify properties, refresh inventory, or perform a power operation on a specific Flex and RackSwitch switch, such as restart, power on, or power off. This REST API is available only for Lenovo XClarity Administrator v1.0.1 and later.

The request body differs depending on the action that you want to perform. You can use this PUT method to perform the following management actions.

- Table 38 “Modify switch properties” on page 462
- Table 39 “Configure device authentication” on page 464
- Table 40 “Modify the power state” on page 465
- Table 41 “Configure LED states” on page 466
- Table 42 “Refresh the inventory” on page 466

This method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/switches/{uuid}`

where *{uuid}* is the UUID of the switch to be retrieved. To obtain the switch UUID, use the GET /switches method.

Query parameters

Attributes	Required / Optional	Description
synchronous=*{value}*	Optional	When modifying attributes, indicates when the job ID is returned • **true**. (default) Returns the job ID and job status after the job is complete. • **false**. Returns the job ID immediately. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. **Note:** This query parameter applies only when one or more property parameters are specified in the request body.

Request body

You can specify attributes from one of the following tables in each request.

Note: If you specify one or more attributes in Table 38 “Modify switch properties” on page 462 (to modify properties), Table 40 “Modify the power state” on page 465 (to modify the power state), or Table 42 “Refresh the inventory” on page 466 (to refresh the inventory), this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, /tasks/12) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Table 38. Modify switch properties

Attributes	Required / Optional	Type	Description
contact	Optional	String	Owner of the switch
hostname	Optional	String	Hostnam
ipv4Address	Optional	Array of strings	Pairs of IPv4 addresses including the old and the new IP address
ipv6Address	Optional	Array of strings	Pairs of IPv6 addresses including the old and the new IP address
ipInterfaces	Optional	Array	Information about the switch IP addresses
IPv4assignments	Optional	Array	Information about IPv4 assignments
address	Optional	String	IPv4 address
gateway	Optional	String	IPv4 gateway
id	Required	Integer	IPv4 assignment ID

Table 38. Modify switch properties (continued)

Attributes	Re-quired / Optional	Type	Description
subnet	Optional	String	IPv4 subnet mask
IPv4DHCPmode	Optional	String	IPv4 address assignment method. This can be one of the following values. • **STATIC_ONLY** • **DHCP_ONLY** • **DHCP_THEN_STATIC** • **UNKNOWN**
IPv4enabled	Optional	Boolean	Identifies whether IPv4 is enabled. This can be one of the following values. • **true**. IPv4 is enabled • **false**. IPv4 is disabled
IPv6assignments	Optional	Array	Information about IPv6 assignments
address	Optional	String	IPv6 address
id	Required	Integer	IPv6 assignment ID
gateway	Optional	String	IPv6 gateway
prefix	Optional	Integer	IPv6 prefix
IPv6DHCPenabled	Optional	Boolean	Identifies whether IPv6 DHCP is enabled. This can be one of the following values. • **true**. IPv6 DHCP is enabled • **false**. IPv6 DHCP is disabled
IPv6enabled	Optional	Boolean	Identifies whether IPv6 is enabled. This can be one of the following values. • **true**. IPv6 is enabled • **false**. IPv6 is disabled
IPv6statelessEnabled	Optional	Boolean	Identifies whether IPv6 stateless is enabled. This can be one of the following values. • **true**. IPv6 stateless is enabled • **false**. IPv6 stateless is disabled
IPv6staticEnabled	Optional	Boolean	Identifies whether IPv6 static is enabled. This can be one of the following values. • **true**. IPv6 static is enabled • **false**. IPv6 static is disabled
name	Required	String	IP interface name
type	Optional	String	Rype. This value is always “Switch.”
userDescription	Optional	String	Free-form description of the switch

The following example modifies configuration settings for the target switch.

```
{
    "hostname":"",
    "ipv4Addresses":["1.2.3.4", "5.6.7.8"],
    "ipv6Addresses":["fe80::00::45", new IP],
    "location":{
        "location":"new location",
        "contact": "new contact"
    }
}
```

Table 39. Configure device authentication and access control

Note: Only users with **lxc-supervisor** or **lxc-security-admin** authority can modify the access-control settings.

Attributes	Required / Optional	Type	Description
securityDescriptor	Required	Object	Information about the authentication enablement and support the associated stored credentials for a managed device
managedAuthEnabled	Optional	Boolean	Indicates whether the device uses managed authentication. This can be one of the following values. • **true**. The device uses managed authentication. • **false**. The device uses local authentication
publicAccess	Optional	Boolean	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups.
roleGroups	Optional	Array of strings	List of role groups that are permitted to view and manage this device
storedCredentials	Required if **managedAuthEnabled** is set to `true`	Object	Information about the stored credential that is associated with this device, if applicable
id	Required if **managedAuthEnabled** is set to `true`	String	ID of the stored credential to associated with the device

The following example restricts access to the managed device to members of the specified role groups:

```
{
   "securityDescriptor": {
      "publicAccess": false,
      "roleGroups": ["sales-os-admin","corp_fw_admin"]
   }
}
```

Table 40. Modify the power state

Attributes	Required / Optional	Type	Description
powerState	Optional	String	Performs a power operation on the switch. This can be one of the following values. • Flex switches – **powerOn**. Powers on the switch. – **powerOff**. Powers off the switch immediately. – **powerCycleSoftGrace**. Restarts the switch immediately. – **reset**. Restarts the switch immediately. – **virtualReseat**. Simulates removing power from the bay. • RackSwitch switches – **powerOn**. Powers on the switch. – **powerOff**. Powers off the switch device immediately. – **powerCycleSoft**. Restarts the switch immediately. **Note:** RackSwitch switches can only be restarted (**powerCycleSoft**). Other power actions are not supported. If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

The following example restarts the target switch.

```
{
    "powerState": "powerCycleSoft"
}
```

Table 41. Configure LED states

Attributes	Required / Optional	Type	Description
leds	Optional	Object	Changes the state of the location LED.
name	Required	String	Description of the LED (for example, “Fault” or “Power”. To obtain the names of LEDs for a specific switch, use the GET /switches/*{uuid_list}* method.
state	Required	String	State of LED. This can be one of the following values. • **off** • **on** • **blinking** To obtain the current state of the LED, use the GET /switches/*{uuid_list}* method.

The following example turns off the Enclosure Identify LED.

```
{
   "leds":[{
      "name":"Enclosure Identify",
      "state":"off"
   }]
}
```

Table 42. Refresh the inventory

Attributes	Required / Optional	Type	Description
refreshInventory	Optional	String	Refreshes inventory for the switch If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response header includes a URI in the form /tasks/*{task_id}* (for example, `/tasks/12`) that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

The following example refreshes inventory for the target switch.

```
{
   "refreshInventory": "true"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response body provides information about the success or failure of the request. The attributes in the response body differ depending on the specified request attributes.

Note: A response body is not returned for some requests.

The following example is returned when the **"refreshInventory": "true"** is specified in the request body to refresh the device inventory.

```
{
   "statusCode": 200,
   "statusDescription": "The request completed successfully.",
   "messages": [{
      "explanation": "refreshInventory request for target 6ED2CB368C594C66C2BB066D5A306138 has
                      completed successfully.",
      "id": "FQXDM0200",
      "recovery": "",
      "recoveryUrl": "",
      "text": "The request completed successfully."
   }]
}
```

Chapter 5. Resource-group

The following resources are available for managing resource groups.

A *resource group* is logical set of managed devices that you can view collectively and act on. There are two types of resource groups:

- **Static**. Customized group of specific devices.
- **Dynamic**. Rule-based group of devices (for example, all servers of a specific type). This group contains a dynamic list of devices based on a set of inventory properties.

Actions cannot be performed on a resource group; however, you can select all devices in the group, and perform actions collectively on all selected devices.

/resourceGroups

Use this REST API to retrieve information about all resource groups, create a single resource group, modify resource-group properties, add devices to a specific static group, or change the criteria of a dynamic resource group.

HTTP methods

GET, PUT, POST

GET /resourceGroups

Use this method to return information about all resource groups.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/resourceGroups`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
groupList	Array of objects	List of all resource groups
See GET /resourceGroups/*{uuid}*	Object	Detailed information about each resource group

The following example is returned if the request is successful.


```
{
   "groupList": [{
      "criteria": null,
      "description": "Business application VMware clusters",
      "healthStatus": "Normal",
      "members": [
         "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
         "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
      ],
      "memberUuids": [
         "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
         "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
      ],
      "name": "e-Commerce Servers",
   "query": null
   "rsql": null,
      "type": "static",
      "uuid": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
   },
   {
      "criteria": {
         "criteria": [{
            "id": "1000",
            "operator": "equals",
            "parent": "root",
            "property": "overallHealthState",
            "value": "Critical"
         },
         {
            "id": "1002",
            "operator": "contains",
            "parent": "root",
            "property": "location.location",
            "value": "Lab10"
         },
         {
            "id": "1002",
            "operator": "contains",
            "parent": "root",
            "property": "location.rack",
            "value": "rack1"
         },
```

```
        {
           "criteria": [{
              "id": "1004",
              "operator": "contains",
              "parent": "1003",
              "property": "machineType",
              "value": "7X07"
           },
           {
              "id": "1005",
              "operator": "contains",
              "parent": "1003",
              "property": "machineType",
              "value": "7X08"
           }],
           "id": "1003",
           "operator": "OR",
           "parent": "root"
        }],
        "id": "root",
        "operator": "AND",
        "parent": "root"
     },
      "description": "All ThinkSystem SR530 servers in room 1 in Lab10 that have critical errors",
      "healthStatus": "Normal",
      "members": [
         "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
         "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB",
         "nodes/CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"
      ],
      "memberUuids": [
         "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
         "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB",
         "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"
      ],
      "name": "Critical SR530 servers",
   "query": null
   "rsql": null,
      "type": "dynamic",
      "uuid": "GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG"
   }]
}
```


PUT /resourceGroups

Use this method to modify resource-group properties, add devices to a specific static group, or change the criteria of a dynamic resource group.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/resourceGroups`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description

criteria	Required if **type** is “dynamic”	Object	(Dynamic groups only) Information about a simple criteria object or criteria set that select which managed devices are members of the dynamic group
			Simple criteria is a query (logical rule) that compares property values. The following example selects managed devices whose contact is John@company.com.
			`{ "property": "contact", "operator": "equals", "value": "John@company.com", }`
			
			A *criteria set* is the root of the tree structure that defines how the simple criteria are logically combined, using Boolean AND and OR relationships. The following example shows a criteria set that logically combines two simple criteria with an AND relationship. It selects managed devices whose contact is John@company.com and are in the Critical state.
			`{ "operator": "AND", "criteria": [{ "property": "contact", "operator": "equals", "value": "John@company.com" }, { "property": "overallHealthState", "operator": "equals", "value": "Critical" }] }`

criteria	Required only for criteria sets	Array of objects	Nested criteria or criteria set that defines the members of the dynamic group. Array elements can be a combination of simple criteria or criteria set objects.
id	Required	String	ID of the simple criteria or criteria set object
operator		String	Operator For criteria, you can obtain a list of valid operator values for each property using GET /resourceGroups/criteriaProperties. For criteria sets, this can be one of the following values: • **AND**. Members must satisfy all specified values. • **OR**. Members must satisfy one or more of the specified values.
parent	Required	String	ID of the parent criteria set. This is “root” when the criteria or criteria set is not nested.
property	Required only for simple criteria	String	Inventory property. To obtain a list of properties, use GET /resourceGroups/criteriaProperties.

Attributes	Re-quired / Optional	Type	Description
value	Required only for simple criteria	String	Value of the property
description	Optional	String	Description of the resource group
members	Optional	Array of strings	(Static groups only) URIs for all managed devices that are members of this resource group Members are automatically removed from the group if the device is not managed by Lenovo XClarity Administrator. For dynamic groups, the members consist of the managed devices that satisfy the criteria at the time that the GET request is done.
name	Required	String	Unique name of the resource group
type	Optional	String	Type of resource group. This can be one of the following values. • **static** • **dynamic** **Note:** The group type cannot be changed.
uuid	Required	String	UUID of the resource group to be modified **Note:** The group UUID cannot be changed.

The following example modifies the properties and membership of a static group.

```
{
   "description": "Business application VMware clusters",
   "members": [
      "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "name": "e-Commerce Servers",
   "type": "static",
   "uuid": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
}
```

The following example modifies the properties and criteria for a dynamic group.

```
{
   "criteria": {
      "operator": "AND",
      "criteria": [{
         "property": "overallHealthState",
         "operator": "equals",
         "value": "Normal"
      },
      {
         "property": "location.location",
         "operator": "contains",
         "value": "Lab10"
      },
      {
         "property": "location.rack",
         "operator": "contains",
         "value": "rack1"
      },
      {
```

```
         "operator": "OR",
         "criteria": [
         {
            "property": "machineType",
            "operator": "contains",
            "value": "7X07"
         },
         {
            "property": "machineType",
            "operator": "contains",
            "value": "7X08"
         }]
      }]
   },
   "description": "All ThinkSystem SR530 servers in room 1 in Lab10 that are offline ",
   "name": "Offline SR530 servers",
   "type": "dynamic",
   "uuid": "GGGGGGGGGGGGGGGGGGGGGGGGGGGGGG"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description

criteria	Object	(Dynamic groups only) Information about a simple criteria object or criteria set that select which managed devices are members of the dynamic group
		Simple criteria is a query (logical rule) that compares property values. The following example selects managed devices whose contact is John@company.com.
		`{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com",`
		`}`
		
		A *criteria set* is the root of the tree structure that defines how the simple criteria are logically combined, using Boolean AND and OR relationships. The following example shows a criteria set that logically combines two simple criteria with an AND relationship. It selects managed devices whose contact is John@company.com and are in the Critical state.
		`{`
		`"operator": "AND",`
		`"criteria": [{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com"`
		`},`
		`{`
		`"property": "overallHealthState",`
		`"operator": "equals",`
		`"value": "Critical"`
		`}]`
		`}`

criteria	Array of objects	Nested criteria or criteria set that defines the members of the dynamic group. Array elements can be a combination of simple criteria or criteria set objects.
id	String	ID of the simple criteria or criteria set object
operator	String	Operator For criteria, you can obtain a list of valid operator values for each property using GET /resourceGroups/criteriaProperties. For criteria sets, this can be one of the following values: • **AND**. Members must satisfy all specified values. • **OR**. Members must satisfy one or more of the specified values.
parent	String	ID of the parent criteria set. This is “root” when the criteria or criteria set is not nested.
property	String	Inventory property. To obtain a list of properties, use GET /resourceGroups/criteriaProperties.
value	String	Value of the property
description	String	Description of the resource group

Attributes	Type	Description
healthStatus	String	Status of the device with the highest severity. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
members	Array of strings	URIs for all managed devices that are members of this resource group Members are automatically removed from the group if the device is not managed by Lenovo XClarity Administrator. For dynamic groups, the members consist of the managed devices that satisfy the criteria at the time that the GET request is done.
memberUuids	Array of strings	UUIDs for all managed devices that are members of this resource group
name	String	Unique name of the resource group
query	String	Internal use only. This attribute is deprecated and will be removed in a future release.
rsql	String	Internal use only. This attribute is deprecated and will be removed in a future release.
type	String	Type of resource group. This can be one of the following values. • **static** • **dynamic**
uuid	String	Resource group UUID

The following example is returned if the request is successful.

```
{
   "criteria": null,
   "description": "Business application VMware clusters",
   "healthStatus": "Critical",
   "members": [
      "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "memberUuids":[
      "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "name": "e-Commerce Servers",
   "type": "static",
   "uuid": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
}
```

POST /resourceGroups

Use this method to create and populate a single resource group.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/resourceGroups`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description

criteria	Required if **type** is "dynamic"	Object	(Dynamic groups only) Information about a simple criteria object or criteria set that select which managed devices are members of the dynamic group
			Simple criteria is a query (logical rule) that compares property values. The following example selects managed devices whose contact is John@company.com.
			`{ "property": "contact", "operator": "equals", "value": "John@company.com", }`
			
			A *criteria set* is the root of the tree structure that defines how the simple criteria are logically combined, using Boolean AND and OR relationships. The following example shows a criteria set that logically combines two simple criteria with an AND relationship. It selects managed devices whose contact is John@company.com and are in the Critical state.
			`{ "operator": "AND", "criteria": [{ "property": "contact", "operator": "equals", "value": "John@company.com" }, { "property": "overallHealthState", "operator": "equals", "value": "Critical" }] }`

criteria	Required only for criteria sets	Array of objects	Nested criteria that defines the members of the dynamic group. Array elements can be a combination of simple criteria or criteria set objects.
id	Required	String	ID of the simple criteria or criteria set object
operator	Required	String	Operator For criteria, you can obtain a list of valid operator values for each property using GET /resourceGroups/criteriaProperties. For criteria sets, this can be one of the following values: • **AND**. Members must satisfy all specified values. • **OR**. Members must satisfy one or more of the specified values.

Attributes	Re-quired / Optional	Type	Description
parent	Required	String	ID of the parent criteria set. This is “root” when the criteria or criteria set is not nested.
property	Required only for simple criteria	String	Inventory property. To obtain a list of properties, use GET /resourceGroups/criteriaProperties.
value	Required only for simple criteria	String	Value of the property
description	Required	String	Description of the resource group
members	Required if **type** is “static”	Array of strings	(Static groups only) Zero or more URIs for *all managed devices* that are members of this resource group URIs that are specified for devices that are not managed by Lenovo XClarity Administrator are not included in the group. Check the **members** response attribute to determine the members that were added to the group.
name	Required	String	Unique name of the resource group. The name can be 1 – 64 characters except the % & < > / characters.
preview	Optional	Boolean	Indicates whether to return members of the resulting group without actually creating the group. This can be one of the following values. • **true**. Returns a list of managed devices that are members of the resulting group without creating the group. For dynamic groups, the members consist of the managed devices that satisfy the criteria at the time that the GET request is performed. • **false**. (default) Creates the resource group.
type	Required	String	The type of resource group. This can be one of the following values. • **static** • **dynamic**

Request example

The following example creates a static group with two members.

```
{
   "description": "Business application VMware clusters",
   "members": [
      "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "name": "e-Commerce Servers",
   "type": "static",
}
```

The following example returns members of a dynamic group based on a set of criteria without creating the group.

```
{
   "criteria": {
      "criteria": [{
         "id": "1000",
```

```
            "operator": "equals",
            "parent": "root",
            "property": "overallHealthState",
            "value": "Critical"
        },
        {
            "id": "1002",
            "operator": "contains",
            "parent": "root",
            "property": "location.location",
            "value": "Lab10"
        },
        {
            "id": "1002",
            "operator": "contains",
            "parent": "root",
            "property": "location.rack",
            "value": "rack1"
        },
        {
            "criteria": [{
                "id": "1004",
                "operator": "contains",
                "parent": "1003",
                "property": "machineType",
                "value": "7X07"
            },
            {
                "id": "1005",
                "operator": "contains",
                "parent": "1003",
                "property": "machineType",
                "value": "7X08"
            }],
            "id": "1003",
            "operator": "OR",
            "parent": "root"
        }],
        "id": "root",
        "operator": "AND",
        "parent": "root"
    },
    "description": "All ThinkSystem SR530 servers in room 1 in Lab10 that have critical errors",
    "members": null,
    "name": "Critical SR530 servers",
    "preview": true,
    "type": "dynamic"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description

criteria	Object	(Dynamic groups only) Information about a simple criteria object or criteria set that select which managed devices are members of the dynamic group
		Simple criteria is a query (logical rule) that compares property values. The following example selects managed devices whose contact is John@company.com.
		`{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com",`
		`}`
		
		A *criteria set* is the root of the tree structure that defines how the simple criteria are logically combined, using Boolean AND and OR relationships. The following example shows a criteria set that logically combines two simple criteria with an AND relationship. It selects managed devices whose contact is John@company.com and are in the Critical state.
		`{`
		`"operator": "AND",`
		`"criteria": [{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com"`
		`},`
		`{`
		`"property": "overallHealthState",`
		`"operator": "equals",`
		`"value": "Critical"`
		`}]`
		`}`

criteria	Array of objects	Nested criteria or criteria set that defines the members of the dynamic group. Array elements can be a combination of simple criteria or criteria set objects.
id	String	ID of the simple criteria or criteria set object

Attributes	Type	Description
operator	String	Operator For criteria, you can obtain a list of valid operator values for each property using GET /resourceGroups/criteriaProperties. For criteria sets. This can be one of the following values. • **AND**. Members must satisfy all specified values. • **OR**. Members must satisfy one or more of the specified values.
parent	String	ID of the parent criteria set. This is “root” when the criteria or criteria set is not nested.
property	String	Inventory property. To obtain a list of properties, use GET /resourceGroups/criteriaProperties.
value	String	Value of the property
description	String	Description of the resource group
healthStatus	String	Status of the device with the highest severity. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
members	Array of strings	URIs for all managed devices that are members of this resource group Members are automatically removed from the group if the device is not managed by Lenovo XClarity Administrator. For dynamic groups, the members consist of the managed devices that satisfy the criteria at the time that the GET request is done.
memberUuids	Array of strings	UUIDs for all managed devices that are members of this resource group
name	String	Unique name of the resource group
preview	Boolean	(Preview mode only) This value is always true, indicating that preview was specified and that the response is a list of members of the resulting group, but the group was not actually created
type	String	Type of resource group. This can be one of the following values. • **static** • **dynamic**
uuid	String	Resource group UUID

The following example is returned for a static group.

```
{
   "criteria": null,
   "description": "Business application VMware clusters",
   "healthStatus": "Normal",
   "members": [
      "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "memberUuids": [
      "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
```

```
   ],
   "name": "e-Commerce Servers",
   "query": null
   "rsql": null,
   "type": "static",
   "uuid": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
}
```

The following example is returned to preview the members of a dynamic group.

```
{
   "criteria": {
      "criteria": [{
         "id": "1000",
         "operator": "equals",
         "parent": "root",
         "property": "overallHealthState",
         "value": "Critical"
      },
      {
         "id": "1002",
         "operator": "contains",
         "parent": "root",
         "property": "location.location",
         "value": "Lab10"
      },
      {
         "id": "1002",
         "operator": "contains",
         "parent": "root",
         "property": "location.rack",
         "value": "rack1"
      },
      {
         "criteria": [{
            "id": "1004",
            "operator": "contains",
            "parent": "1003",
            "property": "machineType",
            "value": "7X07"
         },
         {
            "id": "1005",
            "operator": "contains",
            "parent": "1003",
            "property": "machineType",
            "value": "7X08"
         }],
         "id": "1003",
         "operator": "OR",
         "parent": "root"
      }],
      "id": "root",
      "operator": "AND",
      "parent": "root"
  },
   "description": "All ThinkSystem SR530 servers in room 1 in Lab10 that have critical errors",
   "healthStatus": "Normal",
   "members": [
      "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB",
      "nodes/CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"
```

```
   ],
   "memberUuids": [
      "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB",
      "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"
   ],
   "name": "Critical SR530 servers",
   "preview": true,
   "type": "dynamic",
   "uuid": "GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG"
}
```

/resourceGroups/*{uuid}*

Use this REST API to retrieve information about a specific resource group, change group properties, change the criteria of a dynamic resource group, add or remove devices from a static group, and delete a resource group.

HTTP methods

GET, PUT, PATCH, DELETE

GET /resourceGroups/*{uuid}*

Use this method to retrieve information about a specific resource group.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/resourceGroups/{uuid}`

where *{uuid}* is the UUID of a resource group. To obtain the group UUID, use GET /resourceGroups.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description

criteria	Object	(Dynamic groups only) Information about a simple criteria object or criteria set that select which managed devices are members of the dynamic group
		Simple criteria is a query (logical rule) that compares property values. The following example selects managed devices whose contact is John@company.com.
		`{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com",`
		`}`
		
		A *criteria set* is the root of the tree structure that defines how the simple criteria are logically combined, using Boolean AND and OR relationships. The following example shows a criteria set that logically combines two simple criteria with an AND relationship. It selects managed devices whose contact is John@company.com and are in the Critical state.
		`{`
		`"operator": "AND",`
		`"criteria": [{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com"`
		`},`
		`{`
		`"property": "overallHealthState",`
		`"operator": "equals",`
		`"value": "Critical"`
		`}]`
		`}`

criteria	Array of objects	Nested criteria or criteria set that defines the members of the dynamic group. Array elements can be a combination of simple criteria or criteria set objects.
id	String	ID of the simple criteria or criteria set object
operator	String	Operator For criteria, you can obtain a list of valid operator values for each property using GET /resourceGroups/criteriaProperties. For criteria sets, this can be one of the following values: • **AND**. Members must satisfy all specified values. • **OR**. Members must satisfy one or more of the specified values.
parent	String	ID of the parent criteria set. This is “root” when the criteria or criteria set is not nested.
property	String	Inventory property. To obtain a list of properties, use GET /resourceGroups/criteriaProperties.
value	String	Value of the property
description	String	Description of the resource group

Attributes	Type	Description
healthStatus	String	Status of the device with the highest severity. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
members	Array of strings	URIs for all managed devices that are members of this resource group Members are automatically removed from the group if the device is not managed by Lenovo XClarity Administrator. For dynamic groups, the members consist of the managed devices that satisfy the criteria at the time that the GET request is done.
memberUuids	Array of strings	UUIDs for all managed devices that are members of this resource group
name	String	Unique name of the resource group
query	String	Internal use only. This attribute is deprecated and will be removed in a future release.
rsql	String	Internal use only. This attribute is deprecated and will be removed in a future release.
type	String	Type of resource group. This can be one of the following values. • **static** • **dynamic**
uuid	String	Resource group UUID

The following example is returned if the request is successful for a static group.

```
{
   "criteria": null,
   "description": "Business application VMware clusters",
   "healthStatus": "Normal",
   "members": [
      "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "memberUuids": [
      "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "name": "e-Commerce Servers",
   "query": null
   "rsql": null,
   "type": "static",
   "uuid": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
}
```

The following example is returned if the request is successful for a dynamic group.

```
{
   "criteria": {
      "criteria": [{
         "id": "1000",
         "operator": "equals",
```

```
            "parent": "root",
            "property": "overallHealthState",
            "value": "Critical"
        },
        {
            "id": "1002",
            "operator": "contains",
            "parent": "root",
            "property": "location.location",
            "value": "Lab10"
        },
        {
            "id": "1002",
            "operator": "contains",
            "parent": "root",
            "property": "location.rack",
            "value": "rack1"
        },
        {
            "criteria": [{
                "id": "1004",
                "operator": "contains",
                "parent": "1003",
                "property": "machineType",
                "value": "7X07"
            },
            {
                "id": "1005",
                "operator": "contains",
                "parent": "1003",
                "property": "machineType",
                "value": "7X08"
            }],
            "id": "1003",
            "operator": "OR",
            "parent": "root"
        }],
        "id": "root",
        "operator": "AND",
        "parent": "root"
    },
    "description": "All ThinkSystem SR530 servers in room 1 in Lab10 that have critical errors",
    "healthStatus": "Normal",
    "members": [
        "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
        "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB",
        "nodes/CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"
    ],
    "memberUuids": [
        "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
        "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB",
        "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"
    ],
    "name": "Critical SR530 servers",
    "query": null
    "rsql": null,
    "type": "dynamic",
    "uuid": "GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG"
}
```

PUT /resourceGroups/*{UUID}*

Use this method to modify resource-group properties, add devices to a specific static group, or change the criteria of a dynamic resource group.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/resourceGroups/{UUID}`

where *{UUID}* is the UUID of a resource group. To obtain the group UUID, use GET /resourceGroups.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description

criteria	Required if **type** is "dynamic"	Object	(Dynamic groups only) Information about a simple criteria object or criteria set that select which managed devices are members of the dynamic group
			Simple criteria is a query (logical rule) that compares property values. The following example selects managed devices whose contact is John@company.com.
			`{`
			`"property": "contact",`
			`"operator": "equals",`
			`"value": "John@company.com",`
			`}`
			
			A *criteria set* is the root of the tree structure that defines how the simple criteria are logically combined, using Boolean AND and OR relationships. The following example shows a criteria set that logically combines two simple criteria with an AND relationship. It selects managed devices whose contact is John@company.com and are in the Critical state.
			`{`
			`"operator": "AND",`
			`"criteria": [{`
			`"property": "contact",`
			`"operator": "equals",`
			`"value": "John@company.com"`
			`},`
			`{`
			`"property": "overallHealthState",`
			`"operator": "equals",`
			`"value": "Critical"`
			`}]`
			`}`

criteria	Required only for criteria sets	Array of objects	Nested criteria or criteria set that defines the members of the dynamic group. Array elements can be a combination of simple criteria or criteria set objects.

Attributes	Re-quired / Optional	Type	Description
id	Required	String	ID of the simple criteria or criteria set object
operator		String	Operator For criteria, you can obtain a list of valid operator values for each property using GET /resourceGroups/criteriaProperties. For criteria sets, this can be one of the following values: • **AND**. Members must satisfy all specified values. • **OR**. Members must satisfy one or more of the specified values.
parent	Required	String	ID of the parent criteria set. This is “root” when the criteria or criteria set is not nested.
property	Required only for simple criteria	String	Inventory property. To obtain a list of properties, use GET /resourceGroups/criteriaProperties.
value	Required only for simple criteria	String	Value of the property
description	Optional	String	Description of the resource group
members	Optional	Array of strings	(Static groups only) URIs for all managed devices that are members of this resource group Members are automatically removed from the group if the device is not managed by Lenovo XClarity Administrator. For dynamic groups, the members consist of the managed devices that satisfy the criteria at the time that the GET request is done.
name	Required	String	Unique name of the resource group
type	Optional	String	Type of resource group. This can be one of the following values. • **static** • **dynamic** **Note:** The group type cannot be changed.
uuid	Required	String	UUID of the resource group to be modified **Note:** The group UUID cannot be changed.

The following example modifies the properties and membership of a static group.

```
{
   "description": "Business application VMware clusters",
   "members": [
      "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "name": "e-Commerce Servers",
   "type": "static"
}
```

The following example modifies the properties and criteria for a dynamic group.

```
{
```

```
   "criteria": {
      "criteria": [{
         "property": "overallHealthState",
         "operator": "equals",
         "value": "Normal"
      },
      {
         "property": "location.location",
         "operator": "contains",
         "value": "Lab10"
      },
      {
         "property": "location.rack",
         "operator": "contains",
         "value": "rack1"
      },
      {
         "operator": "OR",
         "criteria": [
         {
            "property": "machineType",
            "operator": "contains",
            "value": "7X07"
         },
         {
            "property": "machineType",
            "operator": "contains",
            "value": "7X08"
         }]
      }],
      "operator": "AND"
   },
   "description": "All ThinkSystem SR530 servers in room 1 in Lab10 that are offline ",
   "name": "Offline SR530 servers",
   "type": "dynamic"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description

criteria	Object	(Dynamic groups only) Information about a simple criteria object or criteria set that select which managed devices are members of the dynamic group
		Simple criteria is a query (logical rule) that compares property values. The following example selects managed devices whose contact is John@company.com.
		`{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com",`
		`}`
		
		A *criteria set* is the root of the tree structure that defines how the simple criteria are logically combined, using Boolean AND and OR relationships. The following example shows a criteria set that logically combines two simple criteria with an AND relationship. It selects managed devices whose contact is John@company.com and are in the Critical state.
		`{`
		`"operator": "AND",`
		`"criteria": [{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com"`
		`},`
		`{`
		`"property": "overallHealthState",`
		`"operator": "equals",`
		`"value": "Critical"`
		`}]`
		`}`

criteria	Array of objects	Nested criteria or criteria set that defines the members of the dynamic group. Array elements can be a combination of simple criteria or criteria set objects.
id	String	ID of the simple criteria or criteria set object
operator	String	Operator For criteria, you can obtain a list of valid operator values for each property using GET /resourceGroups/criteriaProperties. For criteria sets, this can be one of the following values: • **AND**. Members must satisfy all specified values. • **OR**. Members must satisfy one or more of the specified values.
parent	String	ID of the parent criteria set. This is “root” when the criteria or criteria set is not nested.
property	String	Inventory property. To obtain a list of properties, use GET /resourceGroups/criteriaProperties.
value	String	Value of the property
description	String	Description of the resource group

Attributes	Type	Description
healthStatus	String	Status of the device with the highest severity. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
members	Array of strings	URIs for all managed devices that are members of this resource group Members are automatically removed from the group if the device is not managed by Lenovo XClarity Administrator. For dynamic groups, the members consist of the managed devices that satisfy the criteria at the time that the GET request is done.
memberUuids	Array of strings	UUIDs for all managed devices that are members of this resource group
name	String	Unique name of the resource group
query	String	Internal use only. This attribute is deprecated and will be removed in a future release.
rsql	String	Internal use only. This attribute is deprecated and will be removed in a future release.
type	String	Type of resource group. This can be one of the following values. • **static** • **dynamic**
uuid	String	Resource group UUID

The following example is returned if the request is successful.

```
{
   "criteria": null,
   "description": "Business application VMware clusters",
   "healthStatus": "Critical",
   "members": [
      "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "memberUuids":[
      "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "name": "e-Commerce Servers",
   "type": "static",
   "uuid": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
}
```

PATCH /resourceGroups/*{uuid}*

Use this method to add or remove devices from a static resource group.

Authentication

Authentication with username and password is required.

Request URL

`PATCH https://{management_server_IP}/resourceGroups/{uuid}`

where *{uuid}* is the UUID of a resource group. To obtain the group UUID, use GET /resourceGroups.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
op	Required	String	Action to take. This can be one of the following values. • **add**. Adds a member of the resource group • **replace**. Modifies the value of an existing property or replaces the entire member list with specified members. • **remove**. Removes a member of the resource group. **Notes:** – When removing multiple members from an array, remove the member with the higher index first. When you remove a member from the array the members with a higher index are shifted so their index is reduced by one. – Lenovo XClarity Administrator verifies that the specified property value matches the property value of the managed device. If the test fails, the member is not removed from the resource group. • **test**. When removing a member, verifies that the specified URI of the managed device is the expected URI. If the test fails, the remove operation is not performed.
path	Required	String	Property to modify, for example: • To modify all members, specify /members/-. • To modify the first member in the array, specify /members/0. • To modify the name, specify /name.
value	Required	String	Value of the property To specify a member, use the device URI (for example, `nodes/AAAAAAAAAAAAAAAAAAAAAAAA`).

The following example adds a server and a switch to a static group.

```
[{
   "op": "add",
   "path": "/members/-",
   "value": "nodes/89567625677652567276527652 65255"
},
{
   "op": "add",
   "path": "/members/-",
   "value": "switches/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA "
```

```
}]
```

The following example removes two servers from a static group.

```
[{
   "op": "test",
   "path": "/members/3",
   "value": "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB "
},
{
   "op": "remove",
   "path": "/members/3"
},
{
   "op": "test",
   "path": "/members/1",
   "value": "nodes/CCCCCCCCCCCCCCCCCCCCCCCCCCCCCC "
},
{
   "op": "remove",
   "path": "/members/1"
}]
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description

criteria	Object	(Dynamic groups only) Information about a simple criteria object or criteria set that select which managed devices are members of the dynamic group
		Simple criteria is a query (logical rule) that compares property values. The following example selects managed devices whose contact is John@company.com.
		`{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com",`
		`}`
		
		A *criteria set* is the root of the tree structure that defines how the simple criteria are logically combined, using Boolean AND and OR relationships. The following example shows a criteria set that logically combines two simple criteria with an AND relationship. It selects managed devices whose contact is John@company.com and are in the Critical state.
		`{`
		`"operator": "AND",`
		`"criteria": [{`
		`"property": "contact",`
		`"operator": "equals",`
		`"value": "John@company.com"`
		`},`
		`{`
		`"property": "overallHealthState",`
		`"operator": "equals",`
		`"value": "Critical"`
		`}]`
		`}`

criteria	Array of objects	Nested criteria or criteria set that defines the members of the dynamic group. Array elements can be a combination of simple criteria or criteria set objects.
id	String	ID of the simple criteria or criteria set object
operator	String	Operator For criteria, you can obtain a list of valid operator values for each property using GET /resourceGroups/criteriaProperties. For criteria sets, this can be one of the following values: • **AND**. Members must satisfy all specified values. • **OR**. Members must satisfy one or more of the specified values.
parent	String	ID of the parent criteria set. This is “root” when the criteria or criteria set is not nested.
property	String	Inventory property. To obtain a list of properties, use GET /resourceGroups/criteriaProperties.
value	String	Value of the property
description	String	Description of the resource group

Attributes	Type	Description
healthStatus	String	Status of the device with the highest severity. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
members	Array of strings	URIs for all managed devices that are members of this resource group Members are automatically removed from the group if the device is not managed by Lenovo XClarity Administrator. For dynamic groups, the members consist of the managed devices that satisfy the criteria at the time that the GET request is done.
memberUuids	Array of strings	UUIDs for all managed devices that are members of this resource group
name	String	Unique name of the resource group
query	String	Internal use only. This attribute is deprecated and will be removed in a future release.
rsql	String	Internal use only. This attribute is deprecated and will be removed in a future release.
type	String	Type of resource group. This can be one of the following values. • **static** • **dynamic**
uuid	String	Resource group UUID

The following example is returned if the request is successful.


```
{
   "criteria": null,
   "description": "Business application VMware clusters",
   "healthStatus": "Normal",
   "members": [
      "nodes/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "nodes/BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "memberUuids": [
      "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
      "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
   ],
   "name": "e-Commerce Servers",
   "type": "static",
   "uuid": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
}
```


DELETE /resourceGroups/*{uuid}*

Use this method to delete a resource group.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/resourceGroups/{uuid}`

where *{uuid}* is the UUID of a resource group. To obtain the group UUID, use GET /resourceGroups.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/resourceGroups/criteriaProperties

Use this REST API to retrieve inventory properties that you can use to specify criteria for dynamic resource groups.

HTTP methods

GET

GET /resourceGroups/criteriaProperties

Use this method to return inventory properties that you can use to specify criteria for dynamic resource groups.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/resourceGroups/criteriaProperties`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
input	Object	
type	String	Input type. This can be one of the following values. • **enum** • **number** • **text**
values	Array of objects	
label	String	
value	String	
label	Object	
operators	Array of objects	
label	String	Operator label.

Attributes	Type	Description
value	String	Operator type. This can be one of the following values. • **equals** (for strings, numbers, and enumerations) • **contains** (for strings) • **greater t**han (for numbers) • **less than** (for numbers)
property	String	The inventory property. This can be one of the following value: • **addinCardName**. (String). Add-in card name. • **contact**. (String) Device • **description**. (String) Description • **fqdn**. (String) Fully qualified domain name • **hostname**. (String) Device host name • **ipv4Addresses**. (String) IPv4 addresses **Note:** For IPv4 addresses, you can specify a single address or a range of addresses, separated by dash or using an asterisk as wildcard (for example, `1.1.1.*` or `1.1.1.1-1.1.1.255` without spaces). • **ipv6Addresses**. (String) IPv6 addresses • **location**. (String). Location of the device • **machineType**. (String) Device machine type • **model**. (String) Device model • **overallHealthState**. (String) Status of the device with the highest severity. • **processorCores**. (Integer) Number of processor cores. • **productName**. (String) Device product name • **rack**. (String) Rack where the device is located • **room**. (String). Room where the device is located • **userDefinedName**. (String) Device name that is defined by the user

The following example is returned if the request is successful.

```
[{
   "input": {
      "type": "text",
      "values": null
   },
   "label": "Add-in card name",
   "operators": [
      {"label": "contains", "value": "contains"},
      {"label": "equals", "value": "equals"}
   ],
   "property": "addinCardName"
},

{
   "input": {
      "type": "text",
      "values": null
   },
   "label": "Contact",
   "operators": [
      {"label": "contains", "value": "contains"},
```

```
      {"label": "equals", "value": "equals"}
   ],
   "property": "contact"
},
{
   "input": {
      "type": "text",
      "values": null
   },
   "label": "Description",
   "operators": [
      {"label": "contains", "value": "contains"},
      {"label": "equals", "value": "equals"}
   ],
   "property": "description"
},
{
   "input": {
      "type": "text",
      "values": null
   },
   "label": "Fully-qualified domain name",
   "operators": [
      {"label": "contains", "value": "contains"},
      {"label": "equals", "value": "equals"}
   ],
   "property": "fqdn"
},
{
   "input": {
      "type": "text",
      "values": null
   },
   "label": "Hostname",
   "operators": [
      {"label": "contains", "value": "contains"},
      {"label": "equals", "value": "equals"}
   ],
   "property": "hostname"
},
{
   "label": "IPv4 address",
   "input": {
      "type": "text",
      "values": null
   },
   "operators": [
      {"label": "contains", "value": "contains"},
      {"label": "equals", "value": "equals"}
   ],
   "property": "ipv4Addresses"
},
{
   "input": {
      "type": "text",
      "values": null
   },
   "label": "IPv6 address",
   "operators": [
      {"label": "contains", "value": "contains"},
      {"label": "equals", "value": "equals"}
```

```
    ],
    "property": "ipv6Addresses"
},
{
    "input": {
       "type": "text",
       "values": null
    },
    "label": "Location",
    "operators": [
       {"label": "contains", "value": "contains"},
       {"label": "equals", "value": "equals"}
    ],
    "property": "location"
},
{
    "input": {
       "type": "text",
       "values": null
    },
    "label": "Machine type",
    "operators": [
       {"label": "contains", "value": "contains"},
       {"label": "equals", "value": "equals"}
    ],
    "property": "machineType"
},
{
    "input": {
       "type": "text",
       "values": null
    },
    "label": "Model",
    "operators": [
       {"label": "contains", "value": "contains"},
       {"label": "equals", "value": "equals"}
    ],
    "property": "model"
},
{
    "input": {
       "type": "enum",
       "values": [
          {"label": "Normal", "value": "Normal"},
          {"label": "Non-Critical", "value": "Non-Critical"},
          {"label": "Warning", "value": "Warning"},
          {"label": "Minor-Failure", "value": "Minor-Failure"},
          {"label": "Major-Failure", "value": "Major-Failure"},
          {"label": "Non-Recoverable", "value": "Non-Recoverable"},
          {"label": "Critical", "value": "Critical"},
          {"label": "Unknown", "value": "Unknown"}
       ]
    },
    "label": "Overall Health State",
    "operators": [{"label": "equals", "value": "equals"}],
    "property": "overallHealthState"
},
{
    "input": {
       "type": "number",
       "values": null
```

```
    },
    "label": "Processor cores",
    "operators": [
       {"label": "equals", "value": "equals"},
       {"label": "greater than", "value": "greater than"},
       {"label": "less than", "value": "less than"}
    ],
    "property": "processorCores"
},
{
    "input": {
       "type": "text",
       "values": null
    },
    "label": "Product name",
    "operators": [
       {"label": "contains", "value": "contains"},
       {"label": "equals", "value": "equals"}
    ],
    "property": "productName"
},
{
    "input": {
       "type": "text",
       "values": null
    },
    "label": "Rack",
    "operators": [
       {"label": "contains", "value": "contains"},
       {"label": "equals", "value": "equals"}
    ],
    "property": "rack"
},
{
    "input": {
       "type": "text",
       "values": null
    },
    "label": "Room",
    "operators": [
       {"label": "contains", "value": "contains"},
       {"label": "equals", "value": "equals"}
    ],
    "property": "room"
},
{
    "input": {
       "type": "text",
       "values": null
    },
    "label": "User-defined name",
    "operators": [
       {"label": "contains", "value": "contains"},
       {"label": "equals", "value": "equals"}
    ],
    "property": "userDefinedName"
}]
```

Chapter 6. Backup and restore

The following resources are available for backing up and restoring RackSwitch and Flex System switch configurations.

/files/managementServer/data

Use this REST API to import a Lenovo XClarity Administrator backup.

HTTP methods

POST

POST /files/managementServer/data

Use this method to import a Lenovo XClarity Administrator backup.

To import a backup, complete the following steps.

1. Import the backup using POST /files/managementServer/data?action=import. You must specify the passphrase to import the file.
2. Validate the backup and make it available for later use using POST /files/managementServer/data?action=process.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/files/managementServer/data
```

Query parameters

Attributes	Required / Optional	Description
action	Required	Action to take. This can be one of the following values. • **import**. Upload a backup package to the XClarity Administrator repository. • **process**. Validate the backup package for integrity and compatibility, and prepare the backup for later use.

The following example imports the backup to the XClarity Administrator.

```
POST https:// 192.0.2.0/files/managementServer/data?action=import
```

The following example validates and prepares the backup file.

```
POST https:// 192.0.2.0/files/managementServer/data?action=process
```

Request body

The request body differs depending on the value of the **action** query parameter.

action=import

Use the "multipart/form-data" media type to import the backup package. Use the attributes in the following table as the multipart name in the body. For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage.

Attributes	Required / Optional	Type	Description
filename	Required	String	Name of the backup file to import

For example:

HTTP Header

```
Content-Type: multipart/form-data; boundary=AaB03x
```

Request body

```
--AaB03x
   Content-Disposition: form-data; name=" uploadedfile";
                        filename=" LXCA_backup_Jul20.tar"
   Content-Type: application/x-tar
--AaB03x--
```

action=process

Specify a JSON object with the following attribute.

Attributes	Required / Optional	Type	Description
passphrase	Required	String	Package passphrase that was specified by the user

For example:

```
{
   "passphrase": "xxxxxxxxxx"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
201	Created	One or more new resources were successfully created.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "message": []
}
```

/managementServer/data

Use this REST API to manage Lenovo XClarity Administrator backups.

Use this REST API to perform the following actions.

- Create a backup of XClarity Administrator system data, settings, and imported files such as operating-system images and firmware updates
- Restore backed up data, settings, and file to a new or existing XClarity Administrator instance
- Retrieve information about all XClarity Administrator backups
- Copy a backup from the local repository to a remote share or from a remote share to the local repository
- Move a backup from the local repository to a remote share
- Push a backup to another brand new instance

HTTP methods

GET, PUT, POST

GET /managementServer/data

Use this method to return information about all Lenovo XClarity Administrator backups.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/managementServer/data
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
backups	Array of objects	Information about each backup
backupDate	String	Date and time when the backup was created
backupRequestedBy	String	Name of the user that created the backup
chassis	String	Number of managed chassis in the backup
checksum	String	Checksum that is used to verify the backup content
dhcp	Boolean	Indicates whether DHCP mode is enabled on the XClarity Administrator instance that was backed up. This can be one of the following values. • **true** • **failed**
dhcpEth	String	Network interface that uses DHCP (for example, “eth0”) If DHCP mode is disabled on the XClarity Administrator instance that was backed up, this value is empty.
dhcpMac	String	MAC address of the network interface that uses DHCP If DHCP mode is disabled on the XClarity Administrator instance that was backed up, this value is empty.
eth0IPv4	String	IPv4 address of the eth0 interface
eth0IPv6	String	IPv6 address of the eth0 interface
eth1IPv4	String	IPv4 address of the eth1 interface
eth1IPv6	String	IPv6 address of the eth1 interface
filename	String	Name of the XClarity Administrator backup
firmware	String	Total size of all firmware-update packages that are included in the backup

Attributes	Type	Description
ipRedirect	String	IP address that is used to access the source XClarity Administrator. This IP address is used to redirect the browser after import is completed.
label	String	User-defined label for the backup
location	Array of strings	Location of the XClarity Administrator backup. This can be one or more of the following values. • **internal**. XClarity Administrator local repository • *{mount_point}*. Mount point for the remote share that is already configured in the XClarity Administrator instance.
managementServerUuid	String	UUID of the target XClarity Administrator instance that was backed up
managementServerVersion	String	Version of the XClarity Administrator instance that was backed up
osImages	String	Total size of all operating-system images that are included in the backup
osImagesQty	String	Number of operating-system images in the backup
patterns	String	Number of configuration patterns in the backup
racks	String	Number of managed racks in the backup
servers	String	Number of managed servers in the backup
size	Integer	Total size of the backup package
storages	String	Number of managed storage devices in the backup
switches	String	Number of managed switches in the backup
urlRedirect	String	DNS address that is used to access the source XClarity Administrator, if applicable. If the DNS address exists, it is used to redirect the browser after import is completed.
users	String	Number of XClarity Administrator users in the backup
uuid	String	UUID of the backup file
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
message	Object	Information about the error message
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "backups": [{
      "backupDate": "16/10/2017 09:11:26",
      "backupRequestedBy": "SUPERVISOR",
      "chassis": "1",
      "checksum": "36147a5b9aea6e4d66fb6551635ca0f77cf8f622645b6ff949527de48c5dcfd5",
      "dhcp": false,
      "dhcpEth": "",
      "dhcpMac": "",
      "eth0IPv4": "192.0.2.0",
      "eth0IPv6": "fd55:faaf:e1ab:20fb:5054:ff:feb7:cb7c",
      "eth1IPv4": "",
      "eth1IPv6": "",
      "filename": "56be1884-3187-4a4c-90b5-13f05ee824a2_LXCA_Backup1.tar",
      "firmware": "0",
      "ipRedirect": "192.0.2.0",
      "label": "my_backup",
      "location": ["internal", "/mnt/mount1"],
      "managementServerUuid": "B6E7C884D5FE4F41AB0896FC1E74A3DB",
      "managementServerVersion": "2.1.0-154",
      "osImages": "0",
      "osImagesQty": "0",
      "patters": "0",
      "racks": "0",
      "servers": "15",
      "size": 17776640,
      "storages": "0",
      "switches": "4",
      "urlRedirect": "192.0.2.0",
      "users": "4",
      "uuid": "56be1884-3187-4a4c-90b5-13f05ee824a2"
   },
   {
      "backupDate": "23/05/2018 13:30:45",
      "backupRequestedBy": "SUPERVISOR",
      "chassis": "1",
      "checksum": "bb91001e1fe776ea3306c2f733232cb4ff5d09d996dff9b16983300d0a8f591",
      "dhcp": true,
      "dhcpEth": "eth0",
      "dhcpMac": "10:89:22:ab:4f:1d",
      "eth0IPv4": "10.243.16.45",
      "eth0IPv6": "",
      "eth1IPv4": "",
      "eth1IPv6": "",
      "filename": "4edf27ff-08d1-49b5-b7f3-7e8edc4fd278_testbkp.tar",
      "firmware": "0",
      "ipRedirect ": "10.243.16.45",
      "label": "testbkp",
      "location": ["internal"],
      "managementServerUuid": "B6E7C884D5FE4F41AB0896FC1E74A3DB",
      "managementServerVersion": "2.1.0-154",
      "osImages": "0",
      "osImagesQty": "0",
      "patterns": "0",
      "racks": "0",
      "servers": "15",
      "size": 237775640,
      "storages": "0",
      "switches": "4",
      "urlRedirect": "mymgntsrv.labs.lenovo.com",
      "users": "4",
```

```
      "uuid": "4edf27ff-08d1-49b5-b7f3-7e8edc4fd278"
   }],
   "result": "success",
   "message": []
}
```

PUT /managementServer/data

Use this method to copy a Lenovo XClarity Administrator backup from the local repository to a remote share or from a remote share to the local repository, to move a backup from the local repository to a remote share, or to push a backup to a newly setup XClarity Administrator virtual appliance.

Important: After the backup is pushed to the new virtual appliance, you can validate and prepare the backup using POST /files/managementServer/data?action=operation.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/managementServer/data`

Query parameters

None

Request body

Table 43. Copy or move a backup

Attributes	Required / Optional	Type	Description
action	Required	String	Action to take. This can be the following value. • **start**. Starts a job to copy or move the backup.
destination	Required	String	Location to save the backup. This can be one of the following values. • **internal**. XClarity Administrator local repository • *{mount_point}*. Mount point for the remote share that is already configured in the XClarity Administrator instance.
operation	Required	String	Operation to perform on the backup. This can be one of the following values. • **copy**. Copy the backup but do not delete the original copy. • **move**. Copy the backup and delete the original copy.
uuid	Required	String	UUID of the backup. To obtain the UUID, use GET /managementServer/data

The following example copies the backup to the local repository. The remote share from where the backup will be copied is chosen automatically.

```
{
   "action": "start",
   "destination": "internal",
   "operation": "copy",
   "uuid": "4edf27ff-08d1-49b5-b7f3-7e8edc4fd278"
}
```

The following example moves the backup to a specific remote share.

```
{
   "operation": "move",
   "action": "start",
   "uuid": "4edf27ff-08d1-49b5-b7f3-7e8edc4fd278",
   "destination": "/mnt/my_remote_share"
}
```

Table 44. Push a backup to another XClarity Administrator instance

Attributes	Required / Optional	Type	Description
action	Required		Action to take. This can be the following value. • **start**. Start the push operation. This method creates a job to perform the operation. • **cancel**. Cancel the push operation that is in progress.
destination	Required if action is "**start**".		IP address of the target management server
operation	Required		Operation to perform. This can be the following value. • **push**. Pushes the backup to another XClarity Administrator instance
uuid	Required if action is "**start**".		UUID of the backup. To obtain the UUID, use GET /managementServer/data

The following example pushes the backup to another XClarity Administrator instance. If the backup is not on the local repository, the backup is pushed from the remote share where it is located.

```
{
   "action": "start",
   "destination": "10.243.16.45"б
   "operation": "push",
   "uuid": "4edf27ff-08d1-49b5-b7f3-7e8edc4fd278"
}
```

The following example cancels the push operation that is currently in progress.

```
{
   "action": "cancel",
   "operation": "push"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
jobId	String	ID of the job that was created to track the action progress. This attribute is returned only when an operation is started (**action=start**). If no job was created, this attribute is empty. The response body includes a job ID that represents the job that is monitored by the management server. You can use GET /tasks/*{job_list}* to determine the status of the job. If a job was not successfully started, refer to the response code and response body for details. **Attention:** A successful response indicates that the request was successfully created and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
message	Object	Information about the error message
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned when an operation is started.

```
{
   "jobId": "17",
   "result": "success",
   "message": []
}
```

The following example is returned when an operation is canceled.

```
{
   "result": "success",
   "message": []
}
```

POST /managementServer/data

Use this method to backup or restore Lenovo XClarity Administrator system data, settings, and imported files such as operating-system images, firmware updates, and OS device drivers.

During the backup or restore operation, the management server is placed in a quiesced state. You can use the GET /managementServer/quiesce method to retrieve the current status of the management server and of the backup or restore operation that is in progress. Note that while the management server is being quiesced or resumed, status cannot be retrieved.

The restore operation is a multiple-step operation. The backup package must first be decrypted and prepared before the restore can start.

To restore a backup file in a newly setup management server, complete the following steps.

1. Send the backup to the new management server by completing one of the following steps.
   a. Importing the backup to the management server using POST /files/managementServer/data?action=import.
   b. Pushing the backup from an existing management server to the new management server using PUT /managementServer/data and specifying the **operation=push** and **action=start** request attributes.
2. Validate, decrypt, and prepare the backup using POST /files/managementServer/data?action=process.
3. Restore the backup using POST /managementServer/data and specifying the **operation=restore** and **action=start** request attributes.

To restore a backup file in an existing management server, complete the following steps

1. If the package is not in the local repository, either:

- If the file is on the local server, import the file using POST /files/managementServer/data?action=import and then validate and prepare the backup the file using POST /files/managementServer/data?action=process.
- If the file is in a remote share, copy the backup to the local repository using PUT /managementServer/data and specifying the **operation=copy**and **action=start** request attributes.

1. Decrypt and prepare the backup using POST /managementServer/data and specifying the **operation=restore** and **action=prepare** request attributes.
2. Restore the backup using POST /managementServer/data and specifying the **operation=restore** and **action=start** request attributes.

Attention: Review the following considerations before restoring a backup.

- If you want to restore managed devices, you must also restore the network settings except when the target management server uses the same IP address as the source management server when the backup was created. Restoring managed devices without restoring network settings in a management server with different IP address causes most devices to lose connectivity.
- If the backup was created in a management server with a static IP address and you restore network settings, ensure that there will be no IP address conflicts in your network. If another system is using the same IP address, you might not be able access both the existing system and the XClarity Administrator instance.
- If the backup was created in a management server with a DHCP IP address and you restore network settings, ensure that you modify the MAC address for the DHCP server or the XClarity Administrator instance so that the management server can receive the same IP address that the source management server had when the backup package was created.
- The restore operation checks whether the source IP addresses are available to avoid IP conflicts. If at least one of the source IP addresses is already in use and online, the restore operation fails and returns an error message.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/managementServer/data
```

Query parameters

None

Request body

Table 45. Back up data, settings, and imported files

Attributes	Required / Optional	Type	Description
action	Required	String	Action to take. This can be the following value. • **start**. Start the backup operation **Note:** To cancel a backup operation, use GET /managementServer/quiesce.
includeFW	Required	Boolean	Indicates whether to include firmware and OS device-driver updates in the backup. This can be one of the following values. • **true**. Include updates. • **false**. Do not include updates.
includeOS	Required	Boolean	Indicates whether to include operating system images in the backup. This can be one of the following values. • **true**. Include OS images. • **false**. Do not include OS images.
label	Required	String	File name of the backup. If empty, the file name is the current date
operation	Required	String	Type of operation to perform. This can be the following value. • **backup**. Back up data, settings, and imported files
passphrase	Required	String	Passphrase that is required for decrypting and restoring the backup. **Attention:** If you forget the passphrase, it cannot be recovered.
remoteShareDestination	Optional	String	Remote share where you want to store the backup (for example, `/mnt/backups`). If you do not specify a remote share or if the attribute is empty, the backup is stored in the local repository.

The following example creates a backup named “mybackup,” which includes operating-system images, firmware updates, and OS device drivers, and stores the backup on a specific remote share.

```
{
   "action": "start",
   "includeFW": true,
   "includeOS": true,
   "label": "mybackup",
   "operation": "backup",
   "passphrase": "123456789",
   "remoteShareDestination": "/mnt/my_remote_share"
}
```

Table 46. Prepare an existing management server for a restore operation

Attributes	Required / Optional	Type	Description
action	Required	String	Action to take. This can be the following value. • **prepare**. Decrypt the backup and prepare the management server to restore data, settings, and files
operation	Required	String	Operation to perform. This can be the following value. • **restore**. Restore data, settings, and files to an existing or new virtual appliance.
passphrase	Required	String	Passphrase to use to decrypt the backup
uuid	Required	String	UUID of the backup file to restore

The following example prepares the management server to restore data and files.

```
{
   "action": "prepare",
   "operation": "restore",
   "passphrase": "123456789",
   "uuid": "56be1884-3187-4a4c-90b5-13f05ee824a2"
}
```

Table 47. Restore data, settings, and imported files from a backup

Attributes	Required / Optional	Type	Description
action	Required	String	Action to take. This can be the following value. • **start**. Start the restore operation
devices	Required	Boolean	Indicates whether to restore device inventory. This can be one of the following values. • **true**. Restore device inventory. • **false**. Do not restore device inventory.
firmware	Required	Boolean	Indicates whether to restore firmware and OS device-driver updates. This can be one of the following values. • **true**. Restore updates. • **false**. Do not restore updates.
network	Required	Boolean	Indicates whether to restore network settings. This can be one of the following values. • **true**. Restore device network settings. • **false**. Do not restore device network settings.
operation	Required	String	Operation to perform. This can be the following value. • **restore**. Restore data, settings, and files to an existing or new virtual appliance.
osImages	Required	Boolean	Indicates whether to restore operating-system images. This can be one of the following values. • **true**. Restore operating-system images. • **false**. Do not restore operating-system images.

The following example creates a backup named “mybackup2,” which includes operating-system images but not firmware and OS device-driver updates, and stores the backup in the local repository.

```
{
   "action": "start",
```

```
   "includeFW": false,
   "includeOS": true,
   "label": "mybackup2",
   "operation": "backup",
   "passphrase": "123456789"
}
```

The following example restores data and network settings but not operating-system images, firmware updates, and OS device drivers.

```
{
   "action": "start",
   "devices": true,
   "network": true,
   "operation": "restore",
   "osImages": false,
   "firmware": false
}
```

Table 48. Cancel a restore operation

Attributes	Required / Optional	Type	Description
action	Required	String	Action to take. This can be the following value. • **cancel**. Cancel the restore operation that in in progress.
operation	Required	String	Operation to perform. This can be the following value. • **restore**. Restore data, settings, and files to an existing or new virtual appliance.

The following example cancels a restore operation.

```
{
   "action": "cancel",
   "operation": "restore"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "message": []
}
```

/managementServer/data/*{uuid}*

Use this REST API to export (download) a Lenovo XClarity Administrator backup to the local system or delete a backup from a specific location.

HTTP methods

GET, DELETE

GET /managementServer/data/*{uuid}*

Use this method to export (download) a Lenovo XClarity Administrator backup (.tar file) to the local system.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/managementServer/data/{uuid}
```

Where *{uuid}* is the UUID of the package to be downloaded. To obtain the package UUID, use the GET /managementServer/data method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /managementServer/data/*{uuid}*

Use this method to delete a Lenovo XClarity Administrator backup from a specific location.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/managementServer/data/{uuid}`

Where *{uuid}* is the UUID of the package to be downloaded. To obtain the package UUID, use the GET /managementServer/data method.

Query parameters

Parameters	Required / Optional	Description
location=*{location}*	Required	Location from where to delete the backup. This can be one of the following value. • **all**. Deletes the backup from all locations (XClarity Administrator local repository and remote shares). • **internal**. Deletes the backup in the XClarity Administrator local repository. • ***<mount_point>***. Deletes the backup from the remote share that is configured using the specified mount point. To obtain the list of locations where the package exists use the GET /managementServer/data method.

The following example deletes the backup from only the XClarity Administrator local repository.

```
DELETE https://192.0.2.0/managementServer/data/4edf27ff-08d1-49b5-b7f3-7e8edc4fd278?
location=internal
```

The following example deletes the package only from the specified remote share.

```
DELETE https://192.0.2.0/managementServer/data/4edf27ff-08d1-49b5-b7f3-7e8edc4fd278?
location=/mnt/my_remote_share
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "message": []
}
```

/managementServer/data/repository

Use this REST API to determine the amount of disk space that is used for backups in the Lenovo XClarity Administrator local repository.

HTTP methods

GET

GET /managementServer/data/repository

Use this method to determine the amount of disk space that is used for backups in the Lenovo XClarity Administrator local repository.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/managementServer/data/repository`

Query parameters

Parameters	Required / Optional	Description
packageSize=*{size}*	Optional	Size, in bytes, of the XClarity Administrator backup that you want to import

The following example verifies whether the management server has enough disk space to import the backup.

```
GET https://192.0.2.0 /managementServer/data/repository?packageSize=18270472
```

The following example retrieves disk space status.

```
GET https://192.0.2.0 /managementServer/data/repository
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
spaceUsed	String	Amount of disk space that is being used by the backup repository
totalSpace	String	Amount of total disk space that is allocated for the backup repository
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. If the **packageSize** query parameter was specified, this result means that the management server has enough disk space available to import the backup. • **failed**. The request failed. A descriptive error message is returned. If the **packageSize** query parameter was specified, this result means that the management server does not have enough disk space available to import the backup.
message	Object	Information about the error message
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "spaceUsed": "5.1 GB",
   "totalSpace": "50 GB",
   "result": "success",
   "message": []
}
```

/managementServer/quiesce

Use this REST API to retrieve the status of the management server and of an active backup or restore operation or to stop quiescing the management server and resume Lenovo XClarity Administrator.

HTTP methods

GET, PUT

GET /managementServer/quiesce

Use this method to return the status of the management server and of an active backup or restore operation.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/managementServer/quiesce
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

Attributes		Type	Description
backupRequest		Object	Operational status when a backup is being created. If a backup package is not being created, this attribute is not returned.
	backupRequestedBy	String	Name of the user who started the backup creation operation
	filename	String	Name of the XClarity Administrator backup
	includeFW	Boolean	Indicates whether to include firmware and OS device-driver updates in the backup. This can be one of the following values. • **true**. Include updates. • **false**. Do not firmware updates.
	includeOS	Boolean	Indicates whether to include operating system images in the backup. This can be one of the following values. • **true**. Include OS images. • **false**. Do not include OS images.
	jobId	String	ID of the job that was created for the backup operation
	label	String	User-defined label for the backup
	progress	String	Percentage value of the backup creation progress
	remoteShareDestination	String	Mount point of the remote share where the backup is located (for example, /mnt/backups)
	status	String	Status of the backup operation. This can be one of the following values. • EXEC: Ready to begin data export • EXEC: Export thread started • EXEC: Init export package procedures • EXEC: Checking if appliance has enough space to export package • EXEC: Starting the backup procedures • EXEC: Starting export of transformed content • EXEC: Saving xcat data • EXEC: Starting the packaging procedures • EXEC: Packaging LXCA data • EXEC: Validating LXCA data • EXEC: Creating metadata file • EXEC: Appending OS images to external tar • EXEC: Appending FW files to external tar • COMPLETED: *{backup_file_name}* • FAIL: *{error_message}*
	uuid	String	UUID of the backup file

Attributes	Type	Description
restoreRequest	Object	Operational status when a backup is being restored or imported If a backup is not being restored or imported, this attribute is not returned
devices	Boolean	Indicates whether to restore device inventory. This can be one of the following values. • **true**. Restore device inventory. • **false**. Do not restore device inventory.
filename	String	Name of the XClarity Administrator backup
firmware	Boolean	Indicates whether to restore firmware and OS device-driver updates. This can be one of the following values. • **true**. Restore updates. • **false**. Do not restore updates.
network	Boolean	Indicates whether to restore network settings. This can be one of the following values. • **true**. Restore device network settings. • **false**. Do not restore device network settings.
osImages	Boolean	Indicates whether to restore operating-system images. This can be one of the following values. • **true**. Restore operating-system images. • **false**. Do not restore operating-system images.
status	String	Status of the restore/import operation. This can be one of the following values. • uploaded • canceled • EXEC: validated • EXEC: Init restore • EXEC: Starting quiesce • EXEC: Preparing restore environment • EXEC: Restoring network and date settings • EXEC: Restoring date settings • EXEC: Restoring thread started • EXEC: Init restore package procedures • EXEC: Starting restore procedures • EXEC: Starting restore of transformed content • EXEC: Error restoring database • COMPLETED: Restore done • FAIL: *{error _message}*
uuid	String	UUID of the backup file
serviceRunning	String	Service that is currently running. This can be one of the following values. • **LXCA**. XClarity Administrator is either starting or already up and running. • **QUIESCE**. XClarity Administrator is not running while the requested backup, restore, or import operation completes.. XClarity Administrator is either starting or already up and running.
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
message	Object	Information about the error message

Attributes	Type	Description
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned while a backup is being created.

```
{
   "backupRequest": {
      "backupRequestedBy": "ADMIN",
      "filename": "ecea83fd-c68a-41a3-a1b2-cf11e992c1fb_test.tar",
      "includeFW": false,
      "includeOS": false,
      "jobId": "32",
      "label": "test",
      "progress": "65.1",
      "remoteShareDestination": "",
      "status": "COMPLETED: ecea83fd-c68a-41a3-a1b2-cf11e992c1fb_test",
      "uuid": "ecea83fd-c68a-41a3-a1b2-cf11e992c1fb"
   },
   "serviceRunning": "QUIESCE",
   "result": "success",
   "message": []
}
```

The following example is returned while a backup is being restored.

```
{
   "restoreRequest": {
      "devices": true,
      "filename": "ecea83fd-c68a-41a3-a1b2-cf11e992c1fb_test.tar",
      "firmware": false,
      "network": true,
      "osImages": false,
      "status": "COMPLETED: Restore done",
      "uuid": "ecea83fd-c68a-41a3-a1b2-cf11e992c1fb"
   },
   "serviceRunning": "QUIESCE",
   "result": "success",
   "message": []
}
```

The following example is returned while XClarity Administrator is up and there is no backup, restore, or import operation in progress.

```
{
   "serviceRunning": "LXCA",
   "result": "success",
   "message": []
}
```

PUT /managementServer/quiesce

Use this method to stop quiescing the management server and resume Lenovo XClarity Administrator and to cancel a backup operation.

Typically, you do not need to use this request, as both the backup and restore operations automatically quiesce the management server, run the operation, and then resume the management server.

If you use this request when a backup is being created, the backup operation is canceled.

Attention: Do not use this request during a restore operation. If you use this request when a backup is being restored, the restore operation is stopped; however, any that data restored up until that moment is not rolled back. Therefore, data might be lost, and both the management server and the virtual appliance itself might not behave correctly. If network settings were restored, the management server might start using the restored IP address as well.

Authentication

Authentication is not required.

Request URL

`PUT https://{management_server_IP}/managementServer/quiesce`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
action	Required	String	Action to take. This can be the following value. • **resume**. Stop quiescing the management server and resume XClarity Administrator. **Attention:** If a restore or backup process is not in progress when you call this method, the management server is forced to restart.

The following example stops quiescing the management server and resumes XClarity Administrator.

```
{
   "action": "resume"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "message": []
}
```

/switches/configurationData

Use this REST API to retrieve information about all configuration-data files for all managed RackSwitch and Flex System switches, to import a specific configuration-data file in Lenovo XClarity Administrator, or to backup and restore configuration data for one or more RackSwitch or Flex System switches.

HTTP methods

GET, PUT, POST

GET /switches/configurationData

Use this method to return information about all configuration-data files for all managed RackSwitch and Flex System switches.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/switches/configurationData`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
switches	Array of objects	Information about configuration-back files for the switches.
configurationData	Array of objects	Information about each configuration-data file.
comment	String	Comment about the configuration-data file
date	String	Date when the configuration-data file was created.
fileId	String	ID of the configuration-data file
filename	String	Name of the configuration-data file
fwVersion	String	Version of firmware that is running on the switch
size	String	Size of the configuration-data file
switchUuid	String	UUID of the switch
hostname	String	Hostname for the switch
ipAddress	String	IP address of the switch
type	String	Type of switch
uuid	String	UUID of the switch

The following example is returned if the request is successful.

```
{
   "switches": [{
      "configurationData": [{
         "comment": "comment2",
         "date": "2017-03-06T01:47:57Z",
         "fileId": "hwpdo"
         "filename": "config2.cfg",
         "fwVersion": "10.3.1.3",
         "size": "11375",
         "switchUuid": "00000000000010008000A897DCF89800"
      },
      {
         "comment": "comment1",
```

```
          "date": "2017-03-06T01:45:25Z",
          "fileId": "ihwdZ",
          "filename": "config1.cfg",
          "fwVersion": "10.3.1.3",
          "size": "11375",
          "switchUuid": "00000000000010008000A897DCF89800"
       }],
       "hostname": "G8296_CNOS",
       "ipAddress": "10.240.196.152",
       "type": "LENOVO G8296",
       "uuid": "00000000000010008000A897DCF89800"
    }]
}
```

PUT /switches/configurationData

Use this method to restore configuration data for one or more RackSwitch or Flex System switches. The switch configuration-data file is downloaded from Lenovo XClarity Administrator to the target switch, and the configuration takes effect automatically.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/switches/configurationData`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
action	Required	String	Action to perform. This can be the following value. • **restore**. Restore configuration data to a specific switch.
restart	Optional	Boolean	(Switches running CNOS only) Indicates whether to restart the switch after configuration data is restored. • **true**. Restarts the switch after the restore operation completes. • **false**. (default). Do not restart the switch. If you choose not to restart the switch, you must manually restart the switch to activate the restored configuration data.
targets	Required	Array of objects	Information about each target to be restored
filename	Required	String	Name of the configuration-data file to restore on the specified switch
uuid	Required	String	UUID of the switches to be restored. To obtain the switch UUIDs, use the GET /switches method.

The following example restores configuration data for multiple switches and restarts the switches to activate the restored data.

```
{
   "action": "restore",
   "restart": true,
   "targets" : [{
      "filename" : "Switch1.cfg",
      "uuid" : "00000000000010008000A897DCF7FC00"
   },
   {
      "filename" : "Switch2.cfg",
      "uuid" : "A1A9642D7D763A8096A9F1657FB07929"
   }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
statusCode	String	Response code
statusDescription	String	Description of the response code
text	String	Message text associated with the message identifier
uuid	String	Switch UUID

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "explanation": "",
```

```
      "recovery": {
         "text": "text here",
         "URL": "URL here"
      },
      "statusCode": 200,
      "statusDescription": "Configuration data was restored successfully.",
      "text": "",
      "uuid": "00000000000010008000A897DCF7FC00"
   },
   {
      "explanation": "",
      "recovery": {
         "text": "text here",
         "URL": "URL here"
      },
      "statusCode": 200,
      "statusDescription": "Configuration data was restored successfully.",
      "text": "",
      "uuid": "A1A9642D7D763A8096A9F1657FB07929"
   }]
}
```

POST /switches/configurationData

Use this method to import a switch configuration-data file from the local system into Lenovo XClarity Administrator or back up configuration data for one or more RackSwitch or Flex System switches. When backing up configuration data, the switch configuration data is imported into Lenovo XClarity Administrator from the target switch as a configuration-data file.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/switches/configurationData`

Query parameters

None

Request body

Table 49. Backup switch configuration data

Attributes	Required / Optional	Type	Description
action	Required	String	The action to perform. This can be the following value: • **backup**. Back up configuration data from a specific switch.
targets	Required	Array of objects	Information about each target to be restored.
description	Optional	String	Description of the configuration-data file. If a description is not specified, the following default text is used: "<*switch_name}* configuration at *{timestamp*>."

Table 49. Backup switch configuration data (continued)

Attributes	Required / Optional	Type	Description
filename	Optional	String	Name of the configuration-data file. For CNOS devices, the file name can contain alphanumeric characters and the following special characters: underscore (_), hyphen (-) and period (.). For ENOS switches, the file name can contain alphanumeric characters and any special characters. If a file name is not specified, the following default name is used: "<*switch_name*>_<*IP_address*>_<*timestamp*>.cfg."
overwirte	Optional	Boolean	Indicates whether to overwrite an existing switch-configuration file with the same name. This can be one of the following values. • **true**. Overwrite an existing switch-configuration file with the same name. • **false**. Append appended an existing switch-configuration file with the same name with a unique number (for example, [1]). **Note:** If you do not specify this attribute and a switch-configuration file with the same name already exists, the backup process fails.
uuid	Required	String	UUID of the switches to be backed up. To obtain the switch UUIDs, use the GET /switches method.

The following example backs up configuration data for multiple switches.

```
{
   "action": "backup",
   "targets" : [{
      "description" : " Switch1 configuration"
      "filename" : "Switch1.cfg",
      "overwirte" : true,
      "uuid" : "00000000000010008000A897DCF7FC00"
   },
   {
      "description" : " Switch2 configuration"
      "filename" : "Switch2.cfg",
      "overwirte" : true,
      "uuid" : "A1A9642D7D763A8096A9F1657FB07929",
   }]
}
```

Table 50. Import switch configuration-data file

Use the "multipart/form-data" media type to import the configuration-data file. Use the attributes in the following table as the multipart name in the body. For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage.

1. MyBackup_33.cfg

Table 50. Import switch configuration-data file (continued)

Attributes	Required / Optional	Type	Description
fileSize	Required	String	The size of the configuration-data file to be imported (in bytes).
uploadedfile	Required	Object	Information about the configuration-data file being imported.
fileName	Required	String	Name of the configuration-data file. For CNOS devices, the file name can contain alphanumeric characters and the following special characters: underscore (_), hyphen (-) and period (.). For ENOS switches, the file name can contain alphanumeric characters and any special characters.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	The results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages.
explanation	String	Additional information to clarify the reason for the message.
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event.
URL	String	Link to the help system for more information, if available.
statusCode	String	The response code.
statusDescription	String	Description of the response code.
text	String	Message text associated with the message identifier.

The following example is returned if the request is successful.

```
{
```

```
   "result": "success",
   "messages": [{
      "explanation": "",
      "recovery": {
         "text": "text here",
         "URL": "URL here"
      },
      "statusCode": 200,
      "statusDescription": "File imported successfully",
      "text": "".
      "uuid": "00000000000010008000A897DCF7FC00"
   }]
}
{
   "result": "success",
   "messages": [{
      "explanation": "",
      "recovery": {
         "text": "text here",
         "URL": "URL here"
      },
      "statusCode": 200,
      "statusDescription": "File imported successfully",
      "text": "".
      "uuid": "A1A9642D7D763A8096A9F1657FB07929"
   }]
}
```


/switches/*{uuid}*/configurationData

Use this REST API to retrieve information about all configuration-data files in Lenovo XClarity Administrator for a specific managed switch, to export a specific configuration-data file in Lenovo XClarity Administrator.

HTTP methods

GET

GET /switches/*{uuid}*/configurationData

Use this method to return information about all configuration-data files in Lenovo XClarity Administrator for a specific RackSwitch or Flex System switch.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/switches/{uuid}/configurationData`

where *{uuid}* is the UUID of the managed switch to be retrieved. To obtain the switch UUID, use the GET /switches method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
switches	Array of objects	Information about configuration-back files for the switches.
configurationData	Array of objects	Information about each configuration-data file.
comment	String	The date when the configuration-data file was created..
date	String	The date when the configuration-data file was created.
fileId	String	The ID of the configuration-data file
filename	String	The name of the configuration-data file
fwVersion	String	The version of firmware that is running on the switch
size	String	The size of the configuration-data file
switchUuid	String	The UUID of the switch
hostname	String	The hostname for the switch
ipAddress	String	The IP address of the switch
type	String	The type of switch
uuid	String	The UUID of the switch

The following example is returned if the request is successful.


```
{
   "switches": [{
      "configurationData": [{
         "comment": "comment2",
         "date": "2017-03-06T01:47:57Z",
         "fileId": "hwpdo"
         "filename": "config2.cfg",
         "fwVersion": "10.3.1.3",
         "size": "11375",
         "switchUuid": "00000000000010008000A897DCF89800"
      },
      {
         "comment": "comment1",
```

```
            "date": "2017-03-06T01:45:25Z",
            "fileId": "ihwdZ",
            "filename": "config1.cfg",
            "fwVersion": "10.3.1.3",
            "size": "11375",
            "switchUuid": "00000000000010008000A897DCF89800"
        }],
        "hostname": "G8296_CNOS",
        "ipAddress": "10.240.196.152",
        "type": "LENOVO G8296",
        "uuid": "00000000000010008000A897DCF89800"
    }]
}
```


/switches/configurationData/*{file_list}*

Use this REST API to download (export) one or more switch configuration-data files to the local system or delete one or more switch configuration-data files from Lenovo XClarity Administrator.

HTTP methods

GET, DELETE

GET /switches/configurationData/*{file_list}*

Use this method to download (export) one or more switch configuration-data files to the local system.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/switches/configurationData/{file_list}`

where *{file_list}* is a list of one or more IDs, separated by a comma, for the configuration-data files to be exported (for example, `T3CfO,SGmO7`). To obtain a list of configuration-data file IDs, use the GET /switches/configurationData method

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /switches/configurationData/*{file_list}*

Use this method to delete one or more switch configuration-data files from Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/switches/configurationData/{file_list}`

where *{file_list}* is a list of one or more IDs, separated by a comma, for the configuration-data files to be deleted (for example, `T3CfO,SGmO7`). To obtain a list of configuration-data file IDs, use the GET /switches/configurationData method

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier

Attributes	Type	Description
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [
      {
         "statusDescription": "Operation successful",
         "text": "Operation successful",
         "recovery": {
            "text": ""
         },
         "explanation": "File was deleted successfully.",
         "uuid": "",
         "statusCode": 200
      }
   ]
}
```

Chapter 7. Server configuration

The following resources are available for performing server configuration (Configuration Patterns) functions.

/config/target/*{id}*

Use this REST API to retrieve a list of deployable target systems according to their server pattern and profile.

HTTP methods

GET

GET /config/target/*{id}*

Use this method to return a list of deployable target systems according to their pattern and profile.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/config/target/{id}`

where *{id}* is the unique ID for the server pattern or profile that was assigned when the server pattern or profile was created. To obtain the ID for the server pattern or profile, use the GET /patterns/*{id}* or GET /profiles method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
identifier	String	
label	String	

Attributes	Type	Description
items	Object	Information about the deployable target system
firmwareLevel	String	Firmware level of the server or chassis
uuid	String	UUID of the server or chassis
children	Object	List of all deployable servers
ites	Array	Information about each deployable server in the chassis
firmwareLevel	String	Indicates whether the firmware on the server is compatible. This can be one of the following values. • **compatible**. The firmware is compatible with configuration patterns. • **backlevel**. The firmware does not support the current level of configuration patterns.
formFactor	String	Form factor of the server. This can be one of the following values. • **a**. ThinkSystem SR635 or SR655 server • **f**. Flex System server • **f4sc**. 4 bay (2 node) scalable Flex system • **f8sc**. 8 bay (4 node) scalable Flex system • **r**. System x or NeXtScale server • **rc**. Scalable rack system
ips	Array	List of all IP addresses for the server
id	String	UUID of the server
location	String	Location ID of the server
name	String	Name of the server
profile	String	Name of the profile that is assigned to the server
schedule	String	Indicates the server-restart schedule. This can be one of the following values. • **defer**. Activate management-controller settings but do not restart the server. UEFI and server settings are activated after the next restart of the server. • **immediate**. Activate all settings and restart the server immediately. • **pending**. Generate a profile for the server with the settings for review, but do not activate settings on the server. To activate the settings, you must manually activate the server profile and restart the server.
type	String	Type of server. This can be one of the following values. • **bay**. Empty location. • **imm**. A server is present at the location.
access	String	Access level of the server
bays	Array	List of bays that the server takes up
subBays	Array	(Flex System x222 Compute Node only) List of sub-bays that the device takes up

Attributes	Type	Description
architecture	String	Server architecture. This can be one of the following values. • **ia64** • **ppc** • **ppc64** • **x86** • **x86_64** • **Unknown**
rackId	String	ID of the rack that contains the server
unit	String	ID of the lowest rack unit (LRU) that contains the server
productName	String	Description the official product name for the server
deployCompatibility	Array	Information about deployment compatibility
status	String	Deploy status of the device. This can be one of the following values. • **READY** • **PROFILE_ASSIGNED** • **NOT_SUPPORTED** • **NOT_AVAILABLE** • **WARNING** • **UNKNOWN**
message	String	Information about the deployment status
powerStatus	String	Current power state of the server. This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
id	String	UUID of the chassis or server
name	String	Name of the chassis or server
type	String	Type of device. The value is always “chassis.”
access	String	The access-level of the chassis or server. This can be one of the following values. • **ok**. There are no access issues. • **placeholder**. This is a placeholder chassis; there are no access issues. • **partial**. There are possible access issues; inventory is still being discovered. • **unknown**. The access state cannot be determined. • **empty**. This is an empty bay; there are no access issues.
description	String	Description of the chassis or server
ipaddresses	Array	List of all IP addresses for the chassis or server

The following example is returned if the request is successful.

```
{
   "identifier": "id",
   "label": "name",
   "items": [{
      "firmwareLevel": "compatible",
      "uuid": "phc-d6f5c6be4e4c4996a3fbf8ffd17f78c5",
      "children": [{
         "ites": [{
            "firmwareLevel": "compatible",
```

```
        "formFactor": "f",
        "location": "phc-d6f5c6be4e4c4996a3fbf8ffd17f78c5_bay1",
        "ips": [],
        "id": "phc-d6f5c6be4e4c4996a3fbf8ffd17f78c5_bay1",
        "name": "Bay1",
        "profile": "",
        "schedule": "defer",
        "type": "bay",
        "access": "empty",
        "bays": ["1"],
        "subBays": [],
        "architecture": "",
        "rackId": "",
        "unit": 0,
        "productName": "",
        "deployCompatibility": {
           "status": "READY",
           "message": "The pattern can be deployed to this server or bay."
        },
        "powerStatus": "off"
     }]
  },
  {
     "ites": [{
        "firmwareLevel": "compatible",
        "formFactor": "f",
        "location": "phc-d6f5c6be4e4c4996a3fbf8ffd17f78c5_bay2",
        "ips": [],
        "id": "phc-d6f5c6be4e4c4996a3fbf8ffd17f78c5_bay2",
        "name": "Bay2",
        "profile": "",
        "schedule": "defer",
        "type": "bay",
        "access": "empty",
        "bays": ["2"],
        "subBays": [],
        "architecture": "",
        "rackId": "",
        "unit": 0,
        "productName": "",
        "deployCompatibility": {
           "status": "READY",
           "message": "The pattern can be deployed to this server or bay."
        },
         "powerStatus": "off"
     }]
  },
...
  {
     "ites": [{
        "firmwareLevel": "compatible",
        "formFactor": "f",
        "location": "phc-d6f5c6be4e4c4996a3fbf8ffd17f78c5_bay14",
        "ips": [],
        "id": "phc-d6f5c6be4e4c4996a3fbf8ffd17f78c5_bay14",
        "name": "Bay14",
        "profile": "",
        "schedule": "defer",
        "type": "bay",
        "access": "empty",
        "bays": ["14"],
```

```
            "subBays": [],
            "architecture": "",
            "rackId": "",
            "unit": 0,
            "productName": "",
            "deployCompatibility": {
               "status": "READY",
               "message": "The pattern can be deployed to this server or bay."
            },
            "powerStatus": "off"
         }]
      }],
      "id": "47",
      "name": "PHC",
      "type": "chassis",
      "access": "placeholder",
      "description": "",
      "ipaddresses": ""
   }]
}
```


/patterns

Use this REST API to retrieve information about all server patterns that are defined in Lenovo XClarity Administrator and import previously exported patterns. A *server pattern* represents pre-operating-system server configuration, including local storage, I/O adapter, SAN boot, and other baseboard management controller and UEFI firmware settings.

HTTP methods

GET, POST

GET /patterns

Use this method to return information about all server and category patterns that have been defined in the Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/patterns`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
identifier	String	Always set to “id”
items	Array of objects	Information about the server pattern
bmcOnly	Boolean	Indicates whether the server pattern contains only IMM settings, including “System Information,” “Management Interface,” and “Extended BMC” category patterns. This can be one of the following values. • **true**. The server pattern contains only IMM settings. • **false**. The server pattern contains non-IMM settings.
containsM2	Boolean	Indicates whether the server pattern contains M.2 drive settings. This can be one of the following values. • **true**. The server pattern contains M.2 drive settings. • **false**. The server pattern does not contain M.2 drive settings.
description	String	Description of the server pattern that was defined by the user when the pattern was created
formFactor	String	Form factor of the server pattern. This can be one of the following values. • **a**. ThinkSystem SR635 or SR655 server • **f**. Flex System server • **f4sc**. 4 bay (2 node) scalable Flex system • **f8sc**. 8 bay (4 node) scalable Flex system • **r**. System x or NeXtScale server • **rc**. Scalable rack system
id	String	Patterns unique ID that was generated on creation
inUse	Boolean	Indicates whether pattern has been deployed to one or more servers. This can be one of the following values. • **true**. The server pattern has been deployed. • **false**. The server pattern has not been deployed.
name	String	Name of the server pattern
nodeType	String	Type of server to which the pattern applies. This value is always “sysx.”
referencedBy	Array of strings	List of patterns that reference this pattern. For server patterns, this attribute is always empty.
serverType	String	Server type If the type is unknown, this value is“ NA.”

Attributes		Type	Description
	type	String	Type of pattern. This value is always “Server .”
	useCount	Integer	(Category patterns only) Number of server patterns that use this category pattern
	uri	String	URI that is used to make individual REST API calls to the referenced object
	userDefined	Boolean	Indicates whether the server pattern is user-defined or predefined. This can be one of the following values. • **true**. The server pattern is user-defined. • **false**. The server pattern is predefined.
label		String	Always set to “label”

The following example is returned if the request is successful.


```
{
   "identifier": "id",
   "items": [{
      "bmcOnly": false,
      "containsM2": false,
      "description": "",
      "id": "46",
      "inUse": true,
      "formFactor": "f",
      "name": "asdfasdf",
      "nodeType": "sysx",
      "referencedBy": [],
      "serverType": "NA",
      "type": "Server",
      "uri": "/config/template/46",
      "userDefined": true
   }],
   "label": "name"
}
```


POST /patterns

Use this method to import previously exported patterns into a Lenovo XClarity Administrator instance.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/patterns`

Query parameters

None

Request body

The request body must be a correctly formatted JSON of the configuration pattern that you want to import. Use the response body from an exported configuration pattern of the same type of pattern that you want to import using GET /patterns/*{id}*/includeSettings.

The format of the request changes depending on the type of configuration pattern (for example, server or system information) that is being imported. For information about the format for each category pattern, see the following topics:

- System-information pattern attributes
- Management-information pattern attributes
- Device and I/O ports pattern attributes
- Port pattern attributes
- Fibre Channel boot-target pattern attributes
- Extended management-controller pattern attributes
- Extended-UEFI pattern attributes
- Extended-port pattern attributes
- Extended-port pattern attributes
- Extended ThinkSystem SR635/SR655 BIOS pattern attributes

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	String	Unique id of server pattern that was imported
message	String	Message with description of success or failure

The following example is returned if the request is successful.

```
{
    "id": "46",
    "message":"New pattern imported successfully"
}
```

System-information pattern attributes

The following attributes provide information about a system-information category pattern.

These attributes can be included in the request body for the POST /patterns method and the response body for the GET /patterns/*{id}*/includeSettings method.

For more information about system-information patterns, see Defining system information settings in the Lenovo XClarity Administrator online documentation.

Attributes	Type	Description
template_type	String	Type of category pattern. This value is always “SystemInfo.”
template	Array	Information about the system-information category pattern
contact	String	System contact
description	String	Category-pattern description
location	String	The system location
name	String	Category-pattern name
systemName	String	Information about the system name
autogen	String	Indicates whether the system name is automatically generated for each server. This can be one of the following values. • **Custom**. The system name is generated based on a custom naming scheme when the pattern is deployed. • **Disable**. The system name is not changed on each server when the pattern is deployed.
hyphenChecked	Boolean	This value is always “false.”
type	String	Type of category pattern. This value is always “SystemInfo.”
uri	String	URI identifier for the exported pattern
userDefined	String	Identifies whether the category pattern is user define or learned. This can be one of the following values. • **true**. The pattern is defined by the user. • **false**. The pattern is predefined by Lenovo.

Example

```
{
    "template_type" : "SystemInfo",
    "template" : {
        "contact" : "contact",
        "description" : "Pattern created from server: Lenovo x240\n
                         Learned on: Jul 29, 2015 12:08:14 PM",
        "location" : "location",
        "name" : "Learned-System_Info-2",
        "systemName" : {
            "autogen" : "Disable",
            "hyphenChecked" : false
        },
        "type" : "SystemInfo",
        "uri" : "\/config\/template\/61",
        "userDefined" : true
    }
}
```

Management-information pattern attributes

The following attributes provide information about a management-information category pattern.

These attributes can be included in the request body for the POST /patterns method and the response body for the GET /patterns/*{id}*/includeSettings method.

For more information about management-information patterns, see Defining management interface settings in the Lenovo XClarity Administrator online documentation.

Attributes	Type	Description
template_type	String	Type of category pattern. This value is always “Management.”
template	Object	Information about the system-information category pattern
description	String	Category-pattern description
domainNameSystem	Object	Information about the domain name system (DNS)
dynamicDNS	String	Indicates whether dynamic domain name service (DDNS) is enabled or disabled
domainName	String	Domain name (for example, `company.com`)
domainNameSource	String	Indicates whether to obtain the domain name from a DHCP server. This can be one of the following values. • **dhcp**
hostName	Object	Information about the hostname
autogen	String	Indicates whether the hostname of the server is automatically generated. This can be one of the following values. • **Custom**. The hostname is generated based on a custom naming scheme when the pattern is deployed. • **Disable**. The hostname is not changed on each server when the pattern is deployed.
hyphenChecked	Boolean	This value is always “false.”
interfaceSettings	Object	Information about the interface settings
ethInterface	Integer	Network interface that is used for the management network (for example, `0` for Eth0)
maximumTransmissionUnit	String	Maximum transmission unit (MTU)
managementIPAddress	Object	Information about the management IP address
ipV4Settings	String	IPv4 address setting. This can be one of the following values. • **Enable** • **Disable** • **No Change** • This can be one of the following values.
ipV6Settings	String	IPv6 address setting. This can be one of the following values. • **Enable** • **No Change**
name	String	Category-pattern name
portAssignments	Object	Information about the port assignments
cimhttpPort	String	Port number for CIM over HTTP
cimhttpsPort	String	Port number for CIM over secure HTTP
httpPort	String	Port number for HTTP
httpsPort	String	Port number for secure HTTP
telnetcliPort	String	Port number for the Telnet CLI
remotecontrolPort	String	Port number for the remote control console
sshcliPort	String	Port number for the SSH CLI
snmpagentPort	String	Port number for the SNMP agent

Attributes	Type	Description
snmptrapsPort	String	Port number for SNMP traps
type	String	Type of category pattern. This value is always “Management.”
uri	String	URI identifier for the exported pattern
userDefined	String	Identifies whether the category pattern is user define or learned. This can be one of the following values. • **true**. The pattern is defined by the user. • **false**. The pattern is predefined by Lenovo.

Example

```
{
    "template_type" : "Management",
    "template" : {
        "description" : "Pattern created from server: Lenovo x240\n
                         Learned on: Jul 29, 2015 12:08:14 PM",
        "domainNameSystem" : {
            "domainName" : "",
            "domainNameSource" : "dhcp",
            "dynamicDNS" : "enabled"
        },
        "hostName" : {
            "autogen" : "Disable",
            "hyphenChecked" : false
        },
        "interfaceSettings" : {
            "ethInterface" : 0,
            "maximumTransmissionUnit" : "1500"
        },
        "managementIPAddress" : {
            "ipV4Settings" : "No Change",
            "ipV6Settings" : "No Change"
        },
        "name" : "Learned-Management-2",
        "portAssignments" : {
            "telnetcliPort" : "23",
            "snmptrapsPort" : "162",
            "snmpagentPort" : "161",
            "sshcliPort" : "22",
            "remotecontrolPort" : "3900",
            "httpPort" : "80",
            "httpsPort" : "443",
            "cimhttpPort" : "5988",
            "cimhttpsPort" : "5989"
        },
        "type" : "Management",
        "uri" : "\/config\/template\/62",
        "userDefined" : true
    }
}
```

Device and I/O ports pattern attributes

The following attributes provide information about a device and I/O ports category pattern.

These attributes can be included in the request body for the POST /patterns method and the response body for the GET /patterns/*{id}*/includeSettings method.

For more information about device and I/O ports patterns, see Defining devices and I/O ports settings in the Lenovo XClarity Administrator online documentation.

Attributes	Type	Description
template_type	String	Type of category pattern. This value is always “DevicesAndIOPorts.”
template	Array	Information about the system-information category pattern
consoleRedirectionAndComPorts	Array	Information about console redirection
cliMode	String	CLI mode, if service processor redirection is enabled. • **Disabled** • **Enable with user-defined keystroke sequence** • **Enable with EMS compatible keystroke sequence**
cliSequence	String	“Enter CLI” keystroke sequence
comPort1Settings	Array	Information about COM port 1 settings
comPort1	String	Indicates wither COM port 1 is enabled or disabled.
comPort1ActiveAfterBoot	String	Indicates whether the active after boot is enabled or disabled
comPort1BaudRate	String	Baud rate for COM port 1. This can be one of the following values. • **9600** • **19200** • **38400** • **57600** • **115200**
comPort1DataBits	String	Data bits. This value can be 5 - 8.
comPort1FlowControl	String	Indicates whether flow control is enabled or disabled
comPort1Parity	String	Port parity. This can be one of the following values. • **None** • **Odd** • **Even**
comPort1StopBits	String	Stop bits. This value can be 1 or 2.
comPort1TerminalEmulation	String	Text emulation. This can be one of the following values. • **ANSI** • **VT100**
setConsoleRedirection	Boolean	Indicates whether Console Redirection is enabled or disabled for COM Port 1. This can be one of the following values. • **true**. Console Redirection is enabled • **false**. Console Redirection is disabled
comPort2Settings	Array	Information about COM port 2 settings
comPort2	String	Indicates wither COM port 2 is enabled or disabled.
comPort2BaudRate	String	Baud rate for COM port 2. This can be one of the following values. • **9600** • **19200** • **38400** • **57600** • **115200**
comPort2DataBits	String	Data bits. This value can be 5 - 8.

Attributes	Type	Description
comPort2ActiveAfterBoot	String	Indicates whether the active after boot is enabled or disabled
comPort2FlowControl	String	Indicates whether flow control is enabled or disabled
comPort2Parity	String	Port parity. This can be one of the following values. • **None** • **Odd** • **Even**
setConsoleRedirection	Boolean	Indicates whether Console Redirection is enabled or disabled for COM Port 2. This can be one of the following values. • **true**. Console Redirection is enabled • **false**. Console Redirection is disabled
comPort2StopBits	String	Stop bits. This value can be 1 or 2.
comPort2TerminalEmulation	String	Text emulation. This can be one of the following values. • **ANSI** • **VT100**
consoleRedirection	String	Indicates whether console redirection is enabled or disabled
legacyOptionROM	String	Serial data port to use for legacy option ROM. This can be one of the following values. • **COM port 1** • **COM port 2**
remoteConsole	String	Indicates whether the remote console is enabled or disabled
serialPortAccessMode	String	Indicates whether serial over LAN is dedicated or disabled
serialPortSharing	String	Indicates whether serial port sharing is enabled or disabled
description	String	Category-pattern description
type	String	Type of category pattern. This value is always “DevicesAndIOPorts.”
name	String	Category-pattern name
userDefined	String	Identifies whether the category pattern is user define or learned. This can be one of the following values. • **true**. The pattern is defined by the user. • **false**. The pattern is predefined by Lenovo.
uri	String	URI identifier for the exported pattern

Example

```
{
    "template" : {
        "consoleRedirectionAndComPorts" : {
            "cliMode" : "2",
            "cliSequence" : "^[(",
            "consoleRedirection" : "Enabled",
            "legacyOptionROM" : "COM Port 1",
            "remoteConsole" : "Disable",
            "serialPortAccessMode" : "Disable",
            "serialPortSharing" : "Disable"
            "setConsoleRedirection" : true,
            "comPort1Settings" : {
                "comPort1" : "Enable",
                "comPort1ActiveAfterBoot" : "Disable",
                "comPort1BaudRate" : "115200",
```

```
                "comPort1DataBits" : "8",
                "comPort1FlowControl" : "Disable",
                "comPort1Parity" : "None",
                "comPort1StopBits" : "1",
                "comPort1TerminalEmulation" : "ANSI",
                "setConsoleRedirection" : true
            },
            "comPort2Settings" : {
                "comPort2" : "Enable",
                "comPort2ActiveAfterBoot" : "Disable",
                "comPort2BaudRate" : "115200",
                "comPort2DataBits" : "8",
                "comPort2FlowControl" : "Disable",
                "comPort2Parity" : "None",
                "comPort2StopBits" : "1",
                "comPort2TerminalEmulation" : "ANSI",
                "setConsoleRedirection" : true
            },
        },
        "description" : "Pattern created from server: Lenovo x240\n
                         Learned on: Jul 29, 2015 12:08:14 PM",
        "name" : "Learned-Devices_IO-2",
        "type" : "DevicesAndIOPorts",
        "uri" : "\/config\/template\/63",
        "userDefined" : true,
    }
    "template_type" : "DevicesAndIOPorts",
}
```


Port pattern attributes

The following attributes provide information about a port category pattern.

These attributes can be included in the request body for the POST /patterns method and the response body for the GET /patterns/*{id}*/includeSettings method.

For more information about port patterns, see Defining port settings in the Lenovo XClarity Administrator online documentation.

Attributes	Type	Description
template_type	String	Type of category pattern. This value is always “Port.”
template	Object	Information about the system-information category pattern
adapterType	String	Type of adapter to which this port pattern applies
applyToSwitch	Boolean	Indicates whether to apply corresponding settings to the chassis switch internal ports, where applicable. This can be one of the following values. • **true**. Apply the settings to the chassis switch. • **false**. Do not apply the settings to the chassis switch.
chipset	String	Chipset of the adapter that is associated with this pattern
description	String	Category-pattern description
extendedPortTemplateId	String	Pattern IDs of a referenced extended-port category pattern that are used to configure additional port settings that are learned from the server
id	String	Category pattern ID

Attributes		Type	Description
	inUse	Boolean	Identifies whether the category pattern is applied to one or more servers. This can be one of the following values. • **true**. The pattern is in use. • **false**. The pattern is not in use.
	name	String	Category-pattern name
	portCfgMode	String	Target port operational mode. This can be one of the following values. • **pNIC mode** • **vNIC virtual fabric mode** • **vNIC switch independent mode** • **vNIC unified fabric protocol mode**
	portCfgOptionCode	String	Protocols that are enabled for this port, This can be one of the following values. • **ethOnly**. Ethernet • **eth+fcoe**. FCoE • **eth+iscsi**. iSCSI • **NONE**. The protocols are configured at the vport level (see the following row).
	referencedBy	Array of strings	List of pattern IDs for server patterns that reference this category pattern
	type	String	Type of category pattern. This value is always “Port.”
	userDefined	String	Identifies whether the category pattern is user define or learned. This can be one of the following values. • **true**. The pattern is defined by the user. • **false**. The pattern is predefined by Lenovo.
	vendor	String	Vendor of the adapter that is associated with this pattern

	vports	Array of strings	Settings for each of the vports, when port virtualization is enabled, for example
			{
			enabled : true,
			id : 'portVirtualizationPattern:90:vport:91',
			maxSpeed : 100,
			minSpeed : 25,
			networkMode : 'TRUNK',
			portNumber : 1,
			protocol : 'ethOnly',
			vlanId : '2'
			}
			", ..., " {
			enabled : true,
			id : 'portVirtualizationPattern:90:vport:94',
			maxSpeed : 100,
			minSpeed : 25,
			networkMode : 'TRUNK',
			portNumber : 4,
			protocol : 'ethOnly',
			vlanId : '4'
			}

Example

```
{
    "template_type" : "Port",
```

```
    "template" : {
        "adapterType" : "adapter:16",
        "applyToSwitch" : false,
        "chipset" : "Skyhawk",
        "description" : "Pattern created from server: Lenovo x240 M5\n
                         Learned on: Jul 28, 2015 11:42:09 AM",
        "extendedPortTemplateId" : "*NONE",
        "id" : "portVirtualizationPattern:55",
        "inUse" : false,
        "name" : "Learned-Port-1.1.1",
        "portCfgMode" : "",
        "portCfgOptionCode" : "*NONE",
        "referencedBy" : [],
        "type" : "PortVirtualization",
        "userDefined" : true,
        "vendor" : "Emulex",
        "vports" : [
            "{id:'portVirtualizationPattern:55:vport:1',portNumber:1,enabled:true,
             maxSpeed:0,minSpeed:0,networkMode:'TRUNK',protocol:'ethOnly',vlanId:'0'}",
            "{id:'portVirtualizationPattern:55:vport:2',portNumber:2,enabled:true,
              maxSpeed:0,minSpeed:0,networkMode:'TRUNK',protocol:'',vlanId:'0'}",
            "{id:'portVirtualizationPattern:55:vport:3',portNumber:3,enabled:true,
              maxSpeed:0,minSpeed:0,networkMode:'TRUNK',protocol:'ethOnly',vlanId:'0'}",
            "{id:'portVirtualizationPattern:55:vport:4',portNumber:4,enabled:true,
              maxSpeed:0,minSpeed:0,networkMode:'TRUNK',protocol:'ethOnly',vlanId:'0'}"
        ]
    }
}
```

Fibre Channel boot-target pattern attributes

The following attributes provide information about a Fibre Channel boot-target category pattern.

These attributes can be included in the request body for the POST /patterns method and the response body for the GET /patterns/*{id}*/includeSettings method.

For more information about Fibre Channel boot-target patterns, see Defining Fibre Channel boot-target settings in the Lenovo XClarity Administrator online documentation.

Attributes	Type	Description
template_type	String	Type of category pattern. This value is always “FibreChannel.”
template	Array	Information about the system-information category pattern
checkvalue	Boolean	Identifies whether only a primary boot target is defined. This can be one of the following values. • **true**. Only a primary boot target is defined. • **false**. A secondary boot target is enabled.
description	String	Category-pattern description
lunbuttonvalue	Boolean	Indicates whether different LUN IDs are defined for each boot target when a secondary boot target is enabled. This can be one of the following values. • **true**. Different LUN IDs are defined for each boot target. • **false**. The same LUN ID is used for both primary and secondary boot targets, or only a primary target is defined.
name	String	Category-pattern name

Attributes		Type	Description
	primary	String	WWPN address and LUN identifier to use as primary boot targets **Tip:** If you specify `00:00:00:00:00:00:00:00` for the WWPN, Lenovo XClarity Administrator attempts to boot from the first discovered target.
	secondary	String	WWPN address and LUN identifier that is used as the secondary boot target
	type	String	Type of category pattern. This value is always “FibreChannel.”
	userDefined	String	Identifies whether the category pattern is user define or learned. This can be one of the following values. • **true**. The pattern is defined by the user. • **false**. The pattern is predefined by Lenovo.
	uri	String	URI identifier for the exported pattern

Example

```
{
    "template_type" : "FibreChannel",
   "template" : {
        "description" : "",
        "checkvalue" : false,
        "lunbuttonvalue" : false,
        "name" : "Example FC Boot",
        "primary" : "{\"items\":[{\"order\":\"0\",\"wwpn\":\"1A:55:56:43:22:21:00:01\",
                    \"lun\":\"0\",\"drag\":false,\"add\":true,\"remove\":false}]}",
        "type" : "FibreChannel",
        "userDefined" : true,
        "uri" : "\/config\/template\/74"
    }
}
```

Extended management-controller pattern attributes

The following attributes provide information about an extended baseboard management-controller (BMC) category pattern.

These attributes can be included in the request body for the POST /patterns method and the response body for the GET /patterns/*{id}*/includeSettings method.

The settings that are available are dynamic and vary from server to server and adapter to adapter. The following table lists examples of some possible settings.

For more information about extended management-controller patterns, see Defining extended IMM settings in the Lenovo XClarity Administrator online documentation.

Attributes		Type	Description
template_type		String	Type of category pattern. This value is always “ExtendedIMM.”
template		Array	Information about the system-information category pattern
	description	String	Category-pattern description
	name	String	Category-pattern name

Attributes	Type	Description
type	String	Type of category pattern. This value is always “ExtendedIMM.”
userDefined	String	Identifies whether the category pattern is user define or learned. This can be one of the following values. • **true**. The pattern is defined by the user. • **false**. The pattern is predefined by Lenovo.
IMM__GeneralSettings__pxeboot__en	String	Indicates whether the preboot execution environment (PXE) booting is enabled or disabled
IMM__GeneralSettings__snmpalerts__crten	String	This can be one of the following values. • **Enabled** • **Disabled**
IMM__GeneralSettings__snmpalerts__sysen	String	This can be one of the following values. • **Enabled** • **Disabled**
IMM__GeneralSettings__snmpalerts__wrnen	String	This can be one of the following values. • **Enabled** • **Disabled**
IMM__GeneralSettings__timeouts__f	String	This can be one of the following values. • **Enabled** • **Disabled**
IMM__GeneralSettings__timeouts__o	String	This can be one of the following values. • **Enabled** • **Disabled**
IMM__GeneralSettings__timeouts__l	String	This can be one of the following values. • **Enabled** • **Disabled**
IMM__GeneralSettings__usbeth__en	String	Indicates whether the USB Ethernet port is enabled or disabled
IMM__GeneralSettings__usbeth__ip	String	IP address of the USB Ethernet port (for example, 169.254.95.118)
IMM__GeneralSettings__usbeth__ipos	String	(for example, 169.254.95.120)
IMM__GeneralSettings__usbeth__sn	String	Subnetwork mask for the USB Ethernet port (for example, 255.255.0.0)
IMM__NetworkSettings_interface__sshcfg__cstatus	String	This can be one of the following values. • **Enabled** • **Disabled**
Additional attributes	varies	Remaining attributes vary depending on the management-controller firmware level
uri	String	URI Identifier for the exported pattern

Example

```
{
   "template" : {
      "description" : "Pattern created from server: Lenovo x240\n
                       Learned on: Jul 29, 2015 12:08:14 PM",
      "type" : "ExtendedIMM",
      "name" : "Learned-Extended_IMM-2",
```

```
"userDefined" : true,
"IMM__GeneralSettings__alertentries__number" : [{
   "index" : 1,
   "IMM__GeneralSettings__alertentries__number__del" : true
},
{
   "index" : 2,
   "IMM__GeneralSettings__alertentries__number__del" : true
},
...
{
   "index" : 12,
   "IMM__GeneralSettings__alertentries__number__del" : true
}],
"IMM__GeneralSettings__alertcfg__da" : "0.5",
"IMM__GeneralSettings__alertcfg__dr" : "0.5",
"IMM__GeneralSettings__alertcfg__rl" : "5",
"IMM__GeneralSettings__ethtousb__en" : "enabled",
"IMM__GeneralSettings__ethtousb__m" : [{
   "index" : 1,
   "value" : "3389:3389"
},
...
{
   "index" : 10,
   "value" : "0:0"
}]
"IMM__GeneralSettings__portcfg__p" : "none",
"IMM__GeneralSettings__portcfg__s" : "1",
"IMM__GeneralSettings__power__cycle" : true,
"IMM__GeneralSettings__power__cycle__every" : "clear",
"IMM__GeneralSettings__power__off" : true,
"IMM__GeneralSettings__power__off__every" : "clear",
"IMM__GeneralSettings__power__on" : true,
"IMM__GeneralSettings__power__on__d" : "01\/01\/2016",
"IMM__GeneralSettings__power__on__every" : "Day",
"IMM__GeneralSettings__power__on__t" : "00:00",
"IMM__GeneralSettings__pxeboot__en" : "disabled",
"IMM__GeneralSettings__snmpalerts__crt" : "none",
"IMM__GeneralSettings__snmpalerts__crten" : "disabled",
"IMM__GeneralSettings__snmpalerts__sys" : "none",
"IMM__GeneralSettings__snmpalerts__sysen" : "disabled",
"IMM__GeneralSettings__snmpalerts__wrn" : "none",
"IMM__GeneralSettings__snmpalerts__wrnen" : "disabled",
"IMM__GeneralSettings__thermal__mode" : "normal",
"IMM__GeneralSettings__timeouts__f" : "disabled",
"IMM__GeneralSettings__timeouts__o" : "disabled",
"IMM__GeneralSettings__timeouts__l" : "disabled",
"IMM__GeneralSettings__usbeth__en" : "enabled",
"IMM__GeneralSettings__usbeth__ip" : "169.254.95.118",
"IMM__GeneralSettings__usbeth__ipos" : "169.254.95.120",
"IMM__GeneralSettings__usbeth__sn" : "255.255.0.0",
"IMM__NetworkSettings_interface__sshcfg__cstatus" : "enabled",
"ConfigDefinitions" : {
   "items" : [{
      "mriName" : "Inteligent_Management_Module",
      "name" : "Integrated Management Module",
      "ID" : "IMM",
      "group" : [{
         "command" : [{
            "access" : "readwrite",
```

```
            "desc" : "Configure the IMM name, contact, and location",
            "ID" : "info",
            "mriName" : "Integrated_Module_Information",
            "multi-target" : "yes",
            "option" : [{
               "desc" : "Configure the \"IMM Information\", \"LU position\" setting.",
               "ID" : "LUposition"
               "mriName" : "IMMInfo_L_Uposition",
               "name" : "IMM LU Position",
               "text_data" : {
                  "default" : "",
                  "maxchars" : "7",
                  "minchars" : "1",
                  "pattern" : "^.*$",
                  "type" : "regular"
               },
            }]
            "protected" : "false",
            "name" : "Integrated Module Information",
            "target" : "all_different",
         },
         {
            "access" : "readwrite",
            "desc" : "Host power configuration settings",
            "ID" : "power",
            "mriName" : "Integrated_Module_Power",
            "multi-target" : "yes",
            "name" : "Integrated Module Power",
            "option" : [{
               "delim_data" : "true",
               "desc" : "Power on server.",
               "ID" : "on",
               "mriName" : "PowerOnServer",
               "name" : "Power On Server",
               "no_delim_sign" : "true"
               "option" : [{
                  "desc" : "Power on server every",
                  "duplicate_suboption" : "true",
                  "enumerate_data" : {
                     "choice" : [{
                        "value" : "Day",
                        "label" : "Day"
                     },
                     ...,
                     {
                        "value" : "clear",
                        "label" : "Clear"
                     }]
                  },
                  "ID" : "every",
                  "mriName" : "PowerOnEvery",
                  "name" : "Power On Every"
               },
               {
                  "desc" : "Configures the IMM \"Power Cycling Schedule\" to \"Power
on server\". Enter the date in \"mm\/dd\/yyyy\" format.",
                  "ID" : "d",
                  "mriName" : "PowerOnAtSpecifiedDate",
                  "name" : "Power On At Specified Date",
                  "text_data" : {
                     "pattern" : "^([0]\\d|[1][0-2]|\\d)\/([0-2]
```

```
                    \\d|[3][0-1]|\\d)\/(([2][01]|[1]
                    [6-9])\\d{2})"
         }
      },
      {
         "desc" : "Configures the IMM \"Power On Server at Specified Time\"
                   setting. You can schedule your server to be automatically
                   powered up. You have to enter the time in \"hh:mm\"
                   format.",
         "ID" : "t"
         "duplicate_suboption" : "true",
         "mriName" : "PowerOnAtSpecifiedTime",
         "name" : "Power On At Specified Time",
         "text_data" : {
            "pattern" : "^([0-1]\\d|[2][0-3]|\\d):([0-5]\\d|\\d)$"
         }
      },
      {
         "delim_data" : "true",
         "desc" : "Clear date for power on setting.",
         "ID" : "clear",
         "mriName" : "PowerOnClearDate",
         "name" : "Power On Clear Date"
      }]
   },
   {
      "mriName" : "PowerOffServer",
      "delim_data" : "true",
      "desc" : "Power off server.",
      "ID" : "off",
      "name" : "Power Off Server",
      "no_delim_sign" : "true"
      "option" : [{
         "mriName" : "PowerOffEvery",
         "duplicate_suboption" : "true",
         "desc" : "Power off server every",
         "name" : "Power Off Every",
         "ID" : "every",
         "enumerate_data" : {
            "choice" : [{
               "value" : "Day",
               "label" : "Day"
            }, {
               "value" : "Sun",
               "label" : "Sunday"
            },
            ...,
            {
               "value" : "clear",
               "label" : "Clear"
            }]
         }
      },
      {
         "mriName" : "ShutdownAndPowerOff",
         "duplicate_suboption" : "true",
         "delim_data" : "true",
         "desc" : "Shut down OS first and then power off",
         "name" : "Shutdown And Power Off",
         "ID" : "s"
      },
```

```
      {
         "mriName" : "PowerOffAtSpecifiedTime",
         "text_data" : {
            "pattern" : "^([0-1]\\d|[2][0-3]|\\d):([0-5]
                        \\d|\\d)$"
         },
         "duplicate_suboption" : "true",
         "desc" : "Configures the IMM \"Power Off Server at Specified Time\"
                   setting. You can schedule your server to be automatically
                   powered up. You have to enter the time in \"hh:mm\"
                   format.",
         "name" : "Power Off At Specified Time",
         "ID" : "t"
      }],
   },
   {
      "delim_data" : "true",
      "desc" : "Turns off the server power and then turns on the power",
      "ID" : "cycle",
      "mriName" : "PowerOffOnServer",
      "name" : "Power Off On Server",
      "no_delim_sign" : "true",
      "option" : [{
         "duplicate_suboption" : "true",
         "desc" : "Power Off and On server every",
         "enumerate_data" : {
            "choice" : [{
               "value" : "Day",
               "label" : "Day"
            },
            ...,
            {
               "value" : "clear",
               "label" : "Clear"
            }]
         },
         "ID" : "every",
         "mriName" : "PowerOffOnEvery",
         "name" : "Power Off On Every"
      },
      {
         "delim_data" : "true",
            "desc" : "Shut down OS and restart server",
         "duplicate_suboption" : "true",
         "ID" : "s",
         "mriName" : "ShutdownAndRestart",
         "name" : "Shutdown And Restart"
      },
      {
         "desc" : "Configures the IMM \"Power Off then On Server at Specified
                   Time\" setting. You can schedule your server to be
                   automatically powered off then on. You have to enter the
                   time in \"hh:mm\" format.",
         "duplicate_suboption" : "true",
         "ID" : "t",
         "mriName" : "PowerOffOnAtSpecifiedTime",
         "name" : "Power Off On At Specified Time",
         "text_data" : {
            "pattern" : "^([0-1]\\d|[2][0-3]|\\d):([0-5]\\d|\\d)$"
         }
      }]
```

```
            }]
         "protected" : "false",
               "target" : "primary",
         },
         ...,
         {
            "access" : "readwrite",
            "desc" : "Display and configure Ethernet to Ethernet-over-USB port
                      mapping.",
            "ID" : "ethtousb",
            "mriName" : "USBPortForwarding_Setting",
            "multi-target" : "yes",
            "name" : "USB Port Forwarding Setting",
            "option" : [{
               "desc" : "Enabled or disabled port mapping.",
               "name" : "USB Port Forwarding",
               "ID" : "en",
               "enumerate_data" : {
                  "choice" : [{
                     "value" : "disabled",
                     "label" : "Disabled"
                  },
                  {
                     "value" : "enabled",
                     "label" : "Enabled"
                  }]
               }
               "mriName" : "USBPortForwarding",
            },
            {
               "data_index" : "true",
               "desc" : "Configure the port mapping using the format \"port1:port2\",
                         where port1 is the External Ethernet port number and port2
                         is the Ethernet over USB port number.",
               "ID" : "m",
               "mriName" : "USBForwardPort",
               "multi_data" : "true"
               "name" : "USB Forward Port",
               "no_space_after_opt" : "true",
               "numeric_data" : {
                  "min" : "1",
                  "max" : "10",
                  "type" : "dec"
               },
               "text_data" : {
                  "pattern" : "[0-9]{1,5}:[0-9]{1,5}",
                  "minchars" : "3",
                  "maxchars" : "11"
               },
            }],
            "protected" : "false",
            "target" : "all_same"
         }]
         "desc" : "Inteligent Module Information",
         "ID" : "GeneralSettings",
         "mriName" : "General_Settings",
         "name" : "General Settings",
      }]
   }]
}
"uri" : "\/config\/template\/64",
```

}

Extended-UEFI pattern attributes

The following attributes provide information about an extended-UEFI category pattern.

These attributes can be included in the request body for the POST /patterns method and the response body for the GET /patterns/*{id}*/includeSettings method.

The settings that are available are dynamic and vary from server to server and adapter to adapter. The following table lists examples of some possible settings.

For more information about extended UEFI patterns, see Defining extended UEFI settings in the Lenovo XClarity Administrator online documentation.

Attributes	Type	Description
template_type	String	Type of category pattern. This value is always “ExtendedUEFI.”
template	Array	Information about the system-information category pattern
type	String	Type of category pattern. This value is always “ExtendedUEFI.”
name	String	Category-pattern name
description	String	Category-pattern description
userDefined	String	Identifies whether the category pattern is user define or learned. This can be one of the following values. • **true**. The pattern is defined by the user. • **false**. The pattern is predefined by Lenovo.
UEFI__BootModes__asu__set__OptimizedBoot	String	This can be one of the following values. • **Enabled** • **Disabled**
UEFI__BootModes__asu__set__QuietBoot	String	This can be one of the following values. • **Enabled** • **Disabled**
UEFI__DevicesandIOPorts__asu__set__ PCIExpressNativeControlUEFI__DevicesandIOPorts__ asu__ set	String	This can be one of the following values. • **Enabled** • **Disabled**
UEFI__SystemSecurity__TrustedPlatformModuleTPM12__ asu__set__TXTStateUEFI__SystemRecovery__asu__set__ POSTWatchdogTimerValue	String	This can be one of the following values. • **Enabled** • **Disabled**
UEFI__SystemRecovery__asu__set__RebootSystemonNMI	String	This can be one of the following values. • **Enabled** • **Disabled**
uriUEFI__SystemSecurity__TrustedPlatformModuleTPM12__ asu__set__MORState	Boolean	This can be one of the following values. • **Enabled** • **Disabled**
UEFI__SystemSecurity__TrustedPlatformModuleTPM12__ asu__set__TXTState	String	This can be one of the following values. • **Enabled** • **Disabled**

Attributes		Type	Description
	Additional attributes	String	Remaining attributes vary
	uri	String	URI Identifier for the exported pattern

Example

```
{
   "template_type" : "ExtendedUEFI",
   "template" : {
      "description" : "Pattern created from server: Lenovo x240\n
                       Learned on: Jul 29, 2015 12:08:14 PM",
      "name" : "Learned-Extended_UEFI-2",
      "type" : "ExtendedUEFI",
      "userDefined" : true,
      "UEFI__BackupBankManagement__asu__set" : true,
      "UEFI__BackupBankManagement__asu__set__BackupBankManagementMethod" : "User Managed",
      "UEFI__BootModes__asu__set" : true,
      "UEFI__BootModes__asu__set__OptimizedBoot" : "Disable",
      "UEFI__BootModes__asu__set__QuietBoot" : "Enable",
      "UEFI__DevicesandIOPorts__asu__set" : true,
      "UEFI__DevicesandIOPorts__asu__set__ActiveVideo" : "Onboard Device",
      "UEFI__DevicesandIOPorts__asu__set__MMConfigBase" : "3GB",
      "UEFI__DevicesandIOPorts__asu__set__PCIExpressNativeControl" : "Enable",
      "UEFI__DevicesandIOPorts__asu__set__PCI64-BitResourceAllocation" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set" : true,
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             IOExpansion1CardLEGACYOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             IOExpansion1CardUEFIOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             IOExpansion1Dev2LEGACYOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             IOExpansion1Dev2UEFIOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             IOExpansion2CardLEGACYOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             IOExpansion2CardUEFIOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             ETEExpansionConnLEGACYOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             ETEExpansionConnUEFIOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             SASControllerLEGACYOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             SASControllerUEFIOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             VideoLEGACYOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableAdapterOptionROMSupport__asu__set__
             VideoUEFIOPROM" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableOnboardDevices__asu__set" : true,
      "UEFI__DevicesandIOPorts__EnableDisableOnboardDevices__asu__set__ETEExpansionConn" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableOnboardDevices__asu__set__IOExpansion1Card" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableOnboardDevices__asu__set__IOExpansion2Card" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableOnboardDevices__asu__set__IOExpansion1Dev2" : "Enable",
      "UEFI__DevicesandIOPorts__EnableDisableOnboardDevices__asu__set__Video" : "Enable",
      "UEFI__DevicesandIOPorts__PCIeGen1Gen2Gen3SpeedSelection__asu__set" : true,
      "UEFI__DevicesandIOPorts__PCIeGen1Gen2Gen3SpeedSelection__asu__set__
             IOExpansion1CardPCIeSpeed" : "Gen3",
      "UEFI__DevicesandIOPorts__PCIeGen1Gen2Gen3SpeedSelection__asu__set__
```

```
       IOExpansion2CardPCIeSpeed" : "Gen3",
"UEFI__DevicesandIOPorts__PCIeGen1Gen2Gen3SpeedSelection__asu__set__
       ETEExpansionConnPCIeSpeed" : "Gen3",
"UEFI__DevicesandIOPorts__PCIeGen1Gen2Gen3SpeedSelection__asu__set__
       IOExpansion1Dev2PCIeSpeed" : "Gen3",
"UEFI__DevicesandIOPorts__SetOptionROMExecutionOrder__asu__set" : true,
"UEFI__DiskGPTRecovery__asu__set" : true,
"UEFI__DevicesandIOPorts__SetOptionROMExecutionOrder__asu__set__SetOptionROMExecutionOrder" :
       "SAS Controller=Video=I\/O Expansion 1 Card=I\/O Expansion 1 Dev 2=I\/O Expansion 2
        Card",
"UEFI__DiskGPTRecovery__asu__set__DiskGPTRecovery" : "Manual",
"UEFI__LegacySupport__asu__set" : true,
"UEFI__LegacySupport__asu__set__BBSBoot" : "Enable",
"UEFI__LegacySupport__asu__set__ForceLegacyVideoonBoot" : "Enable",
"UEFI__LegacySupport__asu__set__InfiniteBootRetry" : "Disable",
"UEFI__LegacySupport__asu__set__LegacyThunkSupport" : "Enable",
"UEFI__LegacySupport__asu__set__Non-PlanarPXE" : "Enable",
"UEFI__LegacySupport__asu__set__RehookINT19h" : "Disable",
"UEFI__Memory__asu__set" : true,
"UEFI__Memory__asu__set__PagePolicy" : "Adaptive",
"UEFI__Memory__asu__set__PatrolScrub" : "Disable",
"UEFI__Memory__asu__set__MemoryMode" : "Independent",
"UEFI__Memory__asu__set__MemoryPowerManagement" : "Disable",
"UEFI__Memory__asu__set__MemoryRefresh" : "1x",
"UEFI__Memory__asu__set__MemorySpeed" : "Max Performance",
"UEFI__Memory__asu__set__SocketInterleave" : "NUMA",
"UEFI__OperatingModes__asu__set" : true,
"UEFI__OperatingModes__asu__set__ChooseOperatingMode" : "Custom Mode",
"UEFI__POSTAttempts__asu__set" : true,
"UEFI__POSTAttempts__asu__set__POSTAttemptsLimit" : "3",
"UEFI__Power__asu__set" : true,
"UEFI__Power__asu__set__ActiveEnergyManager" : "Capping Disabled",
"UEFI__Power__asu__set__PlatformControlledType" : "Maximum Performance",
"UEFI__Power__asu__set__PowerPerformanceBias" : "Platform Controlled",
"UEFI__Power__asu__set__WorkloadConfiguration" : "Balanced",
"UEFI__Processors__asu__set" : true,
"UEFI__Processors__asu__set__AdjacentCachePrefetch" : "Enable",
"UEFI__Processors__asu__set__C-States" : "Disable",
"UEFI__Processors__asu__set__C1EnhancedMode" : "Disable",
"UEFI__Processors__asu__set__CoresinCPUPackage" : "All"
"UEFI__Processors__asu__set__DCUStreamerPrefetcher" : "Enable",
"UEFI__Processors__asu__set__ExecuteDisableBit" : "Enable",
"UEFI__Processors__asu__set__HardwarePrefetcher" : "Enable",
"UEFI__Processors__asu__set__Hyper-Threading" : "Enable",
"UEFI__Processors__asu__set__IntelVirtualizationTechnology" : "Enable",
"UEFI__Processors__asu__set__QPILinkFrequency" : "Max Performance",
"UEFI__SystemSecurity__TrustedPlatformModuleTPM12__asu__set" : true,
"UEFI__SystemRecovery__asu__set" : true,
"UEFI__SystemRecovery__asu__set__HaltOnSevereError" : "Disable",
"UEFI__Processors__asu__set__DCUIPPrefetcher" : "Enable",
"UEFI__Processors__asu__set__DirectCacheAccessDCA" : "Enable",
"UEFI__Processors__asu__set__ProcessorPerformanceStates" : "Enable",
"UEFI__Processors__asu__set__TurboMode" : "Enable",
"UEFI__SystemRecovery__asu__set__POSTWatchdogTimer" : "Enable",
"UEFI__SystemRecovery__asu__set__POSTWatchdogTimerValue" : "5",
"UEFI__SystemRecovery__asu__set__RebootSystemonNMI" : "Enable",
"UEFI__SystemSecurity__TrustedPlatformModuleTPM12__asu__set__MORState" : "Disable",
"UEFI__SystemSecurity__TrustedPlatformModuleTPM12__asu__set__TXTState" : "Disable",
"ConfigDefinitions" : {
   "items" : [{
      "group" : [{
```

```
   "command" : [{
      "desc" : "Configure the number of attempts to POST,
                before recovery mechanisms are to be invoked.",
      "display" : "false",
      "ID" : "asu",
      "mriName" : "AsuPOSTAttempts",
      "name" : "ASU - POST Attempts",
      "option" : [{
         "delim_data" : "true",
         "desc" : "Modify POST Attempts",
         "display" : "false",
         "ID" : "set",
         "mriName" : "SetPOSTAttempts",
         "name" : "Set POST Attempts",
         "no_delim_sign" : "true",
         "option" : [{
            "mriName" : "POSTAttemptsLimit",
            "desc" : "Enter the number of consecutive
                      failed POST attempts allowed before
                      invoking recovery mechanisms.",
            "dot_delim" : "true",
            "name" : "POST Attempts Limit",
            "ID" : "POSTAttemptsLimit",
            "group_id" : "true",
            "enumerate_data" : {
               "choice" : [{
                  "default" : "true",
                  "label" : "3",
                  "value" : "3"
               }, ...
               {
                  "value" : "Disable",
                  "label" : "Disable"
               }]
            },
            "no_delim_sign" : "true",
            "quote_data" : "true"
         }]
      }]
   }]
   "desc" : "Configure the number of attempts to POST, before
             recovery mechanisms are to be invoked.",
   "ID" : "POSTAttempts",
   "mriName" : "POSTAttempts",
   "name" : "POST Attempts",
   "preceding_option_id" : "true",
},
...,
{
   "command" : [{
      "mriName" : "AsuDiskGPTRecovery",
      "desc" : "Disk GPT (GUID Partition Table) Recovery Options.",
      "name" : "ASU - Disk GPT Recovery",
      "ID" : "asu",
      "display" : "false",
      "option" : [{
         "delim_data" : "true",
         "desc" : "Modify Disk GPT Recovery",
         "display" : "false",
         "ID" : "set",
         "mriName" : "SetDiskGPTRecovery",
```

```
                        "name" : "Set Disk GPT Recovery",
                        "option" : [{
                           "mriName" : "DiskGPTRecovery",
                           "desc" : "
When <Automatic> is selected UEFI will attempt to repair a corrupted GUID Partition
 Table (GPT) by copying the non-corrupt version over the invalid one. A message
will then be logged to the System Event Log to indicate the status of the repair.\n
\n
When <Manual> is selected UEFI will prompt the user before taking any action. The
user will have an opportunity to decide if repair action should be taken. A message
 will be logged to the EventLog to indicate the corruption found and if repair
action was taken then the repair results.\n
\n
With <None> selected no attempt will be made by UEFI to recover a corrupted GPT, a
 message will be logged to the EventLog and the system will continue to POST.
However, if the remaining valid GPT becomes corrupt, the disk drive will no longer
be accessible.",
                           "dot_delim" : "true",
                           "name" : "Disk GPT Recovery",
                           "ID" : "DiskGPTRecovery",
                           "group_id" : "true",
                           "enumerate_data" : {
                              "choice" : [{
                                 "label" : "None",
                                 "value" : "None"
                              },
                              ...,
                              {
                                  "default" : "true",
                                  "label" : "Manual",
                                  "manufacturing" : "true",
                                   "value" : "Manual"
                             }]
                             "reset-required" : "true",
                           },
                           "no_delim_sign" : "true",
                           "quote_data" : "true"
                        }],
                        "no_delim_sign" : "true"
                     }]
                  }],
                  "desc" : "Disk GPT (GUID Partition Table) Recovery Options.",
                  "ID" : "DiskGPTRecovery",
                  "mriName" : "DiskGPTRecovery",
                  "name" : "Disk GPT Recovery",
                  "preceding_option_id" : "true"
               }]
               "ID" : "UEFI",
               "mriName" : "UEFI",
               "name" : "UEFI",
               "preceding_option_id" : "true",
            }]
         },
         "uri" : "\/config\/template\/65",
      }
}
```


Extended-port pattern attributes

The following attributes provide information about an extended-port category pattern.

These attributes can be included in the request body for the POST /patterns method and the response body for the GET /patterns/*{id}*/includeSettings method.

For more information about extended port patterns, see Defining extended port settings in the Lenovo XClarity Administrator online documentation.

Attributes	Type	Description
template_type	String	Type of category pattern. This value is always “ExtendedPort.”
template	Array	Information about the system-information category pattern
bdfList	Array of strings	List of unique option IDs that are associated with the settings for this adapter
chipset	String	Chipset of the adapter that is associated with this pattern
description	String	Category-pattern description
name	String	Category-pattern name
portbdf	String	Unique group ID that is associated with the settings for this pattern
portFunctions	Array	Port functions to which this pattern applies.
protocol	String	Port protocol. This can be one of the following values. • **fc**
type	String	Type of category pattern. This value is always “ExtendedPort.”
userDefined	String	Identifies whether the category pattern is user define or learned. This can be one of the following values. • **true**. The pattern is defined by the user. • **false**. The pattern is predefined by Lenovo.
vendor	String	Vendor name of the adapter that is associated with this pattern
Additional attributes	varies	Remaining attributes vary depending on the adapter type and firmware level
uri	String	URI identifier for the exported pattern

Example


```
{
   "template_type" : "ExtendedPort",
   "template" : {
      "bdfList" : ["FC3172-8GbFCAdapter-1B00", "FC3172-8GbFCAdapter-1B01"],
      "chipset" : "FC3172",
      "description" : "Pattern created from server: Lenovo x240\n
                       Learned on: Jul 29, 2015 12:08:14 PM",
      "name" : "Learned-Extended_Port-2.3",
      "portbdf" : "FC3172-8GbFCAdapter-1B00",
      "portFunctions" : [],
      "protocol" : "fc",
      "type" : "ExtendedPort",
      "userDefined" : true,
      "vendor" : "QLogic",
      "FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1B00__AdapterSettings__asu__set" : true,
      "FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1B00__AdapterSettings__asu__set__
          ConnectionOption" : "Point To Point",
      "FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1B00__AdapterSettings__asu__set__
          DataRate" : "Auto",
      "FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1B00__AdapterSettings__asu__set__
```

```
    EnableHardLoopID" : "Disabled",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdapterSettings__asu__set__
    FCTape" : "Enabled",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdapterSettings__asu__set__
    FrameSize" : "2048",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdapterSettings__asu__set__
    ResetDelay" : "5"
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdapterSettings__asu__set__
    SpinUpDelay" : "Disabled",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set" : true,
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    ExecutionThrottledec" : "65535",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    InterruptDelayTimerdec" : "0",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    LinkDownTimeout" : "30",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    LIPFullLogin" : "Enabled",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    LIPReset" : "Disabled",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    LoginRetryCount" : "8",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    LunsPerTarget" : "256",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    OperationMode" : "Interrupt for every I\/O completion",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    PortDownRetryCount" : "30",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__AdvancedSettings__asu__set__
    TargetReset" : "Enabled",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__BootSettings__asu__set" : true,
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__BootSettings__asu__set__
    AdapterDriver" : "Disabled",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__BootSettings__asu__set__
    SelectiveLogin" : "Disabled",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__BootSettings__asu__set__
    SelectiveLunLogin" : "Disabled",
"FC3172-8GbFCAdapter__FC3172-8GbFCAdapter-1BOO__BootSettings__asu__set__
    WorldLogin" : "Disabled",
"ConfigDefinitions" : {
   "items" : [{
      "group" : [{
         "desc" : "QLogic HBA Driver Configuration",
         "group" : [{
            "mriName" : "AdapterSettings",
            "suppress-if" : "false",
            "name" : "Adapter Settings",
            "ID" : "AdapterSettings",
            "command" : [{
                  "desc" : "ASU",
                  "display" : "false",
                  "ID" : "asu",
                  "mriName" : "AsuAdapterSettings",
                  "name" : "ASU - Adapter Settings",
                  "option" : [{
                     "mriName" : "SetAdapterSettings",
                     "delim_data" : "true",
                     "desc" : "Modify Adapter Settings",
                     "name" : "Set Adapter Settings",
                     "ID" : "set",
                     "display" : "false",
```

```
            "option" : [{
                "desc" : "This setting forces the adapter to attempt to
                          use the ID specified in the Hard Loop ID field.",
                "dot_delim" : "true",
                "enumerate_data" : {
                   "choice" : [{
                       "default" : "true",
                      "label" : "Disabled",
                      "value" : "Disabled"
                   },
                   {
                      "label" : "Enabled",
                      "value" : "Enabled"
                    }]
                },
                "ID" : "EnableHardLoopID",
                "group_id" : "true",
                "mriName" : "EnableHardLoopID",
                "name" : "Enable Hard Loop ID",
                "no_delim_sign" : "true",
                "quote_data" : "true"
             },
             ...,
             {
                "desc" : "When this bit is set, the BIOS waits up to
                          two minutes to find the first drive.",
                "dot_delim" : "true",
                "enumerate_data" : {
                   "choice" : [{
                      "default" : "true",
                      "label" : "Disabled",
                      "value" : "Disabled"
                   },
                   {
                       "label" : "Enabled",
                       "value" : "Enabled"
                    }]
                 },
                 "ID" : "SpinUpDelay",
               "group_id" : "true",
               "mriName" : "SpinUpDelay",
               "name" : "Spin Up Delay",
               "no_delim_sign" : "true",
               "quote_data" : "true"
            }],
            "no_delim_sign" : "true"
         }]
      }]
   },
   ...,,
   {
      "mriName" : "BootSettings",
      "suppress-if" : "false",
      "name" : "Boot Settings",
      "ID" : "BootSettings",
      "command" : [{
         "display" : "false",
         "desc" : "ASU",
         "ID" : "asu",
         "mriName" : "AsuBootSettings",
         "name" : "ASU - Boot Settings",
```

```
            "option" : [{
               "delim_data" : "true",
               "desc" : "Modify Boot Settings",
               "display" : "false",
               "ID" : "set",
               "mriName" : "SetBootSettings",
               "name" : "Set Boot Settings",
               "option" : [{
               "desc" : "Specifies that the driver is to use the WWN
                         Database as a list of devices that the
                         adapter is permitted to login. Enable this
                         option to limit the adapter device discovery
                         to devices matching those in the WWN Database.",
               "dot_delim" : "true",
               "enumerate_data" : {
                  "choice" : [{
                     "default" : "true",
                     "label" : "Disabled",
                     "value" : "Disabled"
                  },
                  {
                     "label" : "Enabled",
                     "value" : "Enabled"
                  }]
               },
               "group_id" : "true",
               "ID" : "SelectiveLogin",
               "mriName" : "SelectiveLogin",
               "name" : "Selective Login",
               "no_delim_sign" : "true",
               "quote_data" : "true"
            },
            ...,
            {
               "desc" : "Used to enable the adapter driver. The driver
                         must be enabled to boot from a Fibre Channel disk.
                         The system will boot faster when the driver is
                         disabled.",
               "dot_delim" : "true",
               "enumerate_data" : {
                  "choice" : [{
                     "default" : "true",
                     "value" : "Disabled",
                     "label" : "Disabled"
                  },
                  {
                    "value" : "Enabled",
                    "label" : "Enabled"
                  }]
               },
               "group_id" : "true",
               "ID" : "AdapterDriver",
               "mriName" : "AdapterDriver",
               "name" : "Adapter Driver",
               "no_delim_sign" : "true",
               "quote_data" : "true"
            }],
            "no_delim_sign" : "true"
         }]
      }]
   }]
```

```
                "ID" : "FC3172-8GbFCAdapter-1B00",
                "mriName" : "FC3172-8GbFCAdapter-21000024FF35EA94",
                "name" : "FC3172-8Gb FC Adapter-21000024FF35EA94",
                "preceding_option_id" : "true",
             }]
             "ID" : "FC3172-8GbFCAdapter",
             "mriName" : "FC3172-8GbFCAdapter",
             "preceding_option_id" : "true",
             "name" : "FC3172-8Gb FC Adapter",
          }]
       },
       "uri" : "\/config\/template\/68"
    }
}
```

Extended ThinkSystem SR635/SR655 BIOS pattern attributes

The following attributes provide information about an extended-BIOS settings for ThinkSystem SR635 and SR655 server category pattern.

These attributes can be included in the request body for the POST /patterns method and the response body for the GET /patterns/*{id}*/includeSettings method.

The settings that are available are dynamic and vary from server to server and adapter to adapter. The following table lists examples of some possible settings.

For more information about extended ThinkSystem SR635/SR655 BIOS patterns, see Defining extended SR635/SR655 BIOS settings in the Lenovo XClarity Administrator online documentation.

Attributes	Type	Description
template_type	String	Type of category pattern. This value is always “ExtendedSR635_SR655BIOS.”
template	Array	Information about the system-information category pattern
type	String	Type of category pattern. This value is always “ExtendedSR635_SR655BIOS.”
name	String	Category-pattern name
description	String	Category-pattern description
uri	String	URI Identifier for the exported pattern
userDefined	String	Identifies whether the category pattern is user define or learned. This can be one of the following values. • **true**. The pattern is defined by the user. • **false**. The pattern is predefined by Lenovo.
Attributes	Array	Information about BIOS attributes that are specific to the manufacturer or provider
RegistryEntries	Object	Information about BIOS attributes and metadata
Attributes	Array of objects	

Attributes	Type	Description
AttributeName	String	
DefaultValue	Integer	
DisplayName	String	
HelpText	String	
LowerBound	Integer	
ReadOnly	Boolean	
ScalarIncrement	Integer	
Type	String	
UpperBound	Integer	
Dependencies	Array	List of dependencies of attributes on this component
Menus	Array	List of attributes menus and their hierarchy

Example

```
{
   "template_type": "ExtendedSR635_SR655BIOS",
   "template": {
      "name": "Learned-ExtendedSR635_SR655BIOS-1",
      "description": "Pattern created from server: 10.245.40.131\n
                      Learned on: Nov 12, 2019, 1:33:30 AM",
      "type": "ExtendedSR635_655BIOS",
      "RegistryEntries": {
         "Menus": [],
         "Attributes": [
            {
               "AttributeName": "Q00307 Preferred IO Device",
               "DefaultValue": 0,
               "DisplayName": "Preferred IO Device",
               "HelpText": "Specify the PCI bus, device, and function number of the target device
                            that will have high priority. This function is not intended to replace
                            Relaxed Ordering (RO) or ID-Based Ordering (IDO). For the 6-digit entry,
                            it is decoded as:  [23:16]=Bus Number in hex  [15: 8]=Device Number in hex
                            [ 7: 0]=Function Number in hex",
               "LowerBound": 0,
               "ReadOnly": false,
               "ScalarIncrement": 0,
               "Type": "Integer",
               "UpperBound": 65535
            },
            ...,
            {
               "AttributeName": "Q00186 Media detect count",
               "DisplayName": "Media detect count",
               "HelpText": "Number of times the presence of media will be checked. Use either +/- or
                            numeric keys to set the value.",
               "ReadOnly": false,
               "Type": "Integer",
               "UpperBound": 50,
               "LowerBound": 1,
               "ScalarIncrement": 1,
```

```
                "DefaultValue": 1
             }
          ],
          "Dependencies": []
       },
       "Attributes": {
          "QOOOO1 Boot Mode": "UEFI only",
          ...,
          "QOO186 Media detect count": 1
       }
    },
       "uri": "/config/template/46",
       "userDefined": true
}
```

/patterns/*{id}*

Use this REST API to retrieve information about a specific server pattern or deploy a server pattern to a target server. A *server pattern* represents pre-operating-system server configuration, including local storage, I/O adapter, SAN boot, and other baseboard management controller and UEFI firmware settings.

HTTP methods

GET, POST

GET /patterns/*{id}*

Use this method to return information about a specific server pattern or category pattern.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/patterns/{id}`

where *{id}* is the unique ID that was assigned when the server pattern was created. To obtain the pattern ID, use the GET /patterns method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
identifier	String	Always set to “id”
items	Array	Information about the pattern
bmcOnly	Boolean	Indicates whether the server pattern contains only IMM settings, including “System Information,” “Management Interface,” and “Extended BMC” category patterns. This can be one of the following values. • **true**. The server pattern contains only IMM settings. • **false**. The server pattern contains non-IMM settings.
containsM2	Boolean	Indicates whether the server pattern contains M.2 drive settings. This can be one of the following values. • **true**. The server pattern contains M.2 drive settings. • **false**. The server pattern does not contain M.2 drive settings.
description	String	Description of the pattern that was defined by the user when the pattern was created
formFactor	String	Form factor of the pattern. This can be one of the following values. • **a**. ThinkSystem SR635 or SR655 server • **f**. Flex System server • **f4sc**. 4 bay (2 node) scalable Flex system • **f8sc**. 8 bay (4 node) scalable Flex system • **r**. System x or NeXtScale server • **rc**. Scalable rack system
id	String	Patterns unique ID that was generated on creation
inUse	Boolean	Indicates whether pattern has been deployed to one or more servers. This can be one of the following values. • **true**. The pattern has been deployed. • **false**. The pattern has not been deployed.
name	String	Name of the pattern
nodeType	String	Type of server to which the pattern applies. This value is always “sysx.”
referencedBy	Array	List of patterns that reference this pattern. For server patterns, this attribute is always empty.
serverType	String	Server type If the type is unknown, this value is“ NA.”
type	String	Type of pattern. This value is always “Server .”
useCount	Integer	(Category patterns only) Number of server patterns that use this category pattern
uri	String	URI that is used to make individual REST API calls to the referenced object
userDefined	Boolean	Indicates whether the pattern is user-defined or predefined. This can be one of the following values. • **true**. The server pattern is user-defined. • **false**. The server pattern is predefined.
label	String	Always set to “label”

The following example is returned for a server pattern if the request is successful.

```
{
   "identifier": "id",
   "items": [{
      "bmcOnly": false,
      "containsM2": false,
      "description": "",
      "formFactor": "f",
      "id": "46",
      "inUse": true,
      "name": "asdfasdf",
      "nodeType": "sysx",
      "referencedBy": [],
      "serverType": "NA",
      "type": "Server",
      "uri": "/config/template/46",
      "userDefined": true
   }],
   "label": "name"
}
```


The following example is returned for a system information category pattern if the request is successful.


```
{
   "identifier": "id",
   "items": [{
      "bmcOnly": false,
      "containsM2": false,
      "description": "",
      "id": "46",
      "inUse": false,
      "name": "sysInfo",
      "referencedBy": [],
      "serverType": "NA",
      "type": "SystemInfo",
      "uri": "/config/template/46",
      "useCount": 2,
      "userDefined": true
   }],
   "label": "name",
}
```


POST /patterns/*{id}*

Use this method to deploy a server pattern to a target server.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/patterns/{id}`

where *{id}* is the unique ID that was assigned when the server pattern was created. To obtain the pattern ID, use the GET /patterns method.

Request body

None

Request body

Attributes	Required / Optional	Type	Description
endpointIds	Required for empty Flex chassis bays and placeholder chassis bays Optional for Flex System servers	Array of strings	A list of one or more UUIDs for the target servers, empty chassis bay, or placeholder chassis bay. To obtain UUIDs for deployable target servers according to their pattern and profile, use the GET /config/target/*{id}* method.
restart	Required	String	Identifies when to activate the configurations. This can be one of the following values. • **defer**. Activate management-controller settings but do not restart the server. UEFI and server settings are activated after the next restart of the server. • **immediate**. Activate all settings and restart the server immediately. • **pending**. Generate a profile for the server with the settings for review, but do not activate settings on the server. To activate the settings, you must manually activate the server profile and restart the server.
uuid	Required for rack and tower servers Optional for Flex System servers	Array of strings	A list of one or more UUIDs for the target servers. To obtains the UUIDs for servers, use the GET /nodes method.

The following example deploys a server pattern to two Flex System Placeholder chassis empty bays using deferred activation.

```
{
    "endpointIds": [
        "phc-efebecbc232a4e418081862589dde160_bay3",
        "phc-efebecbc232a4e418081862589dde160_bay4"
     ],
    "restart": "defer"
}
```

The following example deploys a server pattern to one System x rack server using immediate activation.

```
{
    "uuid": ["1B54B9AEFCE04D5E820C0B6310D03590"],
    "restart": "immediate"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
identifier	String	Always set to “id”
label	String	Always set to “label”
items	Array	Information about each server and category pattern
endpointIds	Array	UUIDs of all targeted servers
endpointNames	Array	Names of all targeted servers
jobName	String	Name of the deploy job created
jobRecordID	String	ID of the deploy job
locationIds	Array	Location IDs for empty bays or placeholder bays that are targeted
locationIdsFailed	Array	Location IDs for targeted bays for which deployment failed
locationNames	Array	Names of all targeted empty bays
message	Null	Currently not used. This value should always be “null.”
redeployedNodeUuids	Array	UUIDs of all servers targeted for redeployment
uuidsFailed	Array	UUIDs of targeted servers for which deployment failed

The following example is returned if the request is successful.

```
{
     identifier: "id"
     label: "id"
     items: [1]
          0:  {
               endpointIds: [0]
               endpointNames: [0]
               jobName: "Server Profile activation: Apr 9, 2015"
               jobRecordId: "48cf5296-9b6a-454e-80ad-b88b98f11b38"
               locationIds: [2]
                    0:  "phc-efebecbc232a4e418081862589dde160_bay3"
                    1:  "phc-efebecbc232a4e418081862589dde160_bay4"
                    ...
```

```
                locationIdsFailed: [0]
                locationNames: [2]
                      0:  "Bay3"
                      1:  "Bay4"
                      ...
                redeployedNodeUuids: [0]
                message: null
                uuidsFailed: [0]
          }
          ...
     ...
}
```

/patterns/*{id}*/includeSettings

Use this REST API to export patterns from the Lenovo XClarity Administrator.

HTTP methods

GET

GET /patterns/*{id}*/includeSettings

Use this method to export the properties for an existing server pattern.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/patterns/{id}/includeSettings`

where *{id}* is the unique ID that was assigned when the server pattern was created. To obtain the pattern ID, use the GET /patterns method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The server pattern includes the category patterns that are reference by the server pattern. The format of the response changes depending on the type and number of referenced category patterns (for example, system-information or port patterns).

Attributes	Type	Description
server_template	Array of objects	Information about the server pattern
adapterSettings	Array of objects	Information about adapter settings that are defined in the server pattern
adapters	Array of strings	List of adapters that were added to this pattern
ethAddressDomain	String	ID of the Ethernet address range that is used in this pattern
ethAddressPool	String	ID of the Ethernet address pool that is used in this pattern
fcAddressDomain	String	ID of the Fibre Channel address range that is used in this pattern
fcAddressPool	String	ID of the Fibre Channel address pool that is used in this pattern
formFactor	String	Form factor. This can be one of the following values. • **a**. ThinkSystem SR635 or SR655 server • **f**. Flex System server • **f4sc**. 4 bay (2 node) scalable Flex system • **f8sc**. 8 bay (4 node) scalable Flex system • **r**. System x or NeXtScale server • **rc**. Scalable rack system
ioAddressingMode	String	Type of I/O addressing that is used. This can be one of the following values. • **burned**. Burned in Addresses. Use existing World Wide Name (WWN) and Media Access Control (MAC) addresses that are provided with the adapter from manufacturing. • **virtual**. Virtual Addresses. Use virtual I/O adapter addressing to simplify the management of LAN and SAN connections to speed deployment and automatic failover by virtualizing WWN and MAC addresses.When virtual addressing is enabled, both Ethernet and Fibre Channel addresses are allocated by default regardless of defined adapters. You can choose the pool from which Ethernet and Fibre Channel addresses are allocated. Virtual addressing is supported for only compute nodes. Rack servers are not supported.
bootSettings	Array of objects	Information about the boot methods that are defined in the server pattern
bootConfig	String	Selected boot configuration type. This value is always “specify.”
bootMode	String	Boot mode set in the pattern. This can be one of the following values. • **UEFI Only**. Select this option to configure a server that supports the Unified Extensible Firmware Interface (UEFI). If you are booting UEFI enabled operating systems, this option might shorten boot time by disabling legacy option ROMs. • **UEFI and Legacy**. Select this option to configure a server to attempt to boot using UEFI first. If there is an issue, the server attempts to boot in legacy mode. Select this option only if you are booting non-UEFI enabled operating systems. • **Legacy Only**. Select this option if you are configuring a server to boot an operating system that requires legacy (BIOS) firmware. Select this option only if you are booking non-UEFI enabled operating systems. • **null**. To keep the existing settings on the target server, leave this attribute blank. No changes to the boot order are made when the pattern is deployed.

Attributes	Type	Description

bootOrderTable	Array of objects	Boot order, for example:
		[{
		"order" : 0,
		"device" : "*NONE",
		"option" : "Embedded Hypervisor"
		}, {
		"order" : 1,
		"device" : "Disk Drive 0",
		"option" : "Disk Drive"
		}, {
		"order" : 1,
		"device" : "*NONE",
		"option" : "CD\/DVD Rom"
		}, {
		"order" : 2,
		"device" : "*NONE",
		"option" : "PXE Network"
		}]

bootWoLTable	Array of objects	Wake-on-LAN boot order when the boot mode is set to “Legacy Only”, for example:
		[{
		"order" : 0,
		"device" : "*NONE",
		"option" : "CD\/DVD Rom"
		}, {
		"order" : 1,
		"device" : "Disk Drive 0",
		"option" : "Disk drive"
		}, {
		"order" : 2,
		"device" : "*NONE",
		"option" : "PXE Network"
		}]

Attributes	Type	Description

learnedBootOptions	Array of objects	Boot-order properties that are dynamically learned from the system when the pattern was created from an existing server. These values vary depending on the learned properties, for example:
		"learnedBootOptions" : [{
		"value" : "Diagnostics",
		"label" : "Diagnostics"
		}, {
		"value" : "IMM1",
		"label" : "IMM1"
		}, {
		"value" : "IMM2",
		"label" : "IMM2"
		}, {
		"value" : "SAS",
		"label" : "SAS"
		}, {
		"value" : "VNIC1",
		"label" : "VNIC1"
		}, {
		"value" : "VNIC2",
		"label" : "VNIC2"
		},
		...
		{
		"value" : "DSA",
		"label" : "DSA"
		}]

learnedWoLBootOptions	Array of objects	Wake-on-LAN boot-order properties that are dynamically learned from the system when the pattern was created from an existing server. These values vary depending on the learned properties, for example:
		"learnedWoLBootOptions" : [{
		"value" : "Diagnostics",
		"label" : "Diagnostics"
		}, {
		"value" : "IMM1",
		"label" : "IMM1"
		}, {
		"value" : "IMM2",
		"label" : "IMM2"
		}, {
		"value" : "SAS",
		"label" : "SAS"
		}, {
		"value" : "VNIC1",
		"label" : "VNIC1"
		}, {
		"value" : "VNIC2",
		"label" : "VNIC2"
		},
		...
		{
		"value" : "DSA",
		"label" : "DSA"
		}]

sanBootTable	Array of objects	Information about the SAN boot device

Attributes	Type	Description
device	String	Device label for the selected SAN boot device (for example, I/O Adapter 1 - Port 1)
devicePort	Integer	Port on the adapter that is selected for booting from SAN
deviceSlot	Integer	Slot number of the adapter that is selected for booting from SAN
deviceType	String	Device type that is selected for SAN boot. This can be one of the following values. • **adapter** • **lom**
functionNumber	String	Function number (virtual port) that is selected for booting from the SAN. If port virtualization is not enabled (for example, on a Fibre Channel adapter), this value is “0.”
option	String	This value is always “Fibre Channel (SAN).”
order	Integer	Order in which to prioritize this entry in the SAN boot order. This can be one of the following values. • **0**. First • **1**. Second • **2**. Third • and so on
target	String	Selected boot target. This can be one of the following values. • **primary** • **secondary**
template	String	ID of the associated Fibre Channel boot target pattern
description	String	Description of the server pattern
formFactor	String	Form factor. This can be one of the following values. • **a**. ThinkSystem SR635 or SR655 server • **f**. Flex System server • **f4sc**. 4 bay (2 node) scalable Flex system • **f8sc**. 8 bay (4 node) scalable Flex system • **r**. System x or NeXtScale server • **rc**. Scalable rack system
name	String	Name of the server pattern
nodeType	String	Type of server to which the pattern applies. This value is always “sysx.”
storageSettings	Array of objects	Information about the storage settings that are defined in the server pattern
storageAttrs	Array of objects	List of storage settings for each volume type that is defined by this pattern, when **storageSelect** is set to “Specify.”
accessPolicy	String	Access policy. This can be one of the following values. • **Blocked** • **Read only** • **Read Write**
cachePolicy	String	Cached policy. This can be one of the following values. • **Unchanged** • **Enabled** • **Disabled**

Attributes	Type	Description
controllerType	String	RAID controller type. This can be one of the following values. • **M2SATASD** • **SDCard** • **RaidAdapter** • **IntelOptaneDCPMM**
controllerSlot	Integer	PCI slot number of the RAID controller
diskDriveBay	String	Number of the bay where the disk drive is located, separated by a colon (for example, 0:1:2). For RAID level 10, 50, 60, and 00, each span is separated by a comma (for example, 0:1:2,3:4:5).
diskType	String	Type of disk drives in the device. This can be one of the following values. • **None** • **HDDSSD** • **M2-SD-CARD**. M.2 storage adapter • **SDCARD**. SSD storage adapter
hotspareDriveBay	String	Number of the bay where the host-spare disk drive is located, separated by a colon (for example, 6:7)
initStatus	String	Initialization status. This can be one of the following values. • **No Initialization** • **Fast Initialization** • **Full Initialization**
ioPolicy	String	I/O policy. This can be one of the following values. • **Direct IO** • **Cached IO**
memoryModePercentage	Integer	(Intel Optane™ DC Persistent Memory DIMMs only) Percentage of total capacity to be used as memory mode. This value can be from 0 - 100.
numDrives	Integer	Number of drives in the device
numHotspares	Integer	Number of host-spare drives in the device
percentageRemaining-Thresholds	Integer	(Intel Optane DC Persistent Memory DIMMs only) Warning threshold for the remaining life of the DIMM, as a percentage value of the factory expected life span. This value can be from 2 - 99.
persistentMemoryType	String	(Intel Optane DC Persistent Memory DIMMs only) Persistent memory type. This can be one of the following values. • **App Direct** • **App Direct Not Interleaved**
raidLevel	String	RAID level. This can be one of the following values. • **RAID 0**. Striping • **RAID 1**. Mirroring • **RAID 5**. Distributed dual-parity • **RAID 6**. Striping with-parity • **RAID 10**. Disk mirroring and disk striping (1+0) • **RAID 50**. Distributed parity and disk striping (5+0) • **RAID 60**. Distributed dual-parity and disk striping (6+0) • **RAID 00** **Note:** RAID level 0, 1, or 5 are supported on all serves. RAID level 6, 10, 50, 60, and 00 are supported only on ThinkSystem servers with XCC version 2.1 and later. (ThinkSystem SR950 requires XCC version 1.4 or later).

Attributes	Type	Description
raidVolumeName	String	RAID volume name
readPolicy	String	Read policy. This can be one of the following values. • **Always Read Ahead** • **No Read Ahead**
stripeSize	String	Stripe size. This can be one of the following values. • **8K** • **16K** • **32K** • **64K** • **128K** • **256K** • **512K** • **1M**
writePolicy	String	Write policy. This can be one of the following values. • **Always Write Back** • **Write Back with BBU** • **Write Through**
storageSelection	String	Store configuration. This can be one of the following values. • **Keep Existing**. Keep existing storage configuration on target. Choose this option to use the storage configuration that is already in place on the target server. • **Specify**. Specify storage configuration. Choose this option to specify the drive type, RAID configuration, and number of drives that are installed in the server. This option is supported only if you are deploying the pattern to one or more servers that do not have existing RAID configurations. • **Disable**. Disable local disk drive. If you are deploying a pattern to a Flex System x240 Compute Node, choose this option to disable the on-board storage controller and storage option ROM (both UEFI and Legacy). Disabling the local disk drive decreases the overall boot time when booting from SAN.
serverType	String	Server type. This can be one of the following value. • **AMI**. The server pattern is learned from a Thinksystem SR635 or SR655 server. • **IMMv3**. The server pattern is learned from Thinksystem. • **IMMv2**. The server pattern is learned from a System X or Flex System server that contains an IMM2. • **NA**. The server pattern is created from scratch.
templates	Array of objects	List of category patterns that are referenced by the server pattern
id	String	ID of the category pattern
type	String	Type of category pattern. This can be one of the following values. • **Server** • **Management** • **SystemInfo** • **DevicesAndIOPorts** • **ExtendedSR635_655BIOS** • **ExtendedIMM** • **ExtendedPort** • **ExtendedUEFI** • **FibreChannel**

Attributes	Type	Description
type	String	The type of server pattern. This value is always “Server.”
userDefined	Boolean	Indicates whether the server pattern is user-defined or predefined. This can be one of the following values. • **true**. The server pattern is user-defined. • **false**. The server pattern is predefined.
sub_templates	Array	Information about each category pattern that is referenced by this server pattern. The attributes vary depending on the category pattern type. For information about the attributes, see the following topics. • System-information pattern attributes • Management-information pattern attributes • Device and I/O ports pattern attributes • Port pattern attributes • Fibre Channel boot-target pattern attributes • Extended management-controller pattern attributes • Extended-UEFI pattern attributes • Extended-port pattern attributes • Extended ThinkSystem SR635/SR655 BIOS pattern attributes
template_type	String	Type of template to be exported. The value is always “server_template.”

The following example is returned if the request is successful.


```
{
   "server_template": {
      "adapterSettings": {
         "adapters": [{
            "adapterId": "adapter:17",
            "controllers": [{
               "id": "adapterSetting:69:controller:1",
               "ports": [{
                  "id": "adapterSetting:69:controller:1:port:1",
                  "portNumber": 1,
                  "templateId": "portVirtualizationPattern:70",
                  "templateType": "PortVirtualization"
               },
               {
                  "id": "adapterSetting:69:controller:1:port:2",
                  "portNumber": 2,
                  "templateId": "portVirtualizationPattern:71",
                  "templateType": "PortVirtualization"
               }],
               "controllerNumber": 1
            }],
            "id": "adapterSetting:69",
            "formFactor": "f",
            "nodeNumber": 1,
            "slotNumber": 0
         },
         {
            "adapterId": "adapter:6",
            "controllers": [{
               "controllerNumber": 1"id": "adapterSetting:72:controller:1",
               "ports": [{
                  "id": "adapterSetting:72:controller:1:port:1",
                  "portNumber": 1,
                  "templateId": "68",
                  "templateType": "ExtendedPort"
```

```
            },
            {
                "id": "adapterSetting:72:controller:1:port:2",
                "portNumber": 2,
                "templateId": "68",
                "templateType": "ExtendedPort"
            }],

        }],
        "formFactor": "f",
        "id": "adapterSetting:72",
        "nodeNumber": ,
        1"slotNumber": 1
    }],
    "ethAddressDomain": "*NONE",
    "ethAddressPool": "*NONE",
    "fcAddressDomain": "*NONE",
    "fcAddressPool": "*NONE""formFactor": "f",
    "ioAddressingMode": "burned",

},
"bootSettings": {
    "bootConfig": "specify",
    "bootMode": "Legacy Only",
    "bootOrderTable": [{
        "order": 0,
        "device": "*NONE",
        "option": "Embedded Hypervisor"
    },
    ....,
    {
        "order": 3,
        "device": "*NONE",
        "option": "PXE Network"
    }],
    "bootWoLTable": [{
        "order": 0,
        "device": "*NONE",
        "option": "CD\/DVD Rom"
    },
    ...,
    {
        "order": 2,
        "device": "*NONE",
        "option": "PXE Network"
    }],
    "learnedBootOptions": [{
        "value": "Diagnostics",
        "label": "Diagnostics"
    },
    ...,
    {
        "value": "DSA",
        "label": "DSA"
    }],
    "learnedWoLBootOptions": [{
        "value": "IMM1",
        "label": "IMM1"
    },
    ...,
    {
```

```
            "value": "DSA",
            "label": "DSA"
         }],
         "localStorageDisabled": false,
         "sanBootTable": []
      },
      "description": "Pattern created from server: Lenovo x240\n
                           Learned on: Jul 29, 2015 12:08:14 PM",
      "formFactor": "f",
      "name": "Learn x240",
      "nodeType": "sysx",
      "storageSettings": {
         "storageAttrs" : [{
            "accessPolicy" : "Read Write",
            "cachePolicy" : "Unchanged",
            "diskType" : "None",
            "initStatus" : "No Initialization",
            "ioPolicy" : "Direct IO",
            "numDrives" : 2,
            "numHotspares" : 0,
            "raidLevel" : "RAID 1",
            "readPolicy" : "No Read Ahead",
            "stripeSize" : "64k",
            "writePolicy" : "Write Through",
         }
         {
            "controllerType": "IntelOptaneDCPMM",
            "memoryModePercentage ": 50,
            "percentageRemainingThresholds": 10
            "persistentMemoryType": "App Direct",
         }],
         "storageSelection": "Specify"
      },
      "templates": [{
         "id": "68",
         "type": "ExtendedPort"
      },
      ...,
      {
         "id": "66",
         "type": "ExtendedPort"
      }],
      "type": "Server",
      "userDefined": true,

   },
   "sub_templates": {
      "template": {
         "contact": "contact",
         "description": "Pattern created from server: Lenovo x240\n
                              Learned on: Jul 29, 2015 12:08:14 PM",
         "location": "location",
         "name": "Learned-System_Info-2",
         "systemName": {
            "autogen": "Disable",
            "hyphenChecked": false
         },
         "type": "SystemInfo",
         "uri": "\/config\/template\/61",
         "userDefined": true
      },
```

```
      "template_type": "SystemInfo"
   },
   {
      "template_type": "Management",
      "template": {
         "description": "Pattern created from server: Lenovo x240\n
                         Learned on: Jul 29, 2015 12:08:14 PM",
         "domainNameSystem": {
            "domainName": "",
            "domainNameSource": "dhcp",
            "dynamicDNS": "enabled"
         },
         "hostName": {
            "autogen": "Disable",
            "hyphenChecked": false
         },
         "interfaceSettings": {
            "ethInterface": 0,
            "maximumTransmissionUnit": "1500"
         },
         "managementIPAddress": {
            "ipV4Settings": "No Change",
            "ipV6Settings": "No Change"
         },
         "name": "Learned-Management-2",
         "portAssignments": {
            "cimhttpPort": "5988",
            "cimhttpsPort": "5989""httpPort": "80",
            "httpsPort": "443",
            "remotecontrolPort": "3900",
            "sshcliPort": "22",
            "snmpagentPort": "161",
            "snmptrapsPort": "162",
            "telnetcliPort": "23",

         },
         "type": "Management",
         "userDefined": true,
         "uri": "\/config\/template\/62"
      }
   },
   ...,
   "template_type": "server_template"
}
```


/profiles

Use this REST API to retrieve information about all server profiles that are defined in Lenovo XClarity Administrator, or to rename one or more server profiles. A *server profile* is an instance of a server pattern that is applied to a specific server. The server profile contains server-specific configuration, including assigned name, IP addresses, and MAC addresses.

HTTP methods

GET, PUT

GET /profiles

Use this method to return information about server profiles from the Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/profiles`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
identifier	String	Always set to "id"
label	String	Always set to "id"
items	Array of objects	Information about each server profile
addressPresent	Boolean	Identifies whether address pools are used. This can be one of the following values. • **true**. Address pools are used. • **false**. Address pools are not used.
bayId	String	ID of the bay in the chassis in which the server is installed, if applicable For a rack server, this value is empty.
chassisName	String	Chassis in which the server is installed, if applicable For a rack server, this value is empty.
complianceStatus	String	Compliance status. This can be one of the following values. • **valid** : Server settings are compliant with the profile • **invalid** : Server settings are Non-compliant with the profile • **none** : Compliance has not been calculated because pattern is still activated, pending or inactive
externalId	String	ID of the server or bay to which the profile is deployed
id	String	Unique ID of the profile
managementPatternPresent	Boolean	Identifies whether a management-interface pattern is used. This can be one of the following values. • **true**. A management-interface pattern is used. • **false**. A management-interface pattern is not used.

Attributes		Type	Description
	profileName	String	Name of the server profile
	profileStatus	String	Current status of the profile. This can be one of the following values. • **ASSIGNED**. The profile is assigned to the server. • **UNASSIGNED**. The profile in not assigned to any server. • **PENDING_ACTIVATION**. The profile is created and targeted to a server but has not been activated yet. • **ACTIVATING**. The profile is currently being activated on the targeted server • **ERROR_ACTIVATING**. There was an error while activating the profile on the targeted server.
	rackID	String	ID of the rack that contains the server to which the profile is deployed
	serverName	String	Name of the server to which the profile is deployed
	subBayId	String	ID of the sub-bay in the chassis in which the server is installed, if the server is a Flex System x222 Compute Node For all other servers, this value is empty.
	templateID	String	ID of the server pattern that was used to create the profile
	templateName	String	Name of the server pattern that was used to create the profile
	type	String	Internal use only
	unit	Integer	ID of the unit that contains the server to which the profile is deployed
	uuid	String	UUID of the server to which the profile is deployed

The following example is returned if the request is successful.


```
{
   "identifier": "id",
   "label": "id",
   "items": [{
      "addressPresent": false,
      "bayId": "12",
      "chassisName": "SN#Y030BG21E01C",
      "complianceStatus": "VALID",
      "managementPatternPresent": false,
      "externalId": "97C28DF7541B4657AB59A26C2640A0A3_bay12",
      "id": "50",
      "profileName": "flex noop-profile4",
      "profileStatus": "ASSIGNED",
      "rackId": "",
      "serverName": "AT-C4022-empt0",
      "subBayId": null,
      "templateId": "46",
      "templateName": "flex noop",
      "type": "root",
      "unit": 0,
      "uuid": "64AADF17B64D11E499180090FA8BC90A"
   },
   ...,
   {
      "addressPresent": false,
      "bayId": "13",
      "chassisName": "SN#Y030BG21E01C",
      "complianceStatus": "NONE",
      "externalId": "97C28DF7541B4657AB59A26C2640A0A3_bay13",
      "id": "49",
```

```
      "managementPatternPresent": false,
      "profileName": "flex noop-profile5",
      "profileStatus": "ASSIGNED",
      "rackId": "",
      "serverName": "IB-C4054R-F5054",
      "subBayId": null,
      "templateId": "46",
      "templateName": "flex noop",
      "type": "root",
      "unit": 0,
      "uuid": "65E7D38AA6D811E298BD0090FA1C0DCE"
   }]
}
```

PUT /profiles

Use this method to rename one or more server profiles.

Note: This REST API requires Lenovo XClarity Administrator v4.1.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/profiles`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
profileId	Required	String	Profile ID
profileName	Required	String	New profile name

The following example renames two server profiles.

```
[{
   "profileId": "4753",
   "profileName": "ThinkSystemSR550-124 "
},
{
   "profileId": "4754",
   "profileName": "ThinkSystemSR550-253 "
}]
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
profileId	String	ID of the server profile that was renamed
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **service_error_profile_not_found.** The profile ID is not valid. • **service_error_name_in_use.** A profile with the same name already exists.

The following example is returned if the request is successful.

```
[{
   "profileId": "4753",
   "result": "success"
},
{
   "profileId": "4754",
   "result": "success"
}]
```

/profiles/*{id}*

Use this REST API to retrieve information about a specific server profile, deploy a server profile to a target server, or delete a server profile. A *server profile* is an instance of a server pattern that is applied to a specific server. The server profile contains server-specific configuration, including assigned name, IP addresses, and MAC addresses.

HTTP methods

GET, POST, DELETE

GET /profiles/*{id}*

Use this method to return information about a specific server profile.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/profiles/{id}`

where *{id}* is the unique ID for the server profile that was assigned when the server pattern was deployed. To obtain the server profile ID, use the GET /profiles method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
addressPresent	Boolean	Indicates whether any address pools are present. This can be one of the following values. • **true** . The address pools are present. • **false**. The address pools are present.
commands	Array	All the commands that are generated by the profile
complianceStatus	String	Compliance status. This can be one of the following values. • **VALID**. Server settings are compliant with the profile • **INVALID**. Server settings are Non-compliant with the profile • **NONE**. Compliance has not been calculated because pattern is still activated, pending or inactive
complianceTimestamp	String	Timestamp when the compliance status was set to **VALID**. This timestamp is specified using ISO-8601 format (for example, 2019-05-02T19:28:14.000Z). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
displayName	String	Displayed name of the profile
dynamicProperties	String	Internal use only
endpointId	String	ID of the device the profile is deployed to
endpointType	String	Type of device the profile is deployed to. This can be one of the following values. • **LOCATION**. A placeholder bay or Flex System server in a chassis • **RACK**. A rack or tower server.
externalId	String	The ID of the device the profile is deployed to.
forScalableNode	Boolean	Indicates whether the server is in a scalable system. This can be one of the following values. • **true**. This is a scalable system. • **false**. This is not a scalable system.
forScalablePrimaryNode	Boolean	Indicates whether the server is the primary node in the scalable system. This can be one of the following values. • **true**. This is the primary node. • **false**. This is not the primary node.
forScalableSecondaryNode	Boolean	Indicates whether the profile is for a secondary node in a scalable system. This can be one of the following values. • **true** . The profile is for a secondary node • **false**. The profile is for a primary node.

Attributes	Type	Description
ID	String	ID of the profile
managementPatternPresent	Boolean	Indicates whether a management interface pattern is present. This can be one of the following values. • **true** . The management interface pattern is present. • **false**. The management interface pattern is not present.
name	String	Name of the profile
primaryProfileID	String	If this is a secondary profile, this is a string that is the primary profiles ID
profilePath	Array of strings	Location where the server profile is assigned. The following strings are returned in this order. 1. The chassis compute-node bay location where the server is installed. 2. The UUID or location ID of the target server 3. For internal use only 4. For internal use only 5. For internal use only
rackId	String	ID of the rack that contains the server that the profile is deployed to
secondaryProfileIDs	Array	IDs of any secondary profiles created as part of a scalable deploy
serverTemplateId	String	ID of the server pattern used to build the profile
templateId	String	ID of the server pattern used to build the profile
unit	Integer	ID of the unit that contains the server that the profile is deployed to

The following example is returned if the request is successful.


```
{
   "addressPresent": false,
   "commands": [
      "#11/06/2017 3:49:51 PM",
      "asu set UEFI.DevicesandIOPorts.RemoteConsole \"Auto\"",
      "asusetUEFI.DevicesandIOPorts.SerialPortSharing\"Disable\"",
      "asusetUEFI.DevicesandIOPorts.SerialPortAccessMode\"Disable\"",
      "asusetUEFI.DevicesandIOPorts.LegacyOptionROMDisplay\"COM Port 1\"",
      "asusetUEFI.DevicesandIOPorts.COMPort1\"Enable\"",
      "asusetUEFI.DevicesandIOPorts.Com1BaudRate\"115200\"",
      "asusetUEFI.DevicesandIOPorts.Com1DataBits\"8\"",
      "asusetUEFI.DevicesandIOPorts.Com1Parity\"None\"",
      "asusetUEFI.DevicesandIOPorts.Com1StopBits\"1\"",
      "asusetUEFI.DevicesandIOPorts.Com1TerminalEmulation\"ANSI\"",
      "asusetUEFI.DevicesandIOPorts.Com1ActiveAfterBoot\"Disable\"",
      "asusetUEFI.DevicesandIOPorts.Com1FlowControl\"Disable\"",
      "asusetUEFI.DevicesandIOPorts.COMPort2\"Enable\"",
      "asusetUEFI.DevicesandIOPorts.Com2BaudRate\"115200\"",
      "asusetUEFI.DevicesandIOPorts.Com2DataBits\"8\"",
      "asusetUEFI.DevicesandIOPorts.Com2Parity\"None\"",
      "asusetUEFI.DevicesandIOPorts.Com2StopBits\"1\"",
      "asusetUEFI.DevicesandIOPorts.Com2TerminalEmulation\"ANSI\"",
      "asusetUEFI.DevicesandIOPorts.Com2ActiveAfterBoot\"Disable\"",
      "asusetUEFI.DevicesandIOPorts.Com2FlowControl\"Disable\"",
      "portcfg-b115200"
   ],
   "complianceStatus": "Invalid",
   "complianceTimestamp": "2022-04-11T18:50:00Z",
   "displayId": "56",
```

```
   "displayName": "flex non-compliant-profile1",
   "dynamicProperties": {},
   "endPointId": "97C28DF7541B4657AB59A26C2640A0A3_bay7",
   "endPointType": "LOCATION",
   "externalId": "97C28DF7541B4657AB59A26C2640A0A3_bay7",
   "forScalableNode": false,
   "forScalablePrimaryNode": false,
   "forScalableSecondaryNode": false,
   "ID": "56",
   "managementPatternPresent": false,
   "name": "flex non-compliant-profile1",
   "primaryProfileID": "",
   "profilePath": ["bay07", "97C28DF7541B4657AB59A26C2640A0A3", "system01", "pod01",
                   "datacenter01"],
   "rackId": "",
   "secondaryProfileIDs": [],
   "serverTemplateId": "55",
   "templateId": "55",
   "unit": 0
}
```


PUT /profiles/*{id}*

Use this method to modify the properties of a specific profile.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/profiles/{id}`

where *{id}* is the unique ID of the server profile that was assigned when the server pattern was deployed. To obtain the server profile ID, use the GET /profiles method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
profileName	Optional	String	New server profile name The profile name must not include these characters & % < >/ “ Ensure that the name you choose is unique. You cannot have two profiles with the same name.
complianceStatus	Optional	String	Compliance status. This can be one of the following values. • **VALID**. Server settings are compliant with the profile. • **INVALID.** Server settings are not compliant with the profile. This can be set only if **complianceStatus** is valid and was set to valid by user.

The following example modifies the name of an existing profile.

```
{
   "profileName": "myNewProfileName",
   "complianceStatus": "VALID"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body. The error message will mention if the status can be set to compliant without redeploying the configuration
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

POST /profiles/*{id}*

Use this method to activate a profile on a target system by assigning an inactive server profile to a target server or redeploying a server profile that is active, pending, or failed activation.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/profiles/{id}`

where *{id}* is the unique ID of the server profile that was assigned when the server pattern was deployed. To obtain the server profile ID, use the GET /profiles method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
restart	Required	String	Indicates when to restart the server to activate the profile. This can be one of the following values. • **immediate**. Restart the server and completes the activation immediately. • **defer**. Does not restart the server. Activate is completed after the server is manually restarted.
uuid	Required if the server profile is inactive (not assigned); otherwise, optional	String	For a rack or tower server, this is the UUID of the target server. For a Flex System server, this is the location ID of the target server. **Important:** An *assigned server profile* (in the active, pending, or failed activation state) can be redeployed only to the server to which the profile is currently assigned. If you do not specify the **uuid** attribute for an assigned server profile, the target-server UUID is retrieved from the server profile. If you specified the **uuid** attribute for an assigned server profile, the specified UUID must match the UUID of the current target server.

The following example activates a profile on the target system and restart the server to activate the profile.

```
{
   "restart": "defer",
   "uuid": "1B54B9AEFCE04D5E820C0B6310D03590_bay3"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /profiles/*{id}*

Use this method to remove a server profile from Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/profiles/{id}`

where *{id}* is the unique ID of the server profile that was assigned when the server pattern was deployed. To obtain the server profile ID, use the GET /profiles method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
message	String	Message

The following example is returned if the request is successful.

```
{
   "message": "service_operational"
}
```

/profiles/status

Use this REST API to retrieve information about the server-profile status for specific servers.

HTTP methods

GET

GET /profiles/status

Use this method to return information about the server-profile status for specific server.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/profiles/status
```

Query parameters

Parameters	Required / Optional	Description
uuids=*{uuid_list}*	Required	List of server UUIDs, separated by a comma

The following example retrieves the profile status for two servers.

```
GET https://192.0.2.0/profiles/status
?uids=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
identifier	String	Always set to “uuid”
items	Array of objects	Configuration status for each server

Attributes	Type	Description
activationStatus	String	Activation status. This can be one of the following values. • **UNKNOWN**. Activation status is in an unknown state. • **RUNNING**. Profile activation is in progress. • **PENDING**. Profile activation is pending. • **COMPLETED**. Profile activation is complete. • **TERMINATED**. Profile activation process was terminated before it completed. • **CONFIGERROR**. Cannot retrieve the configuration definitions from the server. • **LDAPERROR**. Cannot connect to the XClarity Administrator LDAP server.
complianceStatus	String	Compliance status. This can be one of the following values. • **VALID**. Server settings are compliant with the assigned server profile • **INVALID**. Server settings are not compliant with the assigned server profile. • **NONE**. Compliance is not calculated because the pattern is still being activated, pending or inactive.
configStatus	String	Configuration status. This can be one of the following values. • **NO_PROFILE**. A profile has not been assigned to this server. • **PROFILE_USE_NOT_SUPPORTED**. Configuration patterns is not supported for the server. • **DEPLOY_STARTED**. Configuration-Pattern deployment is started. • **BUILDING_PROFILE**. The server profile is being built. • **SAVING_PROFILE**. The server profile is being saved. • **PENDING_PROFILE**. The server profile is pending activation. • **ACTIVATING_PROFILE**. The server profile is being activated. • **ERROR_CREATING_PROFILE**. The server profile cannot be created. • **ERROR_ACTIVATING_PROFILE**. The server profile cannot be activated. • **RESTARTING**. The server is restarting. • **PROFILE_ACTIVATED**. The server profile is activated.
serverName	String	Server name
serverProfileId	String	ID of the server profile that is associated with this server
serverProfileName	String	Name of the server profile that is associated with this server
serverTemplateId	String	ID of the server pattern that was used to create the server profile that is associated with this server
serverTemplateName	String	Name of the server pattern that was used to create the server profile that is associated with this server
uuid	String	Server UUID
virtualAddressStatus	String	Virtual address status. This can be one of the following values. • **NOT_APPLIED**. Virtual addresses are not applied. • **APPLIED**. Virtual addresses are applied.
label	String	Always set to “Server Status”

The following example is returned if the request is successful.


```
{
   "identifier": "uuid",
   "items": [{
      "activationStatus": "COMPLETED",
      "complianceStatus": "VALID ",
```

```
      "configStatus": "PROFILE_ACTIVATED",
      "serverName": "ch02n12-imm",
      "serverProfileId": "69",
      "serverProfileName": "Flex Virtual Fabric Pattern-profile1",
      "serverTemplateId": "68",
      "serverTemplateName": "Flex Virtual Fabric Pattern",
      "uuid": "BA298CD7BC5311E69A000090FAF46898",
      "virtualAddressStatus": "APPLIED"
   }]
   "label": "Server Status",
}
```

/profiles/unassign/*{id}*

Use this REST API to deactivate a profile from a managed server.

HTTP methods

POST

POST /profiles/unassign/*{id}*

Use this method to deactivate a profile from a specific managed server.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/profiles/unassign/{id}`

where *{id}* is the unique ID of the server profile that was assigned when the server pattern was deployed. You can specify multiple profile IDs, separated by commas. To obtain the server profile IDs, use the GET /profiles method.

Query parameters

Parameters	Required / Optional	Description
IncludeResultDetails=*{boolean>*	Optional	Identifies whether to include details about the unassignment request. This can be one of the following values. • **true**. Returns details. • **false**. Returns only a success or failure message.

The following example deactivate a profile from a specific managed server and returns details about the request.

```
PSOT https://192.0.2.0//profiles/unassign/52?IncludeResultDetails=true
```

Request body

Attributes	Required / Optional	Type	Description
force	Optional	Boolean	Identifies whether to force profile deactivation. This can be one of the following values. • **true**. Forces profile deactivation. • **false**. Does not force profile deactivation.
powerDownITE	Optional	Boolean	Identifies whether to power off the server. This can be one of the following values. • **true**. Powers off the server. • **false**. Does not power off the server.
resetIMM	Optional	Boolean	Identifies whether to reset the baseboard management controller. This can be one of the following values. • **true**. Resets the management controller. • **false**. Does not reset the management controller.
resetSwitch	Optional	Boolean	Identifies whether to reset the switch internal port settings to default values. This can be one of the following values. • **true**. Resets the switch internal port settings to default values. • **false**. (default) Does not reset the switch internal port settings.

The following example deactivate a profile from a specific managed server, and resets the baseboard management controller and switch settings.

```
{
   "force": true
   "powerDownITE": true,
   "resetIMM": false,
   "resetSwitch": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
	Array	Information about the actions that were accomplished during the unassignment of the profile
deactivateProfile	Array	Profile is deactivated from LDAP
attempted	Boolean	Indicates whether the disabling profile mode was attempted. This can be one of the following values. • **true**. Deactivating the profile was attempted. • **false**. Deactivating the profile was not attempted.
required	Boolean	Indicates whether the profile must be deactivated. This can be one of the following values. • **true**. Deactivating the profile is required. • **false**. Deactivating the profile is not required.
succeeded	Boolean	Indicates whether the reset was successful. This can be one of the following values. • **true**. Deactivating the profile was successful. • **false**. Deactivating the profile was not successful.
disableProfileMode	Array	Profile is disabled from LDAP
attempted	Boolean	Indicates whether the disabling profile mode was attempted. This can be one of the following values. • **true**. Disabling profile mode was attempted. • **false**. Disabling profile mode was not attempted.
required	Boolean	Indicates whether the profile mode must be disabled. This can be one of the following values. • **true**. Disabling profile mode is required. • **false**. Disabling profile mode is not required.
succeeded	Boolean	Indicates whether the reset was successful. This can be one of the following values. • **true**. Disabling profile mode was successful. • **false**. Disabling profile mode was not successful.
powerOffServer	Array	Server request was sent as a result of unassign. Must be specified as part of the request body.
attempted	Boolean	Indicates whether the powered off was attempted. This can be one of the following values. • **true**. Power off was attempted. • **false** Power off was not attempted.
required	Boolean	Indicates whether the server must be powered off. This can be one of the following values. • **true**. Power off is required. • **false** Power off is not required.
succeeded	Boolean	Indicates whether the powered off was successful. This can be one of the following values. • **true**. Power off was successful. • **false** Power off was not successful.
resetIMMToDefaults	Array	Reset IMM to defaults as a result of unassign. Must be specified as part of the request body.
attempted	Boolean	Indicates whether the reset was attempted. This can be one of the following values. • **true**. Reset was attempted. • **false** Reset was not attempted.

Attributes	Type	Description
required	Boolean	Indicates whether the IMM must be reset to default values. This can be one of the following values. • **true**. Reset is required. • **false**. Reset is not required.
succeeded	Boolean	Indicates whether the reset was successful. This can be one of the following values. • **true**. Reset was successful. • **false** Reset was not successful.
profileId	Integer	ID of profile on which action was attempted
message	String	Detailed description of the message

The following example is returned if the request is successful.

```
{
    [1]
    0: {
        deactivateProfile:
            {
                "required": true,
                "attempted": true,
                "succeeded": true
            },
            ...
        disableProfileMode:
            {
                "required": false,
                "attempted": false,
                "succeeded": false
            },
            ...
        powerOffServer:
            {
                "required": false,
                "attempted": false,
                "succeeded": false
            },
            ...
        resetIMMToDefaults:
            {
                "required": false,
                "attempted": false
                "succeeded": false
            },
            ...
    },
    ...
    profileId: "52",
    message: ""
}
```

Chapter 8. Operating-system deployment

The following resources are available for performing operating-system deployment functions.

/files/osImages?jobId=*{job_id}*

Use this REST API to import an OS image, OS image profile, device driver, boot file, or custom file (such as configuration settings, installation script, software, and unattend file), to the Lenovo XClarity Administrator OS images repository. Only the user that created the job has the permission to import image using the job ID that was returned from that method.

HTTP methods

POST

POST /files/osImages?jobId=*{job_id}*

Use this method to import an OS image, OS image profile, device driver, boot file, or custom file (such as configuration settings, installation script, software, and unattend file) to the Lenovo XClarity Administrator OS images repository. Only the user that created the job has the permission to import a file using the job ID that was returned from that method.

Before you can import , you must first create an import job using the POST /osImages method.

You can monitor the status of the import request using the GET /tasks/*{job_list}* method.

The following types of files can be imported based on the value specified for the **imageType** query parameter.

Image Type	Supported File Type (extension)
BOOT	For Linux and VMware, boot files are not supported. For Windows, the boot files must be in the .zip format for WinPE.
BUNDLE	For Linux and VMWare, bundle files are not supported. For Windows, bundle files must be in the zip format. **Note:** Only official bundle files that are released and signed by Lenovo are supported.
BUNDLESIG	For Linux and VMWare, bundle signature files are not supported. For Windows, bundle signature files must be in the asc format.
CONFIG	JSON- formatted files are supported.
DUD	For Linux, device drivers must be in the .iso or .rpm format. The .iso or .rpm file must contain a device driver in the Device Update Driver format. For Windows, device drivers must be in the .zip format. The .zip file must contain a collection of raw device drivers in the .inf format. For VMWare, device drivers are not supported.
OS	All OS images must be in the .iso format.
OSPROFILE	All profiles must be in the .tar.gz format.
SCRIPT	For Linux, Bash (.sh), Perl (.pm or .pl), Python (.py) files are supported. For Windows, Command file (.cmd), PowerShell (.ps1) files are supported. For VMWare, installation scripts are not supported.

Image Type	Supported File Type (extension)
SOFTWARE	For Linux, archive .tar.gz files are supported. For Windows, archive.zip files are supported.
UNATTEND	For Linux, Kickstart (.ks) and AutoYast (.xml) files are supported. For Windows, Unattend .xml files are supported. For VMWare, installation scripts are not supported.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/files/osImages?jobId={job_id}`

where *{job_id}* is a ID of the import job that is returned by the POST /osImages method.

Query parameters

Parameters	Required / Optional	Description
jobID=*{job_id}*	Required	ID of the job that was created to import files using the last POST /osImages method
checksumType=*{type}*	Optional	Specify the type of checksum to be used. This can be one of the following values. • **MD5** • **SHA1** • **SHA256** It is added as an item of the multi-part body.
checksumValue=*{value}*	Optional	Checksum string of the .ISO file. It is added as an item of the multi-part body
imageName=*{name}*	Required	Name of the OS image to which you want to add the device driver (for example, redhat7.0) **Note:** The operating-system image must exist in the OS images repository.

Parameters	Required / Optional	Description
imageType=*{type}*	Required	Type of image being imported. This can be one of the following values. • **BOOT**. Boot-options file. This is available for only customized Windows operating-system profiles. • **BUNDLE**. Bundle file (in .zip format). This is available for only customized Windows operating-system profiles. • **BUNDLESIG**. Bundle signature files (in .asc format). This is available for only customized Windows operating-system profiles. • **CONFIG**. Configuration-settings file (in JSON format) • **DUD**. Device driver. This is available for customized Windows and Linux operating-system profiles. • **OS**. (default) OS image • **OSPROFILE**. Customized OS image profile • **SCRIPT**. Installation-script file • **SOFTWARE**. Archive file (in .zip or .tar.gz format) that encapsulates the post-install software payload • **UNATTEND**. Unattend file (in kickstart .cfg, autoyast .xml, or Windows .xml format)
os=*{os_type}*	Required when **imageType** is "BOOT," "CONFIG,""DUD," "SCRIPT," "SOFTWARE," or "UNATTEND"	Operating system that is associated with the uploaded file. This can be one of the following values. • **esxi** • **rhels** • **sles** • **win**
path=*{os_path}*	Optional	Full path to the OS image on the remote file server **Note:** This attribute is applicable only when **serverId** is specified.
serverId=*{profile_id}*	Optional	Profile ID for the remote file server To obtain the profile ID, use the GET /osImages method.

The following example imports an OS image using job ID `1`.

```
POST https://192.0.2.0/files/osImages?jobId=1
```

The following example imports a device driver for Red Hat v7.0 using job ID `4`.

```
POST https://192.0.2.0/files/osImages?jobId=4&imageType=DUD&os=RHEL&imageName=redhat7.0
```

The following example imports a boot file for Windows using job ID `5`.

```
POST https://192.0.2.0/files/osImages?jobId=4&imageType=BOOT&os=windows
```

The following example imports a customized OS image profile using job ID `22`.

```
POST https://192.0.2.0/files/osImages?jobId=22&imageType=OSPROFILE
```

Request body

Use the "multipart/form-data" media type to import the ISO image. Use the attributes in the following table as the multipart name in the body. For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage.

The following example imports an ISO image.

HTTP Header

```
Content-Type: multipart/form-data; boundary=AaB03x
```

Request body

```
--AaB03x
    Content-Disposition: form-data; name="checksumType"
    MD5
    --AaB03x
    Content-Disposition: form-data; name="checksumValue"
    DE232312323SXZEW3JDOIWOZLSWJWQ
    --AaB03x
    Content-Disposition: form-data; name="uploadedfile"; filename="redhat7.0.iso"
    Content-Type: application/octet-stream
    ... {CONTENTS OF REDHAT7.0.ISO} ...
    --AaB03x--
```

Response codes

Code	Description	Comments
201	Created	One or more new resources were successfully created.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
412	Precondition failed	Specified data is invalid because of missing values. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
fileid	String	Identifier of the file that was successfully imported
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful. Use GET /tasks/*{job_list}* to monitor the progress of the deployment.

```
{
   "result": "success",
   "fileid": "20161206822241_WinPE_64.wim",
   "messages":[]
}
```

The following example is returned if the request is *not successful*.

```
{
    "result": "failed",
    "messages": [{
        "explanation": "This issue can occur because of network issues or because the wrong
                        checksum file is in the directory.",
        "id": "FQXHMFC0001M",
        "text": "The checksum of the imported ISO image does not match the provided checksum
                 file.",
        "recovery": {
            "URL": "",
            "text": "Make sure that the checksum file matches the ISO image and attempt the
                     operation again. If the problem persists, contact Support."
        }
    }]
}
```

/hostPlatforms

Use this REST API to retrieve information about the host platforms and deploy operating-system images to the host platforms as a job. Host platforms include all managed servers for which an operating system can be deployed from the Lenovo XClarity Administrator server.

HTTP methods

GET, PUT

GET /hostPlatforms

Use this method to return information about the host platforms.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/hostPlatforms`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
availableImages	Array of strings	Operating-system image profile ID. This ID is made up of the OS-image name and image-profile name separated by a bar (for example, `sles12.2|sles12.2-x86_64-install-Basic`).
imagesWithoutWinPERemoved	Boolean	Indicates whether Windows images that have no matching WinPE are removed from the **availableImages** list.
incompatibleImagesRemoved	Boolean	Indicates whether images that not supported in the current security mode are removed from the **availableImages** list
isAuthorized	Boolean	Indicates whether the user is assigned a role that can manage and deploy an operating system. This can be one of the following values. • **true**. The user is authorized. • **false**. The user is not authorized.
items	Array of objects	Information about all other host platforms
availableImages		
label	String	Name of the operating system image profile
selected	Boolean	Internal use only
value	String	ID of the operating system image profile
bay	String	Bay number of the host platform in the chassis, if the host platform is a server in a Flex chassis
bootOrder	Array	
bootOrderList	Array	
currentBootOrderDevices	String	Boot order that is currently configured for a specified boot type
bootType	String	Boot type of the boot order setting. The boot type must match a supported boot type for the server and varies by operating system.
possibleBootOrderDevices	String	Boot order devices that are available for the specified boot type
chassisIpAddress	String	IP address of the chassis that is associated with the host platform. This is applicable only if the host platform is a server in a Flex System chassis.

Attributes	Type	Description
chassisName	String	Name of the chassis that is associated with the host platform. This is applicable only if the host platform is a server in a Flex System chassis.
chassisuuid	String	UUID of the chassis in which the host platform resides, if the host platform is a server in a Flex System chassis

Attributes	Type	Description
deployStatus	String	Deployment status. This can be one of the following values. • **0**. Ready • **1**. Not Ready • **2**. Unknown OS Deploy Status • **3**. No OS being deployed • **4**. OS Deployment Starting • **5**. Pre-deployment Validation • **6**. Node Created • **7**. Node Updated • **8**. Bootable ISO Created • **9**. Bootable ISO Mounted • **10**. Boot Order Sequence Modified • **11**. Node Rebooting • **12**. Node Restarted • **13**. Preparing Server for OS installation • **14**. Installing OS • **15**. Post-Installation Processing • **16**. Starting newly installed OS • **17**. OS Installation Completed • **18**. OS Discovery Started • **19**. Post-Deployment Cleanup Started • **20**. OS Deployment Failed • **21**. OS Deployment Stopped • **22**. Failed Preparing Server for OS Installation - storage failure • **23**. Failed Preparing Server for OS Installation - unsupported USB storage failure • **24**. Failed Preparing Server for OS Installation - unsupported SAN detected failure • **25**. Failed Preparing Server for OS Installation - Windows partition failure XCAT status • **26**. Active directory join failed • **27**. Active directory join succeeded using domain credentials • **28**. Active directory join succeeded using blob • **29.** Failed Preparing Server for OS Installation – hypervisor key detected • **30**. Custom post-install scripts started • **31**. Custom post-install script started • **32**. Custom post-install script completed • **33**. Custom post-install scripts completed • **34**. Downloading custom software payloads • **35**. Downloading custom software payload • **36**. Finished downloading custom software payload • **37**. Error downloading custom software payload • **38**. Finished downloading custom software payloads • **39**. Extracting custom software payloads • **40**. Extracting custom software payload • **41**. Finished extracting custom software payload • **42**. Error extracting custom software payload • **43**. Finished extracting custom software payloads • **44**. Workload deployment succeeded • **45**. Workload deployment is running with warning • **46**. Workload deployment failed • **47**. Workload deployment message • **48**. Custom post-install script error • **49**. Installing custom drivers • **50**. Installing custom driver • **51**. Finished installing custom driver • **52**. Error installing custom driver

Attributes	Type	Description
		• **53**. Finished installing custom drivers **Note:** If the **deployStatus** is “Not Ready,” use the **readyCheck** attribute to get information to help resolve the problem.
deployStatusID	Integer	Status ID of the host platform when the operating system is actively being deployed
id	String	UUID of the host platform
immIpAddress	String	IP address of the baseboard management controller for the host platform
isRealNode	Boolean	Indicates whether the server is real or demo. This can be one of the following values. • **true**. The server is a real server. • **false**. The server is a demo server.
licenseKey	String	License key for Windows or ESXI operating system
mgmtProcType	String	Type of management controller. This can be one of the following values. • **FSP** • **IMM2** • **lenovo-AMI-controller** • **XCC** • **XCC2** • **UNKNOWN**
name	String	Name of the host platform
networkSettings	Array	Information about network settings
dns1	String	Preferred DNS server for the host server to be used after the operating system is deployed
dns2	String	Alternative DNS server for the host server to be used after the operating system is deployed
gateway	String	Gateway of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings.
hostname	String	Hostname that is used for the host server
ipAddress	String	IP address of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. If using static IP addresses, you must specify either the hostname or IP address. If using DHCP, you must specify the hostname of the server.
macAddress	Array	Information about the MAC address
label	String	MAC address of the host platform and the port status, separated by a dash (for example, 08:94:EF:4E:FB:C2 – Up). The port status can be one of the following values. • **Up** • **Down** • **N/A**. Not applicable **Note:** If the device is a ThinkServer server with expansion Ethernet adapter cards, no MAC address is returned. It is recommended that you use the default `AUTO` setting when specifying the MAC address for deployment.

Attributes	Type	Description
selected	String	Internal use only
value	String	MAC address of the host server to which the IP address is to be bound The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment. VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only the MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server. **Note:** If the device is a ThinkServer server with expansion Ethernet adapter cards, no MAC address is returned. It is recommended that you use the default `AUTO` setting when specifying the MAC address for deployment.
mtu	String	Maximum transmission unit for the host to be used after the operating system is deployed
prefixLength	String	Prefix length of the host IP address to be used after the operating system is deployed. This is used when the network setting is set to static IPv6 in the Global OS deployment settings.
subnetMask	String	Subnet mask of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings.
vlanId	String	VLAN ID for operating-system VLAN tagging This attribute is valid only if in VLAN mode is enabled (see GET /osdeployment/globalSettings).
nodeType	String	Type of the host platform
primary	String	Indicates whether the host platform is the primary node within the scalable partition
rackID	String	Name of the rack in which the host platform resides
rackUnit	String	Lowest unit number in the rack for the device on which the host platform resides
readyCheck	Array	
accessState	String	Current state of the host platform. This can be one of the following values. • **Online** • **Offline** • **Partial** • **Pending** • **Unknown** • For servers in a Flex chassis, this reflects the current state. For rack servers, this value is set to “unSupported”. • The access state must be online “Online” or “unSupported” to deploy an operating system on the host platform.

Attributes	Type	Description
isAuthorized	Boolean	Indicates whether the user is assigned a role that can manage and deploy an operating system. This can be one of the following values. • **true**. The user is authorized. • **false**. The user is not authorized.
remotePresenceMode	String	Indicates whether the virtual media (also known as remote media) is enabled. Virtual media must be enabled to deploy operation systems. This can be one of the following values. • **Enabled**. Virtual media is enabled. • **Disabled**. Virtual media is disabled. You cannot deploy an operating system on the server. **Note:** To use virtual media, XClarity Controller Enterprise or the remote-presence FoD key must be enabled on the server.
secureBootMode	String	Indicates whether secure boot mode is enabled. This can be one of the following values. • **Enabled**. Secure boot mode is enabled. You cannot deploy an operating system on the server. • **Disabled**. Secure boot mode is disabled.
uefiMode	String	Indicates whether the UEFI boot mode is enabled. This can be one of the following values. • **Enabled**. The boot mode is UEFI. • **Disabled**. The boot mode is not UEFI. You cannot deploy an operating system on the server. **Tip:** You can modify the UEFI mode using server patterns.
validMac	String	Indicates whether the MAC address is valid. This can be one of the following values. • **ok**. The MAC address is a valid address. • **error**. The MAC address is empty. You cannot deploy an operating system on the server. • **not found**. A valid MAC address was not found. Consider setting the **macAddress** to `AUTO` to automatically detect valid Ethernet MAC addresses that can be used.
vlanAutoMac	String	Indicates whether the MAC addresses are valid under VLAN mode. This can be one of the following values. • **ok**. There are MAC addresses other than AUTO. • **error**. The only MAC address is AUTO, or the selected MAC address is AUTO. You cannot deploy an operating system on the server. **Tip:** If available, select a MAC address other than AUTO. Alternatively, do not use VLANs in global settings.
remoteControl	String	Indicates the remote-control enablement status. This can be one of the following values. • **singleUser**. Only one user can be logged in at a time. • **multiUser**. Multiple users can be logged at a time. • **disabled**. Remote control is disabled.
storageSettings	String	

Attributes	Type	Description
label	String	Name of the preferred storage location on which operating system image is deployed. This can be one of the following values. • **Local disk** • **Embedded USB Hypervisor** • **M.2drive** • **SAN storage** **Note:** For ThinkServer servers, this value is always **Local disk**.
selected	String	Internal use only
value	String	Name of the preferred storage location on which operating system image is deployed. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always **localdisk**.
uuid	String	UUID of the host platform
windowsDomain	Array	Information about Active Directory domains
domainName	String	Name of Active Directory domain to which the Windows operating system is joined
OU	String	Organizational unit of Active Directory domain
partitions	Array	Host platforms that support multiple node functionality
nodes	Array	IP address of the baseboard management controller for the host platform
availableImages	Array	Operating-system profiles that this server supports
label	String	Name of the operating system image profile
selected	Boolean	Internal use only
value	String	ID of the operating system image profile
bay	String	Bay number of the host platform in the chassis, if the host platform is a server in a Flex chassis
bootOrder	Array	
bootOrderList	Array	

Attributes	Type	Description
bootType	String	Boot type of the boot order setting. This can be one of the following values. • **BootOrder** • **CDDVDROMBootOrder** • **HardDiskBootOrder** • **NetworkBootOrder** • **Permanent** • **SingleUse** • **USBBootOrder** • **WakeOnLan** • **Unknown**
currentBootOrderDevices	String	Boot order that is currently configured for a specified boot type
possibleBootOrderDevices	String	Boot order devices that are available for the specified boot type
chassisName	String	Name of the chassis that is associated with the host platform. This is applicable only if the host platform is a server in a Flex chassis.
chassisIpAddress	String	IP address of the chassis that is associated with the host platform. This is applicable only if the host platform is a server in a Flex chassis.
chassisuuid	String	UUID of the chassis in which the host platform resides, if the host platform is a server in a Flex chassis

Attributes	Type	Description
deployStatus	String	Deploy status. This can be one of the following values. • Ready • Not Ready • Unknown OS Deploy Status • No OS being deployed • OS Deployment Starting • Pre-deployment Validation • Node Created • Node Updated • Bootable ISO Created • Bootable ISO Mounted • Boot Order Sequence Modified • Node Rebooting • Node Restarted • Preparing Server for OS installation • Installing OS • Post-Installation Processing • Starting newly installed OS • OS Installation Completed • OS Discovery Started • Post-Deployment Cleanup Started • OS Deployment Failed • OS Deployment Stopped • Failed Preparing Server for OS Installation - storage failure • Failed Preparing Server for OS Installation - unsupported USB storage failure • Failed Preparing Server for OS Installation - unsupported SAN detected failure • Failed Preparing Server for OS Installation - Windows partition failure XCAT status • Active directory join failed • Active directory join succeeded using domain credentials • Active directory join succeeded using blob • Failed Preparing Server for OS Installation – hypervisor key detected • Custom post-install scripts started • Custom post-install script started • Custom post-install script completed • Custom post-install scripts completed • Downloading custom software payloads • Downloading custom software payload • Finished downloading custom software payload • Error downloading custom software payload • Finished downloading custom software payloads • Extracting custom software payloads • Extracting custom software payload • Finished extracting custom software payload • Error extracting custom software payload • Finished extracting custom software payloads • Workload deployment succeeded • Workload deployment is running with warning • Workload deployment failed • Workload deployment message • Installing custom drivers • Installing custom driver • Finished installing custom driver • Error installing custom driver • Finished installing custom drivers

Attributes	Type	Description
		Note: You cannot deploy an operating-system image to that server if the **deployStatus** is “Not Ready.”. Use the **readyCheck** attribute to get information to help resolve the problem. If all of the validation checks pass, verify that the network settings are configured.
deployStatusID	Integer	Status ID of the host platform when the operating system is actively being deployed. This can be one of the following values. • **0**. Ready • **1**. Not Ready • **2**. Unknown OS Deploy Status • **3**. No OS being deployed • **4**. OS Deployment Starting • **5**. Pre-deployment Validation • **6**. Node Created • **7**. Node Updated • **8**. Bootable ISO Created • **9**. Bootable ISO Mounted • **10**. Boot Order Sequence Modified • **11**. Node Rebooting • **12**. Node Restarted • **13**. Preparing Server for OS installation • **14**. Installing OS • **15**. Post-Installation Processing • **16**. Starting newly installed OS • **17**. OS Installation Completed • **18**. OS Discovery Started • **19**. Post-Deployment Cleanup Started • **20**. OS Deployment Failed • **21**. OS Deployment Stopped • **22**. Failed Preparing Server for OS Installation - storage failure • **23**. Failed Preparing Server for OS Installation - unsupported USB storage failure • **24**. Failed Preparing Server for OS Installation - unsupported SAN detected failure • **25**. Failed Preparing Server for OS Installation - Windows partition failure XCAT status • **26**. Active directory join failed • **27**. Active directory join succeeded using domain credentials • **28**. Active directory join succeeded using blob • **29.** Failed Preparing Server for OS Installation – hypervisor key detected • **30**. Custom post-install scripts started • **31**. Custom post-install script started • **32**. Custom post-install script completed • **33**. Custom post-install scripts completed • **34**. Downloading custom software payloads • **35**. Downloading custom software payload • **36**. Finished downloading custom software payload • **37**. Error downloading custom software payload • **38**. Finished downloading custom software payloads • **39**. Extracting custom software payloads • **40**. Extracting custom software payload • **41**. Finished extracting custom software payload • **42**. Error extracting custom software payload • **43**. Finished extracting custom software payloads • **44**. Workload deployment succeeded • **45**. Workload deployment is running with warning

Attributes	Type	Description
		• **46**. Workload deployment failed • **47**. Workload deployment message • **48**. Custom post-install script error • **49**. Installing custom drivers • **50**. Installing custom driver • **51**. Finished installing custom driver • **52**. Error installing custom driver • **53**. Finished installing custom drivers
id	String	Internal use only. Use the **uuid** attribute instead.
immIpAddress	String	IP address of the baseboard management controller for the host platform
isRealNode	Boolean	Indicates whether the server is real or demo. This can be one of the following values. • **true**. The server is a real server. • **false**. The server is a demo server.
licenseKey	String	License key for Windows or ESXI operating system
mgmtProcType	String	Type of management controller. This can be one of the following values. • **FSP** • **IMM2** • **lenovo-AMI-controller** • **XCC** • **XCC2** • **UNKNOWN**
name	String	Name of the host platform
networkSettings	Array	Information about network settings
mtu	String	Internal use only
dns1	String	Internal use only
dns2	String	Internal use only
gateway	String	Internal use only
hostname	String	Internal use only
subnetMask	String	Internal use only
macAddress	Array	Information about the MAC address
label	String	MAC address of the host platform and the port status, separated by a dash (for example, 08:94:EF:4E:FB:C2 – Up). The port status can be one of the following values. • **Up** • **Down** • **N/A**. Not applicable
selected	String	Internal use only
value	String	MAC address of the host platform
prefixLength	String	Internal use only
ipAddress	String	Internal use only
nodeType	String	Type of the host platform

Attributes	Type	Description
rackID	String	Name of the rack in which the host platform resides
rackUnit	String	Lowest unit number in the rack for the device on which the host platform resides
readyCheck	Array	List of validation checks
accessState	String	Current state of the host platform. This can be one of the following values. • **Online** • **Offline** • **Partial** • **Pending** • **Unknown** • For servers in a Flex chassis, this reflects the current state. For rack servers, this value is set to “unSupported”. • The access state must be online “Online” or “unSupported” to deploy an operating system on the host platform.
isAuthorized	Boolean	Indicates whether the user is assigned a role that can manage and deploy an operating system. This can be one of the following values. • **true**. The user is authorized. • **false**. The user is not authorized.
remotePresenceMode	String	Indicates whether the virtual media (also known as remote media) is enabled. Virtual media must be enabled to deploy operation systems. This can be one of the following values. • **Enabled**. Virtual media is enabled. • **Disabled**. Virtual media is disabled. You cannot deploy an operating system on the server. **Note:** To use virtual media, XClarity Controller Enterprise or the remote-presence FoD key must be enabled on the server.
secureBootMode	String	Indicates whether secure boot mode is enabled. This can be one of the following values. • **Enabled** Secure boot mode is enabled. You cannot deploy an operating system on the server. • **Disabled**. Secure boot mode is disabled.
uefiMode	String	Indicates whether the UEFI boot mode is enabled. This can be one of the following values. • **Enabled** The boot mode is UEFI. • **Disabled**. The boot mode is not UEFI. You cannot deploy an operating system on the server. **Tip:** You can modify the UEFI mode using server patterns.
validMac	String	Indicates whether the MAC address is valid. This can be one of the following values. • **ok**. The MAC address is a valid address. • **error**. The MAC address is empty. You cannot deploy an operating system on the server. • **not found**. A valid MAC address was not found. Consider setting the **macAddress** to `AUTO` to automatically detect valid Ethernet MAC addresses that can be used.

Attributes	Type	Description
remoteControl	String	Indicates the remote-control enablement status. This can be one of the following values. • **singleUser**. Only one user can be logged in at a time. • **multiUser**. Multiple users can be logged at a time. • **disabled**. Remote control is disabled.
storageSettings	Array	Preferred storage location on which you want to deploy operating-system images
label	String	Descriptive name of the preferred storage location. This can be one of the following values. • **Local disk** • **Embedded USB Hypervisor** • **M.2drive** • **SAN storage**
selected	Boolean	
value	String	Preferred storage location. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made.
uuid	String	UUID of the host platform
windowsDomain	Array	Information about Active Directory domains
domainName	String	Name of Active Directory domain to which the Windows operating system is joined
OU	String	organizational unit of Active Directory domain
partitionID	String	Partition ID, if the server is in a scalable complex
partitionName	String	Partition name, if the server is in a scalable complex
uuid	String	Partition UUID, if the server is in a scalable complex
result	String	Result of the request. This can be one of the following values. • **Success**. The request was successful. • **Failed**. The request failed.
messages	Array	Information about the message that is related to the result of the request
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
message	String	Message text associated with the message identifier

Attributes	Type	Description
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.


```
{
   "availableImages": ["esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization"],
   "imagesWithoutWinPERemoved": true,
   "incompatibleImagesRemoved": false,
   "isAuthorized": true,
   "items": [{
      "availableImages": [{
         "label": "esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization"
         "selected": true,
         "value": "esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization",
      }],
      "bay": "13",
      "bootOrder": {
         "bootOrderList": [{
            "currentBootOrderDevices": ["None"],
            "bootType": "SingleUse",
            "possibleBootOrderDevices": [
               "None",
               "PXE Network",
               "Disk Drive 0",
               "Diagnostics",
               "CD\/DVD Rom",
               "Boot To F1",
               "Hypervisor",
               "Floppy Disk"
            ]
         },
         ...,
         {
            "bootType": "Permanent",
            "currentBootOrderDevices": [
               "CD\/DVD Rom",
               "Disk Drive 0",
               "PXE Network"
            ],
            "possibleBootOrderDevices": [
               "CD\/DVD Rom",
               "Diagnostics",
               "DSA",
               "Embedded Hypervisor",
               "Floppy Disk",
               "Disk Drive 0",
               "Disk Drive 1",
               "Disk Drive 2",
               "Disk Drive 3",
               "Disk Drive 4",
               "IMM1",
               "IMM2",
               "iSCSI",
               "iSCSI Critical",
               "Legacy Only",
               "NIC1",
```

```
            "NIC2",
            "PXE Network",
            "SAS",
            "SdRaid",
            "Slot1Dev1",
            "Slot1Dev2",
            "Slot1Dev3",
            "Slot2Dev1",
            "Slot2Dev2",
            "Slot2Dev3",
            "Slot3Dev1",
            "Slot3Dev2",
            "USB Storage",
            "USB1",
            "USB2",
            "USB3",
            "VNIC1",
            "VNIC2",
            "VNIC3",
            "VNIC4",
            "VNIC5",
            "VNIC6"
         ]
      }]
},
"chassisIpAddress": "192.0.2.0",
"chassisName": "SN#Y034BG16E0AR",
"chassisuuid": "FBEF740B178F4EFAA846E7225EE256DC"
"deployStatus": "Not Ready",
"deployStatusID": 1,
"id": "69BDF8912E5211E4998B40F2E99033F0",
"immIpAddress": "192.0.2.10",
"isRealNode": true,
"licenseKey": "",
"mgmtProcType": "IMM2",
"name": "node12",
"networkSettings": {
   "dns1": "",
   "dns2": "",
   "gateway": "",
   "hostname": "",
   "ipAddress": "",
   "macAddress": [{
      "label": "AUTO",
      "selected": true,
      "value": "AUTO"
   },
   ...,
   {
      "label": "40:F2:E9:90:33:FC - Down",
      "selected": false,
      "value": "40:F2:E9:90:33:FC"
   }],
   "mtu": 1500,
   "prefixLength": 0,
   "subnetMask": "",
   "vlanId": "2"
},
"nodeType": "ite",
"primary": false,
"rackID": "",
```

```
    "rackUnit": "0",
    "readyCheck": {
       "accessState": "Online",
       "isAuthorized": true,
       "remotePresenceMode": "Enabled",
       "secureBootMode": "Disabled",
       "uefiMode": "Enabled",
       "validMac": "ok"
    },
    "remoteControl": "multiUser",
    "storageSettings": [{
       "label": "Local Disk",
       "selected": true,
       "value": "localdisk"
    },
    {
       "label": "Embedded Hypervisor",
       "selected": false,
       "value": "usbdisk"
    }],
    "uuid": "69BDF8912E5211E4998B40F2E99033F0",
    "windowsDomain": {
       "domainName": "",
       "OU": ""
    },
},
...,
{
    "availableImages": [{
       "label": "esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization",
       "selected": true,
       "value": "esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization"
    }],
    "bay": "3",
    "bootOrder": {
       "bootOrderList": [{
          "currentBootOrderDevices": ["None"],
          "bootType": "SingleUse",
          "possibleBootOrderDevices": [
             "None",
             "PXE Network",
             "Disk Drive 0",
             "Diagnostics",
             "CD\/DVD Rom",
             "Boot To F1",
             "Hypervisor",
             "Floppy Disk"
          ]
       },
       ...,
       {
          "currentBootOrderDevices": [
             "CD\/DVD Rom",
             "Floppy Disk",
             "Disk Drive 0",
             "PXE Network"
          ],
          "bootType": "Permanent",
          "possibleBootOrderDevices": [
             "CD\/DVD Rom",
             "Diagnostics",
```

```
            "DSA",
            "Embedded Hypervisor",
            "Floppy Disk",
            "Disk Drive 0",
            "Disk Drive 1",
            "Disk Drive 2",
            "Disk Drive 3",
            "Disk Drive 4",
            "IMM1",
            "IMM2",
            "iSCSI",
            "iSCSI Critical",
            "Legacy Only",
            "NIC1",
            "NIC2",
            "PXE Network",
            "SAS",
            "SdRaid",
            "Slot1Dev1",
            "Slot1Dev2",
            "Slot1Dev3",
            "Slot2Dev1",
            "Slot2Dev2",
            "Slot2Dev3",
            "Slot3Dev1",
            "Slot3Dev2",
            "USB Storage",
            "USB1",
            "USB2",
            "USB3",
            "VNIC1",
            "VNIC2",
            "VNIC3",
            "VNIC4",
            "VNIC5",
            "VNIC6"
         ]
      }]
   },
   "chassisIpAddress": "10.240.73.217",
   "chassisName": "SN#Y034BG16E0BH",
   "chassisuuid": "8C070E3262114E36B7E68699386FBA53"
   "deployStatus": "Not Ready",
   "deployStatusID": 1,
   "id": "0E0BEA009E2411E2BEB93440B5EFB9B8",
   "immIpAddress": "10.240.74.69",
   "isRealNode": true,
   "licenseKey": "",
   "mgmtProcType": "IMM2",
   "name": "node04_2",
   "networkSettings": {
      "dns1": "",
      "dns2": "",
      "gateway": "",
      "hostname": "",
      "ipAddress": "",
      "macAddress": [{
         "label": "34:40:B5:EF:B9:B8 - Up",
         "selected": true,
         "value": "34:40:B5:EF:B9:B8"
      },
```

```
      {
         "label": "34:40:B5:EF:B9:BC - Down",
         "selected": false,
         "value": "34:40:B5:EF:B9:BC"
      }],
      "mtu": 1500,
      "prefixLength": 0,
      "subnetMask": ""
      "vlanId": "2"
   },
   "nodeType": "ite",
   "primary": false,
   "rackID": "",
   "rackUnit": "0",
   "readyCheck": {
      "accessState": "Online",
      "remotePresenceMode": "Enabled",
      "secureBootMode": "Disabled",
      "uefiMode": "Enabled",
      "validMac": "ok"
   },
   "remoteControl": "multiUser",
   "storageSettings": [{
      "label": "Local Disk",
      "selected": true,
      "value": "localdisk"
   },
   {
      "label": "Embedded Hypervisor",
      "selected": false,
      "value": "usbdisk"
   }],
   "windowsDomain": {
      "domainName": "",
      "OU": ""
   },

   "uuid": "0E0BEA009E2411E2BEB93440B5EFB9B8",
}],
"partitions": [{
   "nodes": [{
      "availableImages": [{
         "label": "rhels6.6|rhels6.6-x86_64-install-Basic",
         "selected": true,
         "value": "rhels6.6|rhels6.6-x86_64-install-Basic"
      },
      {
         "label": "rhels6.6|rhels6.6-x86_64-install-Minimal",
         "selected": false,
         "value": "rhels6.6|rhels6.6-x86_64-install-Minimal"
      },
      ...,
      {
         "label": "esxi6|esxi6-x86_64-install-Virtualization",
         "selected": false,
         "value": "esxi6|esxi6-x86_64-install-Virtualization"
      }],
      "bay": "",
      "bootOrder": {
         "bootOrderList": [{
            "currentBootOrderDevices": ["None"],
```

```
    "bootType": "SingleUse",
    "possibleBootOrderDevices": [
       "None",
       "PXE Network",
       "Disk Drive 0",
       "Diagnostics",
       "CD\/DVD Rom",
       "Boot To F1",
       "Hypervisor",
       "Floppy Disk"
    ]
 },
 ...,
 {
    "currentBootOrderDevices": [
       "PXE Network",
       "CD\/DVD Rom",
       "Disk Drive 0"
    ],
    "bootType": "WakeOnLAN",
    "possibleBootOrderDevices": [
       "PXE Network",
       "CD\/DVD Rom",
       "Disk Drive 0",
       "Red Hat Enterprise Linux",
       "Floppy Disk",
       "Disk Drive 1",
       "Disk Drive 2",
       "Disk Drive 3",
       "Disk Drive 4",
       "USB Storage",
       "Diagnostics",
       "iSCSI",
       "iSCSI Critical",
       "Embedded Hypervisor",
       "Legacy Only",
       "USB0",
       "USB1",
       "USB2",
       "USB3",
       "USB4",
       "USB5",
       "USB6",
       "USB7",
       "DSA",
       "Slot16",
       "Slot17",
       "Slot18",
       "Slot19",
       "Slot12",
       "Slot11",
       "Slot10",
       "Slot1",
       "Slot2",
       "Slot3",
       "Slot4",
       "Slot5",
       "Slot6",
       "Slot7",
       "Slot8",
       "Slot9",
```

```
            "IMM1",
            "IMM2",
            "Node2-USB0",
            "Node2-USB1",
            "Node2-USB2",
            "Node2-USB3",
            "Node2-USB4",
            "Node2-USB5",
            "Node2-USB6",
            "Node2-USB7",
            "Node2-Slot16",
            "Node2-Slot17",
            "Node2-Slot18",
            "Node2-Slot19",
            "Node2-Slot12",
            "Node2-Slot11",
            "Node2-Slot10",
            "Node2-Slot1",
            "Node2-Slot2",
            "Node2-Slot3",
            "Node2-Slot4",
            "Node2-Slot5",
            "Node2-Slot6",
            "Node2-Slot7",
            "Node2-Slot8",
            "Node2-Slot9",
            "Node2-IMM1",
            "Node2-IMM2"
         ]
      }]
},
"chassisIpAddress": "",
"chassisName": "",
"chassisuuid": "",
"deployStatus": "Ready",
"deployStatusID": 0,
"name": "SAMT-D8S-1B",
"id": "401D78E65B2AB7012FCA98E54FA1FAFE",
"immIpAddress": "fd55:faaf:e1ab:20fa:42f2:e9ff:fe4d:2a1",
"isRealNode": true,
"licenseKey": "",
"mgmtProcType": "IMM2",
"name": "SAMT-D8S-1B",
"networkSettings": {
   "dns1": "",
   "dns2": "",
   "gateway": "",
   "hostname": "",
   "ipAddress": "",
   "macAddress": [{
      "label": "00:0A:F7:25:76:C2",
      "selected": true,
      "value": "00:0A:F7:25:76:C2"
   },
   {
      "label": "00:0A:F7:25:76:C3",
      "selected": false,
      "value": "00:0A:F7:25:76:C3"
   }],
   "mtu": 1500,
   "prefixLength": 0,
```

```
            "subnetMask": ""
         "vlanId": "2"
         },
         "nodeType": "rack-tower server",
         "primary": true,
         "rackID": "",
         "rackUnit": "0",
         "readyCheck": {
            "accessState": "Online",
            "isAuthorized": true,
            "remotePresenceMode": "Enabled",
            "secureBootMode": "Disabled",
            "uefiMode": "Enabled",
            "validMac": "ok"
         },
         "remoteControl": "multiUser",
         "storageSettings": [{
            "label": "Local Disk",
            "selected": true,
            "value": "localdisk",,
         },
         {
            "label": "Embedded USB Hypervisor",
            "selected": false,
            "value": "usbdisk"
         }],
         "uuid": "401D78E65B2AB7012FCA98E54FA1FAFE",
         "windowsDomain": {
            "domainName": "",
            "OU": ""
         },
      }],
      "partitionID": "1",
      "partitionName": "SAMT-D8S-1B (Partition 1)"
      "uuid": "401D78E65B2AB7012FCA98E54FA1FAFE",
   }],
   "result": "success",
   "messages": []
}
```


The following example is returned if the request is not successful.


```
{
   "result": "failed",
   "messages": [{
      "explanation": "An internal error occurred while obtaining the list of all nodes.",
      "id": "FQXHMFC0080M",
      "message": "Unable to obtain the list of all nodes.",
      "recovery": {
         "URL": "",
         "text": "Attempt the operation again. If the problem persists, contact Support."
      }
   }]
}
```


PUT /hostPlatforms

Use this method to deploy operating-system images to specific host platforms as a job (batch mode). You can specify configuration information such as network settings, license, user ID and password, and storage settings.

Important: When deploying an operating system on a Fibre Channel or iSCSI SAN target, you must call PUT /osdeployment/hostSettings to set the target before calling PUT /hostPlatforms to start the deployment.

Note: If you deploy a Microsoft Windows image, you can also specify Active Directory settings required to join an Active Directory domain after the image is installed.

Authentication

Authentication is required.

Request URL

`PUT https://{management_server_IP}/hostPlatforms`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
adusername	Optional	String	(Windows only) User name for the Active Directory domain that is specified in the **windowsDomain** attribute **Note:** This attribute is required if you want a Windows operating system to join an Active Directory domain.
adpassword	Optional	String	(Windows only) Password for the Active Directory user name **Note:** This attribute is required if you want a Windows operating system to join an Active Directory domain.
configFileId	Required if **selected-Image** includes a custom configuration-settings file; otherwise ignored.	String	ID of the custom configuration-settings file to use for this OS deployment
licenseKey	Optional	String	License key to be used for Microsoft Windows or VMware ESXi. If you do not have a license key, you can set this attribute to null.
osCredentials	Optional	Object	OS credentials for the operating system
name	Required	String	User name for the target operating system. This could be the following values. • **root**. For Linux or ESXi
password	Required	String	Hashed password for the target operating system
networkSettings	Required	Object	Information about network settings
dns1	Optional	String	Preferred DNS server for the host server to be used after the operating system is deployed
dns2	Optional	String	Alternative DNS server for the host server to be used after the operating system is deployed

Attributes	Required / Optional	Type	Description
gateway	Required if using static IP addresses. Optional if using DHCP.	String	Gateway of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
hostname	Optional	String	Hostname for the host server. If a hostname is not specified, a default hostname is assigned.
ipAddress	Required if using static IP addresses.	String	IP address of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings.
mtu	Optional	Long	Maximum transmission unit for the host to be used after the operating system is deployed
prefixLength	Optional	String	Prefix length of the host IP address to be used after the operating system is deployed. This is used when the network setting is set to static IPv6 in the Global OS deployment settings.
selectedMAC	Required	String	MAC address of the host server to which the IP address is to be bound The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment, and selectedMAC is set to the newly detected MAC address. VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only the MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server. **Tip:** To obtain the MAC address, use the **macaddress** attribute in GET /hostPlatforms.
subnetMask	Required if using static IP addresses. Optional if using DHCP.	String	Subnet mask of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
vlanId	Optional	String	VLAN ID for operating-system VLAN tagging This attribute is valid only if in VLAN mode is enabled (see GET /osdeployment/globalSettings). **Important:** Only specify a VLAN ID when a VLAN tag is required to function on the network. Using VLAN tags can affect the network routability between the host operating system and the Lenovo XClarity Administrator.

Attributes	Required / Optional	Type	Description
selectedImage	Required	String	Profile ID of the operating-system image to be deployed **Tip:** To obtain the operating-system image values, use the **availableImages** attribute in GET /hostPlatforms method.
storageSettings	Required	Object	Preferred storage location on which you want to deploy operating-system images
targetDevice	Required	String	Target device. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always “localdisk.”
unattendFileId	Required if **selected-Image** includes custom unattend files; otherwise ignored.	String	ID of the unattend file to use for this OS deployment
uuid	Required	String	UUID of the host server to which the operating system is to be deployed

Attributes	Required / Optional	Type	Description
windowsDomain	Optional	String	(Windows only) Active Directory domain that the Windows operating system is to join after the operating system is deployed successfully. If an OU is present, specify the string using the format *domain*/*ou*. If the operating system will not join a domain, you can set this attribute to null. **Notes:** • To join an Active Directory domain, you must specify either the **windowsDomain** or **windowsDomainBlob** attribute. If both are specified, the **windowsDomainBlob** attribute is used. • Use the **adusername** and **adpassword** attributes to specify the user name and password for the domain.
windowsDomainBlob	Optional	String	(Windows only) Active Directory Computer Account Metadata (in Base-64 encoded blob format) that can be used to join the Active Directory domain. For instructions for generating a file that contains the metadata blob data, see Integrating with Windows Active Directory in the Lenovo XClarity Administrator online documentation. **Notes:** • To join an Active Directory domain, you must specify either the **windowsDomain** or **windowsDomainBlob** attribute. If both are specified, the **windowsDomainBlob** attribute is used. • You can use metadata blob data when deploying any Windows operating system. However, this method must be used for Windows Nano Server. Specifying a domain in global settings is not supported for Windows Nano Server.

The following example deploys an operating-system to specific host platform.

```
[{
    "networkSettings": {
        "dns1": "192.0.2.255",
        "dns2": "192.0.2.254",
        "gateway": "192.0.2.200",
        "ipAddress": "192.0.2.0",
         "mtu": 1500,
        "prefixLength": 64,
      "selectedMAC": "78:9A:BC:12:34:56",
        "subnetMask": "255.255.255.0"
    },
    "selectedImage": "rhels6.4-x86_64-install-Minimal",
    "storageSettings": {
        "targetDevice": "lunpluswwn=2@50:05:07:68:05:0c:09:bb"
    },
    "uuid": "2D16B4422AC011E38A06000AF72567B0",
    "windowsDomain": null
}]
```

Response codes

Code	Description	Comments
202	Accepted	The request has been accepted for processing, but the processing has not yet completed. The request might or might not be acted upon, depending on the results of the processing.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
jobID	String	ID of the deployment job in job management module
result	String	Result of the request. This can be one of the following values. • **success**. The request was successful. • **failed**. The request failed.
messages	Array	Message list showing to which host systems the operating system to be deployed

The following example is returned if the request is successful. Use the GET /tasks/*{job_list}* resource to monitor the progress of the deployment.

```
{
   "jobId": "123",
   "result": "success",
   "messages": [{
      "explanation": "It might take a few minutes to deploy the images. You can monitor progress
                  from the Jobs list.",
      "id": "FQXHMFC0120I",
      "text": "OS deployment to compute nodes (\"NODE1:DH49AC8012DEF,node2:DX4D01A8C1F0E5A\")
             has been started",
      "recovery": {
         "text": "",
         "URL": "",
      }
   }]
}
```

The following example is returned if the request is not successful.

```
{
   "result": "failed",
   "messages": [{
      "explanation": "",
      "id": "FQXHMFC0004M",
      "text": "An internal error occurred.",
      "recovery": {
         "text": "Attempt to perform the operation again. If the problem persists, contact
                Support.",
         "URL": ""
```

```
      }
   }]
}
```

/osdeployment/globalSettings

Use this REST API to retrieve or modify global operating-system deployment settings. *Global settings* serve as defaults settings when operating systems are deployed.

Global settings include
- The password for the administrator user account to be use for deploying the operating systems
- The method to use to assign IP addresses to servers
- License keys to use when activating the installed operating systems
- Optionally join an Active Directory domain as part of the Windows operating-system deployment

HTTP methods

GET, PUT

GET /osdeployment/globalSettings

Use this method to return the current global settings for operating-system deployment.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/osdeployment/globalSettings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
deploySettings	Object	Information about deployment settings
ipDuplicationCheckEnabled	Boolean	Indicates whether the duplicate-IP check runs at the beginning of an OS deployment. This can be one of the following values. • **true**. Duplicate-IP check runs • **false**. Duplicate-IP check does not run
stateTransitionTimeout	Integer	Amount of time, in seconds, to wait between status updates before failing the OS deployment
globalSetting	Object	Information about global settings
activeDirectory	Object	Information about Active Directory
allDomains	Array of objects	Information about all Active Directory domains
id	String	ID of the Active Directory domain
domainName	String	Name of the Active Directory domain
OU	String	Organizational unit of the Active Directory domain
defaultDomain	String	Name of the default domain. This is one of the Active Directory domains in the **AllDomains** list)
credentials	Array of objects	Information about user credentials
name	String	User name. This can be one of the following values. • **root**. For Linux and ESXi users. • **Administrator**. For Windows users
password	String	Encrypted password
type	String	Operating system type. This can be one of the following values. • **ESXi** • **LINUX** • **WINDOWS**
ipAssignment	String	Host network setting option for operating-system deployment. This can be one of the following values. • **dhcpv4** • **staticv4** • **staticv6**
isVLANMode	Boolean	Indicates whether VLAN mode is used. This can be one of the following values. • **true**. VLAN mode is used. • **false**. VLAN mode is not used.
licenseKeys	Object	Information about volume-license keys
win10	Object	Information about volume-license keys for Microsoft Windows 10
enterpriseLicenseKey	String	Volume-license key that is used to deploy the enterprise version of Microsoft Windows 10
workstationLicenseKey	String	Volume-license key that is used to deploy the workstation version of Microsoft Windows 10
win11	Object	Information about volume-license keys for Microsoft Windows 11
enterpriseLicenseKey	String	Volume-license key that is used to deploy the enterprise version of Microsoft Windows 11

Attributes	Type	Description
workstationLicenseKey	String	Volume-license key that is used to deploy the workstation version of Microsoft Windows 11
win2022r1	Object	Information about volume-license keys for Microsoft Windows 2022 R1
dataCenterLicenseKey	String	Volume-license key that is used to deploy the data center version of Microsoft Windows 2022 R1
standardLicenseKey	String	Volume-license key that is used to deploy the standard version of Microsoft Windows 2022 R1
win2019r1	Object	Information about volume-license keys for Microsoft Windows 2019 R1
dataCenterLicenseKey	String	Volume-license key that is used to deploy the data center version of Microsoft Windows 2019 R1
standardLicenseKey	String	Volume-license key that is used to deploy the standard version of Microsoft Windows 2019 R1
win2016r1	Object	Information about volume-license keys for Microsoft Windows 2016 R1
dataCenterLicenseKey	String	Volume-license key that is used to deploy the data center version of Microsoft Windows 2016 R1
standardLicenseKey	String	Volume-license key that is used to deploy the standard version of Microsoft Windows 2016 R1
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Message that is related to the result of the request
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned when the request is successful.

```
{
   "deploySettings": {
      "ipDuplicationCheckEnabled": false,
      "stateTransitionTimeout": 120
   },
   "globalSetting": {
      "activeDirectory": {
         "allDomains": [{
            "domainName": "domain1",
            "id": 0,
            "OU": "domain1-unit1"
         },
         {
```

```
            "domainName": "domain2",
            "id": 1,
            "OU": "domain2-unit"
         }],
         "defaultDomain": "domain2/domain2-unit"
      },
      "credentials": [{
         "passwordChanged": false,
         "password": null,
         "type": "ESXi"
      },
      {
         "passwordChanged": false,
         "password": null,
         "type": "LINUX"
      },
      {
         "passwordChanged": false,
         "password": null,
         "type": "RHEL/ESXi"
      },
      {
         "password": "U2FsdGVkX1/fiTzKhVZaIG4JcGBuCkoqucvGBmrjtK5/ejaLy8TFkFgb9AeDoZtt",
         "passwordChanged": false,
         "type": "WINDOWS"
      }],
      "deploySettings": {
         "ipDuplicationCheckEnabled": false,
         "stateTransitionTimeout": 120
      },
      "ipAssignment": "dhcpv4",
      "isVLANMode": false,
      "licenseKeys": {
         "win10": {
            "enterpriseLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
            "workstationLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
         },
         "win11": {
            "enterpriseLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
            "workstationLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
         },
         "win2022r1": {
            "dataCenterLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
            "standardLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
         },
         "win2019r1": {
            "dataCenterLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
            "standardLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
         },
         "win2016r1": {
            "dataCenterLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
            "standardLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
         }
      }
   }
}
```


PUT /osdeployment/globalSettings

Use this method to modify the current global settings for operating-system deployment.

Authentication

Authentication with username and password is required.

Request URL

```
PUT https://{management_server_IP}/osdeployment/globalSettings
```

Query parameters

None

Request body

Parameters	Required / Optional	Type	Description
activeDirectory	Required	Object	Information about Active Directory
allDomains	Required	Array of objects	Information about all Active Directory domains
domainName	Required	String	Name of the Active Directory domain
id	Required	String	ID of the Active Directory domain
OU	Required	String	Organizational unit of the Active Directory domain
defaultDomain	Required	String	Name of the default domain. This is one of the Active Directory domains in the **AllDomains** list).
credentials	Required	Array of objects	Information about user credentials
password	Required	String	Password of the operating system to be deployed For Windows 2012, this is the password for the “Administrator” user. For Linux and ESXi, this is the password for the “root” user.
passwordChanged	Required	Boolean	Indicates whether to modify the password. This can be one of the following values. • **true** • **false**
type	Required	String	Operating system type. This can be one of the following values. • **ESXi** • **LINUX** • **WINDOWS**
deploySettings	Optional	Object	Information about deployment settings
ipDuplicationCheckEnabled	Optional	Boolean	Indicates whether the duplicate-IP check runs at the beginning of an OS deployment. This can be one of the following values. • **true**. Duplicate-IP check runs • **false**. Duplicate-IP check does not run
stateTransitionTimeout	Optional	Integer	Amount of time, in seconds, to wait between status updates before failing the OS deployment
ipAssignment	Required	String	Host network setting option for operating system deployment. This can be one of the following values. • **dhcpv4** • **staticv4** • **staticv6**

Parameters	Required / Optional	Type	Description
isVLANMode	Required	String	Indicates whether VLAN mode is used. This can be one of the following values. • **true**. VLAN mode is used. • **false**. VLAN mode is not used.
licenseKeys	Required	Object	Information about volume-license keys
win11	Required	Object	Information about volume-license keys for Microsoft Windows 11
enterpriseLicenseKey	Required	String	Volume-license key that is used to deploy the enterprise version of Microsoft Windows 11
workstationLicenseKey	Required	String	Volume-license key that is used to deploy the workstation version of Microsoft Windows 11
win10	Required	Object	Information about volume-license keys for Microsoft Windows 10
enterpriseLicenseKey	Required	String	Volume-license key that is used to deploy the enterprise version of Microsoft Windows 10
workstationLicenseKey	Required	String	Volume-license key that is used to deploy the workstation version of Microsoft Windows 10
win2022r1	Required	Object	Information about volume-license keys for Microsoft Windows 2022 R1
dataCenterLicenseKey	Required	String	Volume-license key that is used to deploy the data center version of Microsoft Windows 2022 R1
standardLicenseKey	Required	String	Volume-license key that is used to deploy the standard version of Microsoft Windows 2022 R1
win2019r1	Required	Object	Information about volume-license keys for Microsoft Windows 2019 R1
dataCenterLicenseKey	Required	String	Volume-license key that is used to deploy the data center version of Microsoft Windows 2019 R1
standardLicenseKey	Required	String	Volume-license key that is used to deploy the standard version of Microsoft Windows 2019 R1
win2016r1	Required	Object	Information about volume-license keys for Microsoft Windows 2016 R1
dataCenterLicenseKey	Required	String	Volume-license key that is used to deploy the data center version of Microsoft Windows 2016 R1
standardLicenseKey	Required	String	Volume-license key that is used to deploy the standard version of Microsoft Windows 2016 R1

The following example modifies the global OS-deployment settings.

```
{
   "activeDirectory": {
      "allDomains": [{
         "domainName": "domain1",
         "id": 0,
         "OU": "domain1-unit1"
      },
      {
         "domainName": "domain2",
         "id": 1,
         "OU": "domain2-unit"
```

```
      }],
      "defaultDomain": "domain2/domain2-unit"
   },
   "credentials": [{
      "passwordChanged": false,
      "password": null,
      "type": "ESXi"
   },
   {
      "passwordChanged": false,
      "password": null,
      "type": "LINUX"
   },
   {
      "passwordChanged": false,
      "password": null,
      "type": "RHEL/ESXi"
   },
   {
      "password": "U2FsdGVkX1/fiTzKhVZaIG4JcGBuCkoqucvGBmrjtK5/ejaLy8TFkFgb9AeDoZtt",
      "passwordChanged": false,
      "type": "WINDOWS"
   }],
   "deploySettings": {
      "ipDuplicationCheckEnabled": false,
      "stateTransitionTimeout": 120
   },
   "ipAssignment": "dhcpv4",
   "isVLANMode": false,
   "licenseKeys": {
      "win10": {
         "enterpriseLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
         "workstationLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
      },
      "win11": {
         "enterpriseLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
         "workstationLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
      },
      "win2022r1": {
         "dataCenterLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
         "standardLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
      },
      "win2019r1": {
         "dataCenterLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
         "standardLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
      },
      "win2016r1": {
         "dataCenterLicenseKey": "AAAA4-BBBBB-CCCCC-DDDDD-EEEEE",
         "standardLicenseKey": "AAAA3-BBBBB-CCCCC-DDDDD-EEEEE"
      }
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned when the request is successful.

```
{
   "result": "success",
   "messages": [ ]
}
```

/osdeployment/hostSettings

Use this REST API to retrieve information about the network and storage settings for all servers, and create or modify the network and storage settings for one or more servers.

HTTP methods

GET, PUT, POST

GET /osdeployment/hostSettings

Use this method to return information about the network and storage settings for all servers.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/osdeployment/hostSettings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
hosts	Array of objects	Information about hosts settings for each server
networkSettings	Object	Information about network settings
dns1	String	Preferred DNS server for the host server to be used after the operating system is deployed
dns2	String	Alternative DNS server for the host server to be used after the operating system is deployed
gateway	String	Gateway of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings. To determine the IP mode, use GET /osdeployment/globalSettings.
hostname	String	Hostname of the host server If a hostname is not specified, a default hostname is assigned.
ipAddress	String	IP address of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings.
mtu	Long	Maximum transmission unit for the host to be used after the operating system is deployed

Attributes	Type	Description
prefixLength	String	Prefix length of the host IP address to be used after the operating system is deployed. This is used when the network setting is set to static IPv6 in the Global OS deployment settings.
selectedMAC	String	MAC address of the host server to which the IP address is to be bound The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment. VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only the MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server. To obtain the MAC address, use the macaddress **value** attribute in the GET /hostPlatforms method.
subnetMask	String	Subnet mask of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. To determine the IP mode, use the GET /osdeployment/globalSettings method.
vlanId	String	VLAN ID for operating-system VLAN tagging This attribute is valid only if in VLAN mode is enabled (see GET /osdeployment/globalSettings). **Important:** Only specify a VLAN ID when a VLAN tag is required to function on the network. Using VLAN tags can affect the network routability between the host operating system and the Lenovo XClarity Administrator.
selectedImage	String	Name of the selected OS image to be deployed
storageSettings	Object	Preferred storage location on which you want to deploy operating-system images
targetDevice	String	Target device. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always “localdisk.”

Attributes	Type	Description
uuid	String	UUID of the host platform
result	String	Result of the request. This can be one of the following values. • **Success**. The request was successful. • **Failed**. The request failed.
messages	Array	Information about the message that is related to the result of the request
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
message	String	Message text associated with the message identifier
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "hosts": [{
      "networkSettings": {
         "dns1": "",
         "dns2": "",
         "gateway": "",
         "hostname": "",
         "ipAddress": "",
         "mtu": 1500,
         "prefixLength": 0,
         "selectedMAC": "AUTO",
         "subnetMask": "",
         "vlanId": "2"
      },
      "storageSettings": {
         "targetDevice": "localdisk"
      },
      "uuid": "69BDF8912E5211E4998B40F2E99033F0",
   }],
   "result": "success",
   "messages": []
}
```

PUT /osdeployment/hostSettings

Use this method to modify the network and storage settings for one or more specific servers.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/osdeployment/hostSettings`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
networkSettings	Optional	Object	Information about network settings
dns1	Optional	String	Preferred DNS server for the host server to be used after the operating system is deployed
dns2	Optional	String	Alternative DNS server for the host server to be used after the operating system is deployed
gateway	Optional	String	Gateway of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
hostname	Optional	String	Hostname for the host server. If a hostname is not specified, a default hostname is assigned.
ipAddress	Optional	String	IP address of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings.
mtu	Optional	Long	Maximum transmission unit for the host to be used after the operating system is deployed
prefixLength	Optional	String	Prefix length of the host IP address to be used after the operating system is deployed. This is used when the network setting is set to **static IPv6** in the Global OS deployment settings.
selectedMAC	Optional	String	MAC address of the host server to which the IP address is to be bound The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment, and selectedMAC is set to the newly detected MAC address. VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only the MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server. **Tip:** To obtain the MAC address, use the **macaddress.value** attribute in GET /hostPlatforms.
subnetMask	Optional	String	Subnet mask of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.

Attributes	Required / Optional	Type	Description
vlanId	Optional	String	VLAN ID for operating-system VLAN tagging This attribute is valid only if in VLAN mode is enabled (see GET /osdeployment/globalSettings). **Important:** Only specify a VLAN ID when a VLAN tag is required to function on the network. Using VLAN tags can affect the network routability between the host operating system and the Lenovo XClarity Administrator.
selectedImage	Optional	String	Name of the selected OS image to be deployed
storageSettings	Optional	Object	Preferred storage location on which you want to deploy operating-system images
targetDevice	Optional	String	Target device. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always **localdisk**.
uuid	Required	String	UUID of the host platform

The following example modifies the network and storage settings for one or more specific servers.

```
[{
   "networkSettings": {
      "dns1": "",
      "dns2": "",
      "gateway": "",
      "hostname": "",
      "ipAddress": "",
      "mtu": 1500,
      "prefixLength": 0,
      "selectedMAC": "AUTO",
      "subnetMask": "",
      "vlanId": "2"
   },
   "storageSettings": {
      "targetDevice": "localdisk"
   },
   "uuid": "69BDF8912E5211E4998B40F2E99033F0"
```

```
}]
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Result of the request. This can be one of the following values. • **Success**. The request was successful. • **Failed**. The request failed.
messages	Array	Information about the message that is related to the result of the request
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
message	String	Message text associated with the message identifier
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": []
}
```

POST /osdeployment/hostSettings

Use this method to create the network and storage settings for one or more specific servers.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/osdeployment/hostSettings
```

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
networkSettings	Optional	Object	Information about network settings
dns1	Optional	String	Preferred DNS server for the host server to be used after the operating system is deployed
dns2	Optional	String	Alternative DNS server for the host server to be used after the operating system is deployed
gateway	Optional	String	Gateway of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
hostname	Optional	String	Hostname for the host server. If a hostname is not specified, a default hostname is assigned.
ipAddress	Optional	String	IP address of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings.
mtu	Optional	Long	Maximum transmission unit for the host to be used after the operating system is deployed
prefixLength	Optional	String	Prefix length of the host IP address to be used after the operating system is deployed. This is used when the network setting is set to **static IPv6** in the Global OS deployment settings.
selectedMAC	Optional	String	MAC address of the host server to which the IP address is to be bound The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment, and selectedMAC is set to the newly detected MAC address. VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only the MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server. **Tip:** To obtain the MAC address, use the **macaddress.value** attribute in GET /hostPlatforms.
subnetMask	Optional	String	Subnet mask of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.

Attributes	Required / Optional	Type	Description
vlanId	Optional	String	VLAN ID for operating-system VLAN tagging This attribute is valid only if in VLAN mode is enabled (see GET /osdeployment/globalSettings). **Important:** Only specify a VLAN ID when a VLAN tag is required to function on the network. Using VLAN tags can affect the network routability between the host operating system and the Lenovo XClarity Administrator.
selectedImage	Optional	String	Name of the OS image to be deployed
storageSettings	Optional	Object	Preferred storage location on which you want to deploy operating-system images
targetDevice	Optional	String	Target device. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always “localdisk.”
uuid	Required	String	UUID of the host platform

The following example creates the network and storage settings for one or more specific servers.

```
[{
   "networkSettings": {
      "dns1": "",
      "dns2": "",
      "gateway": "",
      "hostname": "",
      "ipAddress": "",
      "mtu": 1500,
      "prefixLength": 0,
      "selectedMAC": "AUTO",
      "subnetMask": "",
      "vlanId": "2"
   },
   "storageSettings": {
      "targetDevice": "localdisk"
   },
   "uuid": "69BDF8912E5211E4998B40F2E99033F0"
```

}]

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Result of the request. This can be one of the following values. • **Success**. The request was successful. • **Failed**. The request failed.
messages	Array	Information about the message that is related to the result of the request
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
message	String	Message text associated with the message identifier
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": []
}
```

/osdeployment/hostSettings/*{uuid}*

Use this REST API to retrieve information about, modify, or delete the network and storage settings for a specific server.

HTTP methods

GET, PUT, DELETE

GET /osdeployment/hostSettings/*{uuid}*

Use this method to return information about the network and storage settings for a specific server.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/osdeployment/hostSettings/{uuid}`

where *{uuid}* is the UUID of the server. To obtain the UUID, use the GET /nodes method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
host	Object	Information about host settings for the specified server
networkSettings	Object	Information about network settings
dns1	String	Preferred DNS server for the host server to be used after the operating system is deployed
dns2	String	Alternative DNS server for the host server to be used after the operating system is deployed
gateway	String	Gateway of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings. To determine the IP mode, use GET /osdeployment/globalSettings.
hostname	String	Hostname of the host server If a hostname is not specified, a default hostname is assigned.
ipAddress	String	IP address of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings.
mtu	Long	Maximum transmission unit for the host to be used after the operating system is deployed

Attributes	Type	Description
prefixLength	String	Prefix length of the host IP address to be used after the operating system is deployed. This is used when the network setting is set to static IPv6 in the Global OS deployment settings.
selectedMAC	String	MAC address of the host server to which the IP address is to be bound The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment. VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only the MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server. To obtain the MAC address, use the macaddress **value** attribute in the GET /hostPlatforms method.
subnetMask	String	Subnet mask of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. To determine the IP mode, use the GET /osdeployment/globalSettings method.
vlanId	String	VLAN ID for operating-system VLAN tagging This attribute is valid only if in VLAN mode is enabled (see GET /osdeployment/globalSettings). **Important:** Only specify a VLAN ID when a VLAN tag is required to function on the network. Using VLAN tags can affect the network routability between the host operating system and the Lenovo XClarity Administrator.
selectedImage	String	Name of the selected OS image to be deployed
storageSettings	Object	Preferred storage location on which you want to deploy operating-system images
targetDevice	String	Target device. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always “localdisk.”

Attributes	Type	Description
result	String	Result of the request. This can be one of the following values. • **Success**. The request was successful. • **Failed**. The request failed.
messages	Array	Information about the message that is related to the result of the request
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
message	String	Message text associated with the message identifier
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "hosts": {
      "networkSettings": {
         "dns1": "",
         "dns2": "",
         "gateway": "",
         "hostname": "",
         "ipAddress": "",
         "mtu": 1500,
         "prefixLength": 0,
         "selectedMAC": "AUTO",
         "subnetMask": "",
         "vlanId": "2"
      },
      "storageSettings": {
         "targetDevice": "localdisk"
      }
   },
   "result": "success",
   "messages": []
}
```

PUT /osdeployment/hostSettings/*{uuid}*

Use this method to modify the network and storage settings for a specific server.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/osdeployment/hostSettings/{uuid}`

where *{uuid}* is the UUID of the server. To obtain the UUID, use the GET /nodes method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
networkSettings	Optional	Object	Information about network settings
dns1	Optional	String	Preferred DNS server for the host server to be used after the operating system is deployed
dns2	Optional	String	Alternative DNS server for the host server to be used after the operating system is deployed
gateway	Optional	String	Gateway of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
hostname	Optional	String	Hostname for the host server. If a hostname is not specified, a default hostname is assigned.
ipAddress	Optional	String	IP address of the host server to be used after the operating system is deployed. This is used when the network setting is set to **static** in the Global OS deployment settings.
mtu	Optional	Long	Maximum transmission unit for the host to be used after the operating system is deployed
prefixLength	Optional	String	Prefix length of the host IP address to be used after the operating system is deployed. This is used when the network setting is set to **static IPv6** in the Global OS deployment settings.
selectedMAC	Optional	String	MAC address of the host server to which the IP address is to be bound The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment, and selectedMAC is set to the newly detected MAC address. VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only the MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server. **Tip:** To obtain the MAC address, use the **macaddress.value** attribute in GET /hostPlatforms.
subnetMask	Optional	String	Subnet mask of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.

Attributes	Required / Optional	Type	Description
vlanId	Optional	String	VLAN ID for operating-system VLAN tagging This attribute is valid only if in VLAN mode is enabled (see GET /osdeployment/globalSettings). **Important:** Only specify a VLAN ID when a VLAN tag is required to function on the network. Using VLAN tags can affect the network routability between the host operating system and the Lenovo XClarity Administrator.
selectedImage	Optional	String	Name of the selected OS image to be deployed
storageSettings	Optional	Object	Preferred storage location on which you want to deploy operating-system images
targetDevice	Optional	String	Target device. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always “localdisk.”

The following example modifies the network and storage settings for one or more specific servers.

```
{
   "networkSettings": {
      "dns1": "",
      "dns2": "",
      "gateway": "",
      "hostname": "",
      "ipAddress": "",
      "mtu": 1500,
      "prefixLength": 0,
      "selectedMAC": "AUTO",
      "subnetMask": "",
      "vlanId": "2"
   },
   "storageSettings": {
      "targetDevice": "localdisk"
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Result of the request. This can be one of the following values. • **Success**. The request was successful. • **Failed**. The request failed.
messages	Array	Information about the message that is related to the result of the request
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
message	String	Message text associated with the message identifier
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": []
}
```

DELETE /osdeployment/hostSettings/*{uuid}*

Use this method to delete all network and storage settings for a specific server.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/osdeployment/hostSettings/{uuid}`

where *{uuid}* is the UUID of the server. To obtain the UUID, use the GET /nodes method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
412	Precondition failed	Specified data is invalid because of missing values. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Result of the request. This can be one of the following values. • **Success**. The request was successful. • **Failed**. The request failed.
messages	Array	Information about the message that is related to the result of the request
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
message	String	Message text associated with the message identifier
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": []
}
```

/osdeployment/osInfo

Use this REST API to retrieve the information about the operating system that was deployed successfully by this Lenovo XClarity Administrator instance for each managed server.

HTTP methods

GET

GET /osdeployment/osInfo

Use this method to return information about the operating system that was deployed successfully by this Lenovo XClarity Administrator instance for each managed server.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/osdeployment/osInfo`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
items	Array of objects	Information about all operating systems that were deployed on managed server using this XClarity Administrator instance
deployStatus	String	Deployment status. This can be the following value. • **OS Installation Completed** **Note:** Results for only successful deployments are currently saved.
hostname	String	Hostname that is used for the host server
installedOS	String	OS profile that is deployed on the host server
name	String	Name of the host server
networkSettings	Object	Information about network settings
dns1	String	Preferred DNS server for the host server
dns2	String	Alternative DNS server for the host server
gateway	String	Gateway of the host server. This is used when the network setting is set to “static” in the Global OS deployment settings.

Attributes	Type	Description
ipAddress	String	IP address of the host server. This is used when the network setting is set to “static” in the Global OS deployment settings.
ipMode	String	Method for assigning IP addresses for operating-system deployment. This can be one of the following values. • **dhcpv4** • **staticv4** • **staticv6**
macAddress	Long	Information about the MAC address
mtu	Long	Maximum transmission unit for the host
prefixLength	String	Prefix length of the host IP address. This is used when the network setting is set to “static IPv6” in the Global OS deployment settings.
subnetMask	String	Subnet mask of the host server. This is used when the network setting is set to static in the Global OS deployment settings.
vlanId	String	VLAN ID for operating-system VLAN tagging This attribute is valid only if in VLAN mode is enabled (see GET /osdeployment/globalSettings).
storageSettings	Object	Information about the storage location on which the operating-system image is deployed
label	String	Storage location on which operating system image is deployed. This can be one of the following values. • **Local disk** • **Embedded USB Hypervisor** • **M.2drive** • **SAN storage**
value	String	Storage location on which operating system image is deployed. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always “localdisk.”
uuid	String	UUID of the host server
result	String	Result of the request. This can be one of the following values. • **Success**. The request was successful. • **Failed**. The request failed.
messages	Array	Information about the message that is related to the result of the request

Attributes			Type	Description
	explanation		String	Additional information to clarify the reason for the message
	id		String	Message identifier of a returned message
	message		String	Message text associated with the message identifier
	recovery		Array	Recovery information
		text	String	User actions that can be taken to recover from the event
		URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.


```
{
   "items": [{
      "deployStatus": "OS Installation Completed",
      "hostname": "nodeC",
      "installedOS": "win2019-x86_64-install-Standard",
      "name": "Mehlow-SR250-2",
      "networkSettings": [{
         "dns1": "",
         "dns2": "",
         "gateway": "10.240.210.1",
         "ipAddress": "10.240.210.154",
         "ipMode": "staticv4",
         "macAddress": "AUTO",
         "mtu": 1500,
         "subnetMask": "255.255.254.0"
      }],
      "storageSettings": {
         "label": "Local Disk Drive",
         "value": "localdisk"
      },
      "uuid": "C3050752827D4AD8B4D5AE60B332C4BD"
   },
   {
      "deployStatus": "OS Installation Completed",
      "hostname": "node750CE30C694",
      "installedOS": "win2019-x86_64-install-Standard_core",
      "name": "Mehlow-SR150-2",
      "networkSettings": [{
         "dns1": "",
         "dns2": "",
         "ipMode": "dhcpv4",
         "macAddress": "AUTO",
         "mtu": 1500
      }],
      "storageSettings": {
         "label": "Local Disk Drive",
         "value": "localdisk"
      },
      "uuid": "750CE30C694745BCB4631ADBEA3C66C9"
   }],
   "result": "success",
   "messages": []
}
```

/osdeployment/osInfo/*{uuid_list}*

Use this REST API to retrieve the information about the operating system that was deployed successfully by this Lenovo XClarity Administrator instance for a specific managed server.

HTTP methods

GET

GET /osdeployment/osInfo/*{uuid_list}*

Use this method to return information about the operating system that was deployed successfully by this Lenovo XClarity Administrator instance for a specific managed server

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/osdeployment/osInfo/{uuid_list}`

where *{uuid_list}* is one or more UUIDs of managed servers, separated by a comma. To obtain the UUIDs, use the GET /nodes.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
items	Array of objects	Information about all operating systems that were deployed on managed server using this XClarity Administrator instance
deployStatus	String	Deployment status. This can be the following value. • **OS Installation Completed** **Note:** Results for only successful deployments are currently saved.

Attributes	Type	Description
hostname	String	Hostname that is used for the host server
installedOS	String	OS profile that is deployed on the host server
name	String	Name of the host server
networkSettings	Object	Information about network settings
dns1	String	Preferred DNS server for the host server
dns2	String	Alternative DNS server for the host server
gateway	String	Gateway of the host server. This is used when the network setting is set to “static” in the Global OS deployment settings.
ipAddress	String	IP address of the host server. This is used when the network setting is set to “static” in the Global OS deployment settings.
ipMode	String	Method for assigning IP addresses for operating-system deployment. This can be one of the following values. • **dhcpv4** • **staticv4** • **staticv6**
macAddress	Long	Information about the MAC address
mtu	Long	Maximum transmission unit for the host
prefixLength	String	Prefix length of the host IP address. This is used when the network setting is set to “static IPv6” in the Global OS deployment settings.
subnetMask	String	Subnet mask of the host server. This is used when the network setting is set to static in the Global OS deployment settings.
vlanId	String	VLAN ID for operating-system VLAN tagging This attribute is valid only if in VLAN mode is enabled (see GET /osdeployment/globalSettings).
storageSettings	Object	Information about the storage location on which the operating-system image is deployed
label	String	Storage location on which operating system image is deployed. This can be one of the following values. • **Local disk** • **Embedded USB Hypervisor** • **M.2drive** • **SAN storage**

Attributes	Type	Description
value	String	Storage location on which operating system image is deployed. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always “localdisk.”
uuid	String	UUID of the host server
result	String	Result of the request. This can be one of the following values. • **Success**. The request was successful. • **Failed**. The request failed.
messages	Array	Information about the message that is related to the result of the request
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
message	String	Message text associated with the message identifier
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.


```
{
   "items": [{
      "deployStatus": "OS Installation Completed",
      "hostname": "nodeC",
      "installedOS": "win2019-x86_64-install-Standard",
      "name": "Mehlow-SR250-2",
      "networkSettings": [{
         "dns1": "",
         "dns2": "",
         "gateway": "10.240.210.1",
         "ipAddress": "10.240.210.154",
         "ipMode": "staticv4",
         "macAddress": "AUTO",
         "mtu": 1500,
         "subnetMask": "255.255.254.0"
      }],
      "storageSettings": {
         "label": "Local Disk Drive",
         "value": "localdisk"
```

```
      },
      "uuid": "C3050752827D4AD8B4D5AE60B332C4BD"
   },
   "result": "success",
   "messages": []
}
```

/osImages

Use this REST API to retrieve information about and create a job to import OS images, OS-image profiles, device driver, boot files, and custom files (such as configuration settings, installation scripts, software, and unattend files) , or to customize an OS-image profile.

To import a new file, follow these steps:

1. Start a job to import the file using POST /osImages.
2. Import the file using POST /files/osImages?jobId=*{job_id}* method, where the job ID is the ID that was returned in step 1.
3. Monitor the status of the import job using GET /tasks/*{job_list}*, where the job ID is the ID that was returned in step 1.

When you import an OS image, Lenovo XClarity Administrator creates one or more OS-image profiles in the OS image repository. The profile includes both the OS image and the installation options for that image.

HTTP methods

GET, POST

GET /osImages

Use this method to return information about the OS images and OS-image profiles, including the associated device drivers, boot-options files, and custom files (such as configuration settings, installation scripts, software, and unattend files), that are loaded in the Lenovo XClarity Administrator OS-images repository.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/osImages
```

Query parameters

Parameters	Required / Optional	Description
imageType=OSPROFILE	Optional	Returns information for specific OS-image profiles
id=*{id_list}*	Optional	Returns information for specific OS-image profiles, specified by ID. Separate multiple IDs using a comma. To obtain the ID, use the GET /osImages method.

The following example returns information for all OS-image profiles.

```
GET https://192.0.2.0/osImages
```

The following example returns information only for the OS-image profile with the specified ID.

```
GET https://192.0.2.0/osImages
```

```
?imageType=OSPROFILE&id=win2012r2|win2012r2-x86_64-install-Datacenter_Virtualization
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attention: The **drivers** response attribute and its child attributes are not supported in Lenovo XClarity Administrator v1.3.0 and later.

Attributes	Type	Description
bootFiles	Array of object	List of boot-option files that are imported and available to the OS image profiles
bundleId	String	ID of the OS bundle from which the boot file was imported
description	String	Boot-option file description
id	String	Boot-option file identifier
name	String	Boot-option file name
os	String	The operating system that is associated with the boot-options file. This can be one of the following values. • **win**
osrelease	String	Operating system release that supports the device driver.
size	Integer	Size, in KB, of the boot-options file
type	String	Type of boot-options file. This can be one of the following values. • **custom**. The file was manually imported and added to a customized OS-images profile. • **predefined**. The file was preloaded by XClarity Administrator.
version	String	Boot-options file version (for example, v1 or v2)
bundleFiles	Array of object	List of bundle files that are imported and available to the OS image profiles
description	String	Description of the bundle file
id	String	ID of the bundle file
name	String	Name of the bundle file
os	String	The operating system that is associated with the bundle file. This can be one of the following values. • **win**
osrelease	String	Operating system release that supports the bundle file

Attributes	Type	Description
releasedate	String	Release date of the bundle file
size	String	Size, in MB, of the bundle file
version	String	Version of the bundle file (for example, v1 or v2)
customConfigFiles	Array of objects	List of configuration-settings files that are imported and available to the OS image profiles
associatedFileId	String	ID of the unattend file that was optionally associated with the configuration-settings file
content	String	Contents of the configuration-settings file
customMacros	Array of objects	List of custom macros that are derived from the configuration-settings file
macroName	String	Name of the macro
description	String	Description of the configuration-settings file
id	String	ID of the configuration-settings file
name	String	Name of the configuration-settings file
os	String	Operating system that is associated with the configuration-settings file. This can be one of the following values. • **esxi** • **rhel** • **sles** • **win**
osrelease	String	Operating system release
type	String	Type of boot-options file. This can be one of the following values. • **custom**. The file was manually imported and added to a customized OS-images profile. • **predefined**. The file was preloaded by Lenovo XClarity Administrator.
version	String	Version of the configuration-settings file
diskUsage	Object	Information about disk usage
bootFileDiskUsage	Long	Disk space that is used by the boot-options files (such as WinPE)
configFileDiskUsage	Long	Disk space that is used by the configuration-settings files
deviceDriverDiskUsage	Long	Disk space that is used by the disk drivers
osImageDiskUsage	Long	Disk space that is used by only the operating-system image.
scriptFileDiskUsage	Long	Disk space that is used by the installation-script file
softwareFileDiskUsage	Long	Disk space that is used by the software files
totalDiskUsage	Long	Total amount of disk space used.
unattendFileDiskUsage	Long	Disk space that is used by the unattend files
driverFiles	Array of object	List of device drivers that are imported and available to the OS image profiles

Attributes	Type	Description
bundleId	String	ID of the OS bundle from which the boot file was imported
description	String	Device driver description
devicetype	String	Device driver adapter type. This can be one of the following values. • **nic**. Network interface adapter • **storage**. Storage adapter, such as SAS or RAID • **hba**. Fibre Channel adapter • **other**. Other adapters, such as chipset device adapters
id	String	Device driver identifier
name	String	Device driver name
os	String	Operating system that is associated with the boot-options file. This can be one of the following values. • **esxi** • **rhel** • **sles** • **win**
osrelease	String	Operating system release that supports the device driver
type	String	Type of device driver. This can be one of the following values. • **custom**. The file was manually imported and added to a customized OS-images profile. • **predefined**. The file was preloaded by Lenovo XClarity Administrator.
version	String	Device driver version (for example, v1, v2, etc.)
installScriptFiles	Array of objects	List of installation-script files that are imported and available to the OS-image profile Currently, only post-installation scripts are supported.
description	String	Installation-script description
id	String	Installation-script identifier
name	String	Installation-script file name
os	String	Operating system that is associated with the installation-script file. This can be one of the following values. • **esxi** • **rhel** • **sles** • **win**
type	String	Type of installation-script file. This can be one of the following values. • **custom**. The file was manually imported and added to a customized OS-images profile. • **predefined**. The file was preloaded by Lenovo XClarity Administrator.
version	String	Version of the installation-script
isAuthorized	Boolean	Indicates whether the user is assigned a role that can manage and deploy an operating system. This can be one of the following values. • **true**. The user is authorized. • **false**. The user is not authorized

Attributes	Type	Description
items	Array of objects	Information about each operating-system image
description	String	Description for the operating system image
deployStatus	String	Deployment status of the operating system image. This can be one of the following values. • **ready**. The operating system can be deployed. A matching WinPE image is in the OS-images repository, and all Windows profiles are using a custom WinPE image. • **warning**. The operating system can be deployed; however, there is a potential issue with the OS image. – An unsupported WinPE file is in the OS-images repository, and one or more profiles are using the unsupported WinPE file. – The operating system is not compatible with Thinksystem servers. • **notReady**. The operating system cannot be deployed because a matching WinPE image is not in the OS-images repository. **Notes:** – The deployStatus for placeholder profiles is always set to “Not Ready.” – If the **deployStatus** is “Not Ready,” use the **readyCheck** attribute to get information to help resolve the problem.
id	String	ID of the OS image
isCustomizedISO	Boolean	Indicates whether the OS image is customized. This can be one of the following values. • **true**. This is a custom image. • **false**. This is a base image.
name	String	Name of the OS image
osBuildId	String	Build number of the operating-system image
osrelease	String	Release for the operating system
profiles	Array of objects	Information about one or more OS profiles
attributes	Array of strings	
customizationOptions	Object	Information about all options that can be customized in this operating system If the base operating system for the profile does not support customization, this attribute is null. If the base operating system for the profile supports customization but does support certain child attributes, the unsupported chile attributes are returned as empty strings.
bootOptions	Object	Information about predefined and imported boot-options files that are associated with this customized OS image profile

Attributes	Type	Description
bootFileIds	Array of strings	Boot-options file IDs that correlate to the imported boot-options files Use POST /osImages to import the boot-options file, and then use POST /files/osImages?jobId={job_id} to import the boot-options file into the OS images repository.
customConfigOptions	Object	Information about the custom configuration settings that are associated with this customized OS-image profile
customConfigFileIds	Array of strings	List of IDs for each configuration-settings file that is associated with the OS-image profile
customSoftwareOptions	Object	Information about custom software payloads that are associated with this customized OS image profile
customSoftwareIds	Array of strings	List of IDs for each software payload that is associated with the OS-image profile
customType	Integer	Customization type. This can be one of the following values. • **1**. Custom unattend file and associated custom config file. • **2**. Custom unattend file only. • **3**. Custom unattend file and custom config file. • **4**. Custom config file only. • **5**. No custom unattend or config file.
deployDataAndSoftwareLocation	String	Path to the extracted software payload, custom files, and deployment data (such as certificates and logs) on the deployment host. The following directories are used by default. • **Linux**: `/home/lxca` • **Windows**: `c:\lxca`
driverOptions	Object	Information about predefined and imported device drivers that are associated with this customized OS image profile
driverFileIds	Array of strings	Device driver file IDs that is associated with the OS-image profile Use POST /osImages to import the device drivers, and then use POST /files/osImages?jobId={job_id} to import the device drivers into the OS images repository.
installScriptOptions	Object	Information about installation-script files associated with this customized OS image profile
scriptFileIds	Array of strings	List of IDs for each installation-script file that is associated with the OS-image profile Use POST /osImages to import the Installation-script files, and then use POST /files/osImages?jobId={job_id} to import the installation-script files into the OS-images repository.
unattendOptions	Array of objects	Information about unattend files that are associated with this customized OS-image profile
unattendFileIds	Array of strings	List of IDs for each unattend file that is associated with the OS-image profile

Attributes	Type	Description
deployStatus	String	Deployment status of the operating system image. This can be one of the following values. • **ready**. The operating system can be deployed. A matching WinPE image is in the OS-images repository, and all Windows profiles are using a custom WinPE image. • **warning**. The operating system can be deployed; however, there is a potential issue with the OS image. – An unsupported WinPE file is in the OS-images repository, and one or more profiles are using the unsupported WinPE file. – The operating system is not compatible with Thinksystem servers. • **notReady**. The operating system cannot be deployed because a matching WinPE image is not in the OS-images repository. **Notes:** – The deployStatus for placeholder profiles is always set to “Not Ready.” – If the **deployStatus** is “Not Ready,” use the **readyCheck** attribute to get information to help resolve the problem.
description	String	A description for the OS profile
id	String	The operating-system image profile ID. This ID is made up of the OS-image name and image-profile name separated by a bar (for example, `sles12.2|sles12.2-x86_64-install-Basic`).
isAllowedInCurrentSecurityMode	Boolean	**Note:** This attribute will be deprecated in a future release. Use **items.readyCheck.isNotAllowedInCurrentSecurityMode** instead
isCustomizedISO	Boolean	Indicates whether the OS image is customized. This can be one of the following values. • **true**. This is a custom image. • **false**. This is a base image.
name	String	Name of the OS profile
osBuildId	String	
osrelease	String	
readyCheck	Object	Information about the whether the OS-image profile is ready for deployment
incompatibleWithThinksystem	Boolean	Indicates whether the OS-image profile is not compatible with ThinkSystem servers. This can be one of the following values. • **true**. The profile is not compatible with ThinkSystem servers • **false**. The profile is compatible with ThinkSystem servers
isPlaceholder	Boolean	Indicates whether the OS-image profile is a placeholder. This can be one of the following values. • **true**. The profile is a placeholder • **false**. The profile is not a placeholder

Attributes	Type	Description
noPackages	Boolean	Indicates whether the SLES 15 installer image has corresponding packages file imported for deployment. If the profile is not for SLES 15, you can ignore this attribute. This can be one of the following values. • **true**. The packages image does not exist. • **false**. The packages image exists.
noWinpe	Boolean	Indicates whether the OS-image profile does not use a WinPE boot file. If the profile is not Windows, you can ignore this attribute. This can be one of the following values. • **true**. The profile does not use a WinPE boot file • **false**. The profile uses a WinPE boot file.
preloadedWinpe	Boolean	Indicates whether the OS-image profile uses a preloaded WinPE boot file. If the profile is not for Windows, you can ignore this attribute. This can be one of the following values. • **true**. The profile does not use a preloaded WinPE bootoptions file • **false**. The profile uses a preloaded WinPE boot file.
requiresThinksystemKiso	Boolean	Indicates whether the SLES image requires a kISO image to be compatible with ThinkSystem servers. This can be one of the following values. If the profile is not for SLES, you can ignore this attribute. • **true**. A kISO image is required. • **false**. A kISO image is not required.
supportedOsRelease	String	Operating-system release that is supported by the OS profile
type	String	The type of OS profile. This can be one of the following values. • **custom**. The profile was created when a boot file or device driver was manually uploaded and added to an operating system. • **predefined**. The profile was preloaded by Lenovo XClarity Administrator.
readyCheck	Object	Information about the whether the OS image is ready for deployment
isNotAllowedInCurrentSecurityMode	Boolean	Indicates whether the OS profile is supported in the current security mode. For customized OS image profiles, this indicates the security mode of the base operating system. This can be one of the following values. • **true**. The OS profile is not supported in the current security mode • **false**. The OS profile is supported in the current security mode
incompatibleWithThinksystem	Boolean	Indicates whether the OS image is not compatible with ThinkSystem servers. This can be one of the following values. • **true**. The OS image is not compatible with ThinkSystem servers • **false**. The OS image is compatible with ThinkSystem servers
size	Integer	Size, in KB, of the OS-image file

Attributes	Type	Description
supportedOsRelease	String	Operating-system release that is supported by the OS profile
type	String	Type of OS image. This can be one of the following values. • **custom**. The OS image does not contain predefined profiles. Custom profiles must be used to deploy this image. • **base**. The OS image contains only predefined profiles. Custom and predefined profiles can be used to deploy this image.
lastRefreshed	String	Timestamp of the last predefined OS-image repository refresh
number	Integer	Number of OS images
predefinedMacros	Array of objects	List of predefined macros (configurable settings) that are provided by XClarity Administrator
macroName	String	Name of the macro
softwareFiles	Array of objects	List of custom software payloads that are imported and available to the OS image profiles
description	String	Description of the software payload
id	String	ID of the software payload
name	String	Name of the software payload
os	String	Operating system that is associated with the software payload. This can be one of the following values. • **esxi** • **rhel** • **sles** • **win**
osrelease	String	Operating system release
size	Integer	Size, in KB, of the software-payload file
type	String	Type of software payload. This can be one of the following values. • **custom**. The file was manually imported and added to a customized OS-images profile. • **predefined**. The file was created by Lenovo.
version	String	Version of the software payload
supportedImages	Array of objects	Information about each supported operation system image
allowCustomBootFile	String	Indicates whether the specified image supports custom boot files. This can be one of the following values. • **true**. Customizing boot files is supported. • **false**. Customizing boot files is not supported.

Attributes	Type	Description
allowCustomConfigFile	String	Indicates whether the specified image supports custom configuration settings. This can be one of the following values. • **true**. Custom configuration settings are supported. • **false**. Custom configuration settings are not supported. **Note:** If **name** is rhels, this value must be false.
allowCustomDriver	String	Indicates whether the specified image supports custom device drivers. This can be one of the following values. • **true**. Customizing device drivers is supported. • **false**. Customizing device drivers is not supported.
allowCustomInstallScriptFile	String	Indicates whether the specified image supports custom installation script files. This can be one of the following values. • **true**. Customizing installation script files is supported. • **false**. Customizing installation script files is not supported.
allowCustomPath	String	Indicates whether the specified image supports a custom data and files path. This can be one of the following values. • **true**. Customizing the data and files path is supported. • **false**. Customizing the data and files path is not supported.
allowCustomSoftwareFile	String	Indicates whether the specified image supports custom software files. This can be one of the following values. • **true**. Custom software files are supported. • **false**. Custom software files are not supported.
allowCustomUnattendFile	String	Indicates whether the specified image supports custom unattend files. This can be one of the following values. • **true**. Custom unattend files are supported. • **false**. Custom unattend files are not supported. **Note:** If **name** is rhels, this value must be false.
allowedBootFileExtension	Array of strings	List of file extensions that are permitted for custom boot files. This can be one or more of the following values. • **zip**
allowedBundleFileExtension	Array of strings	List of file extensions that are permitted for bundle files. This can be one or more of the following values. • **zip**
allowedConfigFileExtension	Array of strings	List of file extensions that are permitted for custom configuration settings files. This can be one or more of the following values. • **json**
allowedDriverFileExtension	Array of strings	List of file extensions that are permitted for custom device drivers. This can be one or more of the following values. • **iso** • **rpm** • **vib** • **zip**

Attributes	Type	Description
allowedScriptFileExtension	Array of strings	List of file extensions that are permitted for custom installation scripts. This can be one or more of the following values. • **cmd** • **pl** • **pm** • **ps1** • **psm1** • **py** • **sh**
allowedSoftwareFileExtension	Array of strings	List of file extensions that are permitted for custom software. This can be one or more of the following values. • **tar.gz** • **zip**
allowedUnattendFileExtension	Array of strings	List of file extensions that are permitted for custom unattend files. This can be one or more of the following values. • **cfg** • **xml**
customBootReleases	Array of strings	List of specific OS releases that are supported for custom boot files **Note:** If **allowCustomBootFile** is false, this value is empty.
customConfigReleases	Array of strings	List of specific OS releases that are supported for custom configuration settings **Note:** If **allowCustomConfigFile** is false, this value is empty.
customDriverReleases	Array of strings	List of specific OS releases that are supported for custom device drivers **Note:** If **allowCustomDriver** is false, this value is empty.
customInstallScriptReleases	Array of strings	List of specific OS releases that are supported for custom installation script files **Note:** If **allowCustomInstallScriptFile** is false, this value is empty.
customSoftwareReleases	Array of strings	List of specific OS releases that are supported for custom software files **Note:** If **allowCustomSoftware** is false, this value is empty.
customUnattendReleases	Array of strings	List of specific OS releases that are supported for custom unattend files **Note:** If **allowCustomUnattendFile** is false, this value is empty.
displayName	String	Display name for the specified image, in English only
name	String	OS image name. This can be one of the following values. • **esxi** • **rhels** • **sles** • **ubuntu** • **win**
releases	Array of objects	List of specific releases that are supported for the specified image

Attributes	Type	Description
unattendFiles	Array of objects	List of unattend files that are imported and available to the OS image profiles. A custom unattend file can only be associated with 1 profile.
associatedFileId	String	ID of the custom schema file that was optionally associated with the unattend file
content	String	Content of the unattend file
description	String	Description of the unattend file
id	String	ID of the unattend file
name	String	Name of the unattend file
os	String	Operating system that is associated with the unattend file. This can be one of the following values. • **esxi** • **rhel** • **sles** • **win**
osrelease	String	Operating system release
type	String	Type of unattend file. This can be one of the following values. • **custom**. The file was manually uploaded and added to an operating system. • **predefined**. The file was preloaded by XClarity Administrator.
version	String	Version of the unattend file
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Object	Information about one or more messages If the result is successful, an empty array is returned.
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful for a base operating system image.

```
{
   "bootdFiles": [{
      "description": "Predefined WinPE wim file for Windows Server 2012 and 2016",
      "failedToLoad": false,
      "id": "winpe-64-base",
      "name": "WinPE_64",
      "os": "win",
```

```
      "osrelease": "2012,2012r2,2016,2016v1709",
      "size": 480224,
      "type": "Predefined",
      "version": "1"
   }],
"bundleFiles": [{
      "description": "LXCA-provided WinPE and drivers for Windows Server 2016",
      "id": "win2016-bundle",
      "minlxcarelease": "210",
      "name": "Windows Server 2016 Driver and Boot File Bundle",
      "os": "win",
      "osrelease": "2016",
      "releasedate": "2018-01-16",
      "size": "454 MB",
      "version": "1"
   }],
   "customConfigFiles": [{
      "associatedFileId": "",
      "content": "{\"category\": \"dynamic\",\r\n \"content\": [{\r\n \"category\": \"dynamic\",\r\n …}"
      "customMacros": [
         { "macroName": "server-settings.node.fileserver" },
         { "macroName": "server-settings.node.lampserver" },
         { "macroName": "server-settings.node.mailserver" },
         { "macroName": "timezone"}
      ],
      "description": "",
      "id": "2018012943821_SLES_customConfigInstallPackages.json",
      "name": "SLES_customConfigInstallPackages",
      "os": "sles",
      "osrelease": "",
      "type": "Custom",
      "version": ""
   },
   {
      "associatedFileId": "",
      "content": "{\"category\": \"dynamic\",\r\n \"content\": [{\r\n \"category\": \"dynamic\",\r\n …}"
      "customMacros": [
         { "macroName": "server-settings.node.keyboardLocale" },
          { "macroName": "server-settings.node.locale" }
      ],
      "description": "",
      "id": "2018012943854_SLES_customConfigLocale.json",
      "name": "SLES_customConfigLocale",
      "os": "win",
      "osrelease": "",
      "type": "Custom",
      "version": ""
   }],
   "diskUsage": {
      "bootFileDiskUsage": 436856,
      "configFileDiskUsage": 36,
      "deviceDriverDiskUsage": 420723,
      "osImageDiskUsage": 5974153,
      "scriptFileDiskUsage": 20
      "softwareFileDiskUsage": 224284,
      "totalDiskUsage": 7056100,
      "unattendFileDiskUsage": 28,
   },
   "driverFiles": [{
      "description": "LSI MPT3 SAS v8.00.00.00_k3.12.28-4-4 storage driver for SLES 12",
      "devicetype": "storage",
```

```
   "failedToLoad": false,
   "hwplatform": "immv2,thinkserver",
   "id": "storage-broadcom-mpt3sas-sles12",
   "name": "lsi-mpt3sas-kmp-default-8.00.00.00_k3.12.28_4-4.x86_64",
   "os": "sles",
   "osrelease": "12",
   "type": "Predefined",
   "version": "1",
},
...,
{
   "description": "Matrox Video v4.11.0 for RHEL 7.3",
   "devicetype": "other",
   "failedToLoad": false,
   "hwplatform": "immv3",
   "id": "other-matrox-rhel73",
   "name": "dd-mgag200-4.11.0_dup7.3-5.el7_3",
   "os": "rhels",
   "osrelease": "7.3",
   "type": "Predefined",
   "version": "1",
}],
"installScriptFiles": [{
   "description": "",
   "id": "2018012943624_install_custom_sw.sh",
   "name": "install_custom_sw",
   "os": "sles",
   "type": "Custom",
   "version": ""
},
{
   "description": "",
   "id": "2018012943641_Windows_sw-installScript.ps1",
   "name": "Windows_sw-installScript",
   "os": "win",
   "type": "Custom",
   "version": ""
}],
"isAuthorized": true,
"items": [{
   "description": "",
   "deployStatus": "ready",
   "id": "win2016|",
   "isCustomizedISO": false,
   "name": "win2016",
   "osBuildId": "",
   "osrelease": "2016",
   "profiles": [{
      "attributes": [],
      "customizationOptions": {
         "bootOptions": {
            "bootFileIds": ["winpe-64-base"]
         },
         "deployDataAndSoftwareLocation": "C:\\lxca"
         "driverOptions": {
            "driverFileIds": [
               "nic-broadcom-bnxtnd-win2016",
               "storage-broadcom-megasas35-win2016",
               ...,
               "storage-brdcm-dd-megaraid5-win2016",
               "other-mrvl-utl-dd-win2016"
```

```
            ]
         }
      },
      "description": "",
      "deployStatus": "ready",
      "id": "win2016|win2016-x86_64-install-Datacenter",
      "isAllowedInCurrentSecurityMode": true,
      "isCustomizedISO": false,
      "name": "win2016-x86_64-install-Datacenter",
      "osBuildId": "",
      "osrelease": "",
      "readyCheck": [{
         "incompatibleWithThinksystem": true,
         "isPlaceholder": true,
         "noWinpe": true,
         "preloadedWinpe": true
      }]
      "type": "predefined"
   },
   ...,
   ],
   "readyCheck": [{
      "isAllowedInCurrentSecurityMode": true,
      "incompatibleWithThinksystem": true,
      "requiresThinksystemKiso": true
   }]
   "size": 7624844,
   "type": "base"
}],
"lastRefreshed": "",
"number": 1,
"predefinedMacros": [
   { "macroName": "predefined.hostPlatforms" },
   { "macroName": "predefined.hostPlatforms.licenseKey" },
   ...,
   { "macroName": "predefined.unattendSettings.postinstallConfig" },
   { "macroName": "predefined.unattendSettings.reportWorkloadNotComplete" }
],
"softwareFiles": [{
   "description": "",
   "id": "2018012943447_jre-8u151-linux-x64.tar.gz",
   "name": "jre-8u151-linux-x64",
   "os": "sles",
   "osrelease": "",
   "size": 8596,
   "type": "Custom",
   "version": ""
},
{
   "description": "",
   "id": "2018012943535_eclipse-4.6.3-3.1.x86_64.tar.gz",
   "name": "eclipse-4.6.3-3.1.x86_64",
   "os": "sles",
   "osrelease": "",
   "size": 8789,
   "type": "Custom",
   "version": ""
}],
"supportedImages": [{
   "allowCustomBootFile": "false",
   "allowCustomConfigFile": "false",
```

```
    "allowCustomDriver": "true",
    "allowCustomInstallScriptFile": "false",
    "allowCustomSoftwareFile": "false",
    "allowCustomUnattendFile": "false",
    "customBootReleases": [],
    "customConfigReleases": [],
    "customDriverReleases": ["6.2", "6.3", "6.4", "6.5", "6.6", ... "7.5"],
    "customInstallScriptReleases": [],
    "customSoftwareReleases": [],
    "customUnattendReleases": [],
    "displayName": "Red Hat Enterprise Linux",
    "name": "rhels",
    "releases": [
       { "6.2": ["IMM2", "thinkserver"] },
       { "6.3": ["IMM2", "thinkserver"] },
       ...,
       { "7.4": ["IMM2", "thinkserver",   "IMM3v1"] },
       { "7.5": ["IMM2", "thinkserver",   "IMM3v1"] }
    ]
},
...,
{
    "allowCustomBootFile": "false",
    "allowCustomConfigFile": "false",
    "allowCustomDriver": "false",
    "allowCustomInstallScriptFile": "false",
    "allowCustomSoftwareFile": "false",
    "allowCustomUnattendFile": "false",
    "customBootReleases": [],
    "customConfigReleases": [],
    "customDriverReleases": [],
    "customInstallScriptReleases": [],
    "customSoftwareReleases": [],
    "customUnattendReleases": [],
    "displayName": "VMWare ESXi",
    "name": "esxi",
    "releases": [
       { "5.1": ["IMM2", "thinkserver"] },
       { "5.1U1": ["IMM2", "thinkserver"] },
       ...,
       { "6.5U1": ["IMM2", "thinkserver", "IMM3v1"] },
       { "6.7": ["IMM2", "thinkserver", "IMM3v1"] }
    ]
}],
"unattendFiles": [{
    "associatedFileId": "",
    "content": "<?xml version=\"1.0\"?>\r\n\r\n<!DOCTYPE profile SYSTEM \"\/usr\/share\/YaST2\    ",
    "description": "",
    "id": "2018012943724_Windows_customUnattendInstallFeatures.xml",
    "name": "Windows_customUnattendInstallFeatures",
    "os": "win",
    "osrelease": "",
    "type": "Custom",
    "version": "",
},
{
    "associatedFileId": "",
    "content": "<?xml version=\"1.0\"?>\r\n<!DOCTYPE profile SYSTEM \"\/usr\/share\/YaST2\ ...",
    "description": "",
    "id": "2018012943748_SLES_customUnattendInstallPackage.xml",
    "name": "SLES_customUnattendInstallPackage",
```

```
      "os": "sles",
      "osrelease": "",
      "type": "Custom",
      "version": "",
   }],
   "result": "success",
   "messages": [],
}
```


The following example is returned if the request is successful for a base operating system image.


```
{
   "description": "",
   "deployStatus": "ready",
   "id": "win2019|",
   "isCustomizedISO": true,
   "name": "win2019",
   "osBuildId": "",
   "osrelease": "2019",
   "profiles": [{
      "attributes": [],
      "customizationOptions": null,
      "deployStatus": "ready",
      "description": "",
      "id": "win2019|win2019-x86_64-install-Datacenter_customized",
      "isAllowedInCurrentSecurityMode": true,
      "isCustomizedISO": true,
      "name": "win2019-x86_64-install-Datacenter_customized",
      "osBuildId": "",
      "osrelease": "",
      "readyCheck": {
         "isPlaceholder": false,
         "incompatibleWithThinksystem": false,
         "missingThinksystemKiso": false,
         "preloadedWinpe": false,
         "requiresThinksystemKiso": false,
         "noPackages": false,
         "noWinpe": false
      },
      "supportedOsRelease": "",
      "type": "predefined"
   }],
   "readyCheck": {
      "incompatibleWithThinksystem": false,
      "isNotAllowedInCurrentSecurityMode": false
   },
   "size": 4941784,
   "supportedOsRelease": "2019",
   "type": "base"
}
```


The following example is returned if the request is successful.


```
{
   "result": "failed",
   "messages": [{
      "explanation": "",
      "id": "FQXHMFC0003M",
      "recovery": {
          "text": "Restart the management server and attempt the operation again. If
                 the problem persists, contact Support."
         "URL": "",
      },
```

```
      "text": "The imported operating systems could not be retrieved from the image
             repository."
   }]
}
```

POST /osImages

Use this method to create a job that can be used to import an OS image, device driver, boot file, and custom files (such as configuration settings, installation scripts, software, and unattend files), or to customize OS image profile.

This method returns the job ID, which you can then use with the POST /files/osImages?jobId=*{job_id}* method.

To import a new file, follow these steps:

1. Start a job to import the file using POST /osImages.
2. Import the file using POST /files/osImages?jobId=*{job_id}* method, where the job ID is the ID that was returned in step 1.
3. Monitor the status of the import job using GET /tasks/*{job_list}*, where the job ID is the ID that was returned in step 1.

When you import an OS image, Lenovo XClarity Administrator creates one or more OS-image profiles in the OS image repository. The profile includes both the OS image and the installation options for that image.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/osImages`

Query parameters

Parameters	Required / Optional	Description
imageType=*{type}*	Optional	Imports an image of the specified type. This can be one of the following values. • **BOOT**. Boot-options file. This is available for only customized Windows operating-system profiles. • **BUNDLE**. Bundle file (in .zip format). This is available for only customized Windows operating-system profiles. • **BUNDLESIG**. Bundle signature files (in .asc format). This is available for only customized Windows operating-system profiles. • **CONFIG**. Configuration-settings file (in JSON format) • **DUD**. Device driver. This is available for customized Windows and Linux operating-system profiles. • **OS**. (default) OS image • **OSPROFILE**. Customized OS image profile • **SCRIPT**. Installation-script file • **SOFTWARE**. Archive file (in .zip or .tar.gz format) that encapsulates the post-install software payload • **UNATTEND**. Unattend file (in kickstart .cfg, autoyast .xml, or Windows .xml format) **Note:** Unattend files and custom configuration-schema files are specific to a custom OS-image profile and are added and modified using PUT /hostPlatforms.
importByContent=*{type}*	Optional	When imageType is UNATTEND or CONFIG , indicates the type of import method to use. This can be one of the following values. • **true**. Import using this POST method to by specifying the file metadata and contents in the request body. A job will not be generated. • **false**. (default) Import using this POST method to create a job, and then using the POST /files/osImages?jobId=*{job_id}* method to import the file.

The following example starts a job to import an operating-system image.

```
POST https://192.0.2.0/osImages
```

The following example starts a job to import a device driver.

```
POST https://192.0.2.0/osImages?imageType=DUD
```

The following example starts a job to import a boot file.

```
POST https://192.0.2.0/osImages/?imageType=BOOT
```

The following example starts a job to import a customized OS image profile.

```
POST https://192.0.2.0/osImages?imageType=OSPROFILE
```

The following example starts a job to import a custom configuration-settings file without using a job and using this POST method to by specifying the file metadata and contents in the request body.

```
POST https://ajsga200.labs.lenovo.com/osImages?imageType=CUSTOM_CONFIG&importByContent=true
```

Request body

Table 51. Import by creating a job

Attributes	Required / Optional	Type	Description
Action	Required	String	This value must be `init`.
fileSize	Optional	String	Size of the file to be imported (in bytes)

This following example creates a job that can be used to import a file using the POST /files/osImages?jobId=*{job_id}*.

```
{
   "Action": "Init",
   "fileSize": "338763776"
}
```

Table 52. Import by specifying metadata and content

Attributes	Required / Optional	Type	Description
associatedFileId	Optional	String	If imageType=CONFIG, this is the ID of the associated unattend file If imageType=UNATTEND, this is the ID of the associated configuration-settings file.
content	Required	String	Contents of the file to be imported This cannot be null or an empty string.
description	Optional	String	Description of the file
deviceType	Optional	String	Type of device that is associated with the uploaded file. This can be one of the following values. • **hba** • **nic** • **storage** • **other**
fileSize	Optional	String	Size of the file to be imported (in bytes)
name	Optional	String	Name of the file
os	Required	String	Operating system that is associated with the uploaded file. This can be one of the following values. • **esxi** • **rhels** • **sles** • **win** **Note:** This attribute is ignore when imageType=CONFIG.
osrelease	Required if imageType is UNATTEND	String	Operating-system release that is associated with the uploaded file **Note:** This attribute is ignore when imageType=CONFIG.

This following example imports a file without using a job.

```
{
"content": [{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
```

```
    "common": false,
    "name": "server-settings",
    "optional": false,
    "template": [{
        "autoCreateInstance": true,
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
        "category": "dynamic",
        "common": true,
        "description": "A NTP Server",
        "label": "NTP Server",
        "name": "ntpserver",
        "optional": true,
        "regex": "[\\w\\.]{1,64}$",
        "type": "string"
    }],
    "type": "array"
},
{
    "category": "static",
    "common": true,
```

```
        "description": "Directory for post-installation script logging.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
},
"description": "My file description."
"devicetype": "other"
"name": "myconfigfile.json"
"os": "win"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
jobId	String	ID for the job. This ID can be used by the POST /files/osImages?jobId=*{job_id}* method to import an image into the OS image repository. **Note:** This attribute is returned only when a job is created.
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages If the result is successful, an empty array is returned.
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
    "jobId": "1",
    "result": "success",
    "messages": []
}
```

The following example is returned if the request is not successful.

```
{
    "result": "failed",
    "messages": [{
        "explanation": "The management server supports a maximum of 5 imported operating system
                        images.",
        "id": "FQXHMFC0057M",
        "recovery": {
            "URL": "",
            "text": "Delete an operating system image and attempt to import the image again."
        }
        "text": "The maximum number of imported operating systems has been reached.",
    }]
}
```

/osImages/*{file_name}*

Use this REST API to export a customized OS image profile to a remote file server or local system.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET

GET /osImages/*{file_name}*

Use this method to export a customized OS image profile to a remote file server or local system.

You must first create a tar.gz file that contains the customized OS image profile using the GET /osImages/*{id}* method.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/osImages/{file_name}`

where *{file_name}* is the name of the tar.gz file that contains the customized OS image profile. The file name was returned when the GET /osImages/*{id}* method completed successfully.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/osImages/*{id}*

Use this REST API to remove one or more OS images, OS-image profiles, device driver, boot files, and custom files (such as configuration settings, installation scripts, software, and unattend files) from the Lenovo XClarity Administrator OS images repository, create a customized OS-image profile from a base operating system and add custom files, modify, or create a downloadable tar.gz file that contains a customized OS-image profile, or modify an existing device driver or boot file.

HTTP methods

GET, PUT, POST, DELETE

GET /osImages/*{id}*

Use this method to create a downloadable tar.gz file that contains a customized OS-image profile.

The tar.gz file that contains the following files:
- Custom device drivers
- Custom boot files
- Metadata that describes the installation options including predefined unattend files
- Custom files (such as configuration-settings, installation scripts, software, and unattend files)
- Checksum for the tar.gz file

You can use the GET /osImages/*{file_name}* method to download the tar.gz file that is created by this method.

This method starts a job that runs in the background to perform the operation. The job ID is returned using the **jobID** attribute in the response body. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Attention: A successful response indicates that the request was successfully transmitted and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/osImages/{id}`

where *{id}* is the ID of the customized OS image profile. To obtain the ID, use the GET /osImages method.

Query parameters

Parameters	Required / Optional	Description
path=*{path}*	Optional	Full path on the remote file server where the operating-system image is to be downloaded **Note:** This attribute is only applicable when **serverId** is specified.
serverId=*{id}*	Optional	Profile ID for the remote file server. To obtain the profile ID, use the GET /osImages/remoteFileServers/*{id}* method **Note:** When this query parameter is specified, the customized OS-image profile is exported to a remote file server. If it is not specified, it is exported to the local system.

The following example exports a customized Windows Server 2016 profile to a remote image server.

```
GET https://192.0.2.0 /osImages/win2016|win2016-x86_64-install-Standard_core?serverId=101
&path=%2F/some%2F/path%2F/to%2F/file
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
filename	String	Name of the tar.gz file that is generated by the export process. You can download this file from the management server after the job completes successfully.
jobID	String	Job identifier
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of strings	Detailed information about errors that occurred during the exporting process

The following example is returned if the request is successful.

```
{
   "filename "2016121921921_Custom-2016-datacenter-profile.tar.gz",
   "jobID": "12",
   "result": "success"
   "messages": []
}
```

PUT /osImages/*{id}*

Use this method to modify a customized OS image profile, or to add or remove device drivers, boot files, and custom files (such as configuration settings, installation scripts, software, and unattend files) from the customized OS image profile.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/osImages/{id}`

where *{id}* is the base OS-image ID, customized OS-image profile ID, device driver ID, or boot file ID respectively. To obtain the ID, use the GET /osImages method.

Query parameters

Parameters	Required / Optional	Description
imageType=*{type}*	Optional	Type of custom file to be modified. This can be one of the following values. • **CONFIG**. Configuration-settings file (in JSON format) • **SCRIPT**. Installation-script file. • **SOFTWARE**. Archive file (in .zip or .tar.gz format) that encapsulates the post-install software payload. • **UNATTEND**. Unattend file (in kickstart ,cfg, autoyast .xml, or Windows .xml format). **Note:** The *{id}* that is specified in the URL must correlate to an existing file that matches the value that is specified in this attribute.

The following example modifies an OS-image profile.

```
PUT https://192.0.2.0/osImages/win2016|win2016-x86_64-install-Standard_core?serverId=101
&path=%2F/some%2F/path%2F/to%2F/file
```

The following example modifies an unattend file.

```
PUT https://192.0.2.0/osImages/win2016|win2016-x86_64-install-Standard_core?serverId=101
&path=%2F/some%2F/path%2F/to%2F/file?imageType=UNATTEND
```

Request body

Table 53. Modify a custom file

Attributes	Required / Optional	Type	Description
associatedFileId	Optional	String	ID of the unattend file that was optionally associated with this configuration-settings file
customConfigFile	Required if **imageType** is CONFIG	Object	Configuration-settings files to be modified **Note:** Configuration settings are supported only for specific OS versions. To determine whether the OS supports configuration settings, use the **customConfigReleases** attribute in GET /osImages.
description	Optional	String	Description of the configuration-settings file
content	Optional	String	Contents of the configuration-settings file
version	Optional	String	Version of the configuration-settings file
customSoftware	Required if **imageType** is SOFTWARE	Object	Software files to be modified
description	Optional	String	Description of the software payload
version	Optional	String	Version of the software payload
installScriptFile	Required if **imageType** is SCRIPT	Object	Installation script files to be modified
description	Optional	String	Description of the installation-script
unattendFile	Required if **imageType** is UNATTEND	Object	Unattend files to be modified **Note:** Unattend files are supported only for specific OS versions. To determine whether the OS supports unattend files , use the **customUnattendReleases** attribute in GET /osImages.
content	Optional	String	Contents of the unattend file
description	Optional	String	Description of the unattend file
version	Optional	String	Version of the unattend file

The following example associating a custom config file with a custom unattend file.

```
{
   "associatedFileId":"20190424120112_SLES_InstallPackages_customUnattend.xml"
}
```

Table 54. Create or modify a customized OS image profile

Attributes	Required / Optional	Type	Description
profile	Required if a customized OS-image profile ID is specified in the URL.	Object	Information about a customized OS image profile **Note:** Preloaded OS image profiles cannot be modified.
customizationOptions	Optional	Object	Information about all options that can be customized in this operating system If the base operating system for the profile does not support customization, this attribute is null. If the base operating system for the profile supports customization but does support certain child attributes, the unsupported child attributes are returned as empty strings.
bootOptions	Optional	Object	Information about customizable boot options.
bootFileIds	Optional	Array of strings	Boot file IDs that correlate to boot file in the customized OS image profile • If a specified ID is not currently in the customized OS image profile, the boot file is added to the profile. • If an ID is currently in the customized OS image profile but is not specified, the boot file is removed from the profile. **Note:** Boot files must be imported in the OS-image repository before they can be added to a customized OS image profile. Use POST /osImages to import the boot file, and then use POST /files/osImages?jobId=*{job_id}* to import the boot file into the OS images repository.
customConfigOptions	Optional	Object	Information about the custom configuration settings that are associated with this customized OS-image profile
customConfigFileIds	Optional	Array of strings	IDs of the configuration-settings files that are associated with this customized OS-image profile
customSoftwareOptions	Optional	Object	Information about custom software payloads that are associated with this customized OS image profile
customSoftwareIds	Optional	Array of strings	List of IDs for each software payload that is associated with this customized OS image profile
deployDataAndSoftwareLocation	Optional	String	Path to the extracted software payload, custom files, and deployment data (such as certificates and logs) on the deployment host. The following directories are used by default. • **Linux**: `/home/lxca` • **Windows**: `c:\lxca`

Table 54. Create or modify a customized OS image profile (continued)

Attributes	Required / Optional	Type	Description
driverOptions	Optional	Object	Information about predefined and imported device drivers that are associated with this customized OS image profile
driverFileIds	Optional	Array of strings	Device-driver IDs that correlate to all device-drivers in the customized OS image profile • If a specified ID is not currently in the customized OS image profile, the device driver is added to the profile. • If an ID is currently in the customized OS image profile but is not specified, the device-driver is removed from the profile. **Note:** Device drivers must be imported in the OS-image repository before they can be added to a customized OS image profile. Use POST /osImages to import the device driver, and then use POST /files/osImages?jobId=*{job_id}* to import the device driver into the OS images repository.
scriptFileIds	Optional	Array of strings	List of IDs for each installation-script file that is associated with this customized OS image profile • If a specified ID is not currently in the customized OS image profile, the installation-script file is added to the profile. • If an ID is currently in the customized OS image profile but is not specified, the installation-script file is removed from the profile. **Note:** Installation-script files must be imported in the OS-image repository before they can be added to a customized OS image profile. Use POST /osImages to import installation-script files, and then use POST /files/osImages?jobId=*{job_id}* to import installation-script files into the OS images repository.
unattendOptions	Optional	Object	Information about predefined unattended-file options
unattendFileIds	Optional	Array of strings	List of IDs for each unattend file that is associated with this customized OS image profile
description	Optional	String	Description for the customized OS image profile

Table 54. Create or modify a customized OS image profile (continued)

Attributes		Required / Optional	Type	Description
	name	Optional	String	Name of the customized OS image profile
	type	Optional	String	Type of OS profile. This can be one of the following values. • **custom**. The profile was created when a boot file or device driver was manually uploaded and added to an operating system. • **predefined**. The profile was preloaded by Lenovo

The following example creates a new customized OS image profile for Windows 2016 and adds custom files to the profile.

```
{
   "profile": {
      "customizationOptions": {
         "bootOptions": {
            "bootFileIds": ["winpe-64-base"]
         },
         "customConfigOptions" : {
            "customConfigFileIds" : []
         },
         "customSoftwareOptions" : {
            "customSoftwareIds" : []
         }
         "driverOptions": {
            "driverFileIds": [
               "nic-broadcom-bnxtnd-win2016-v1",
               "storage-broadcom-megasas35-win2016-v1",
               "hba-broadcom-itsas35-win2016-v1",
               "hba-elxcna-windows2016-v1"
            ]
         }
         "installScriptOptions": {
            "scriptFileIds": []
         },
         "unattendOptions": {
            "unattendFileId": []
         },
         "unattendOptions": {
            "unattendFileIds": []
         },
      },
      "name": "Win2016-Custom-Datacenter-2",
      "description": "My custom profile - Rename",
      "type": "custom"
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages":[]
}
```

The following example is returned if the request is not successful.

```
{
    "result": "failed",
    "messages": [{
        "explanation": "The request resource cannot be found.",
        "id": "FQXHMFC0XXXM ",
        "text": "Modify your request data. If the problem persists, contact Support.",
        "recovery": {
            "URL": "",
            "text": "Unable to modify the specified resource ID. The ID is not found."
        }
    }]
}
```

POST /osImages/*{id}*

Use this method to create a customized OS-image profile from a base operating system and add custom files (such as configuration settings, installation scripts, software, and unattend files).

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/osImages/{id}`

where *{id}* is the ID of the predefined OS-image profile that you want to customize. To obtain the ID, use the value in the **items.profiles. id** response attribute that is returned by the GET /osImages method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
profile	Required	Object	Information about one or more customized OS image profiles Preloaded OS image profiles cannot be imported.
customizationOptions	Required	Object	Information about all options that can be customized in this operating system If the base operating system for the profile does not support customization, this attribute is null. If the base operating system for the profile supports customization but does support certain child attributes, the unsupported chile attributes are returned as an empty strings.
bootOptions	Optional	Object	Information about customizable boot options
bootFileIds	Optional	Array of strings	Boot file IDs that correlate to the imported boot files Use POST /osImages to import the boot file, and then use POST /files/osImages?jobId=*{job_id}* to import the boot file into the OS images repository.
customConfigOptions	Optional	Object	Information about the custom profile-configuration settings
customConfigFileIds	Optional	Array of objects	IDs of the configuration-settings files
customSoftwareOptions	Optional	Object	Information about custom software payloads that are associated with this customized OS image profile
customSoftwareIds	Optional	Array of strings	List of IDs for each software payload

Attributes	Required / Optional	Type	Description
customType	Required	Integer	Customization type. This can be one of the following values. • **1**. Custom unattend file and associated custom config file. • **2**. Custom unattend file only. • **3**. Custom unattend file and custom config file. • **4**. Custom config file only. • **5**. No custom unattend or config file.
deployDataAndSoftwareLocation	Optional	String	Path to the extracted software payload, custom files, and deployment data (such as certificates and logs) on the deployment host The following directories are used by default. • **Linux**: `/home/lxca` • **Windows**: `c:\lxca`
driverOptions	Optional	Object	Information about predefined and imported device drivers that are associated with this customized OS image profile
driverFileIds	Optional	Array of strings	Device driver IDs that correlate to imported device-drivers Use POST /osImages to import the device driver, and then use POST /files/osImages?jobId=*{job_id}* to import the device driver into the OS images repository.
installScriptOptions	Optional	Object	Information about install script files associated with this customized OS image profile
scriptFileIds	Optional	Array of strings	List of IDs for each installation script • If a specified ID is not currently in the customized OS image profile, the installation-script file is added to the profile. • If an ID is currently in the customized OS image profile but is not specified, the installation-script file is removed from the profile. **Note:** Installation-script files must be imported in the OS-image repository before they can be added to a customized OS image profile. Use POST /osImages to import installation-script files, and then use POST /files/osImages?jobId=*{job_id}* to import installation-script files into the OS images repository.
unattendOptions	Optional	Object	Information about predefined unattended-file options
unattendFileIds	Optional	Array of strings	List of IDs for each unattend-file that correlate to imported unattend files
description	Optional	String	Description for the customized OS image profile
name	Required	String	Name of the customized OS image profile
type	Optional	String	Type of OS profile. This can be the following value. • **custom**. (default) The profile was created when a custom file (such as a boot file or device driver) was manually uploaded and added to an operating system.

The following example creates a customized OS-image profile.

```
{
   "profile": {
      "customizationOptions": {
```

```
        "bootOptions": {
           "bootFileIds": ["winpe-64-base"]
        },
        "customConfigOptions " : {
           "customConfigFileIds" : []
        },
        "customSoftwareOptions " : {
           "customSoftwareIds" : []
        },
        "customType": 5,
        "driverOptions": {
           "driverFileIds": [
              "nic-broadcom-bnxtnd-win2016-v1",
              "storage-broadcom-megasas35-win2016-v1",
              "hba-broadcom-itsas35-win2016-v1",
              "hba-elxcna-windows2016-v1"
           ]
        },
        "installScriptOptions": {
           "scriptFileIds": []
        },
        "unattendOptions": {
           "unattendFileId": []
        }
     },
     "description": "My custom profile",
     "name": "Win2016-Custom-Datacenter-2",
     "type": "custom"
  }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message

Attributes	Type	Description
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": []
}
```

DELETE /osImages/*{images_list}*

Use this method to remove one or more OS images, OS image-profiles, and custom files (such as device drivers, boot files, configuration settings, installation scripts, software, and unattend files) from the Lenovo XClarity Administrator OS images repository.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/osImages/{images_list}`

where <*images_list}* is a list of one or more IDs, separated by a comma, for OS images, OS image profile, and custom files such as device drivers, boot files, configuration settings, installation scripts, software, and unattend files (for example, `hba-elxcna-windows2016-v1,hba-elxfc-windows2016-v1`). To obtain the ID, use the GET /osImages method.

Notes:

- If you specify an operating-system image, the operating system image and all associated profiles are deleted. If you specify an OS profile, only the profile is deleted; all other profiles for the operating system remain.
- Specify either a full OS image ID *or* one or more OS image profile IDs for that OS image. Specifying both the full OS image ID *and* OS image profile IDs for that OS image in the same URI might result in errors.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
204	No Content	The request completed successfully, but no response content is returned.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
412	Precondition failed	Specified data is invalid because of missing values. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/osImages/customSettings

Use this REST API to validate a custom configuration-settings file (in JSON format).

HTTP methods

POST

POST /osImages/customSettings

Use this method to validate the JSON scheme in a custom configuration settings file. If valid, this method returns a list of custom macros that are derived from the file. If not valid, this method returns a detailed error report that includes the locations in the file that failed validation.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/osImages/customSettings`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
customConfigValues	Required	Object	JSON-formatted string that represents the custom configuration settings If valid, a list of custom macros that are derived from the custom configuration settings are returned in the **customMacros** response attribute. If not valid, a list of errors and locations in the schema are returned in the **errorReport** response attribute.

The following example represents the custom configuration settings to be validated.

```
[{
```

```
   "customConfigValues": {
      "category": "dynamic",
      "content": [{
         "category": "dynamic",
         "common": false,
         "name": "server-settings",
         "optional": false,
         "template": [{
            "category": "dynamic",
            "common": false,
            "content": [{
               "category": "dynamic",
               "choices": ["en_US","ja_JP","pt_BR"],
               "common": false,
               "description": "This parameter defines the OS language locale to use with this
                               deployment. (English, Brazilian Portuguese, Japanese) are
                               supported.",
               "label": "OS Locale",
               "name": "locale",
               "optional": false,
               "type": "string",
               "value": "en_US"
            },
            {
               "category": "dynamic",
               "choices": ["english-us","japanese","portugese-br"],
               "common": false,
               "description": "This parameter defines the keyboard locale to use with this
                              deployment. (English, Brazilian Portuguese, Japanese) are
                              supported.",
               "label": "Keyboard Locale",
               "name": "keyboardLocale",
               "optional": false,
               "type": "string",
               "value": "english-us"
            }],
            "name": "node",
            "optional": false,
            "type": "assoc_array"
         }],
         "type": "assoc_array"
      }],
      "description": "Custom configuration file for deployment of custom locale to OS.",
      "label": "My Custom Deployment",
      "name": "myCustomDeploy",
      "optional": false,
      "type": "array"
   }
}]
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
customMacros	Array of objects	List of custom macros that are defined for the custom configuration settings
macroName	String	Name of a custom macro that is derived from the specified JSON schema
errorReport	Array of objects	List of schema errors that were found during the validation
location	String	Location of error in the JSON schema
message	String	Detailed message about the schema error
messages	Array of objects	Information about one or more messages If the result is successful, an empty array is returned.
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful with no validation errors.

```
{
   "result": "success",
   "customMacros": [{
      "macroName": ""
   }],
   "messages":[]
}
```

The following example is returned if the request is successful with validation errors.

```
{
   "result": "success",
```

```
   "errorReport": [{
      "location": "",
      "message": ""
   }],
   "messages":[]
}
```

The following example is returned if the request is not successful.

```
{
   "result": "failed",
   "messages": [{
      "explanation": "",
      "id": "FQXHMFC0004M",
      "text": "An internal error occurred.",
      "recovery": {
         "text": "Attempt to perform the operation again. If the problem persists, contact
                 Support.",
         "URL": ""
      }
   }]
}
```

/osImages/remoteFileServers

Use this REST API to retrieve information about all remote file-server profiles or to create or modify a remote file-server profile.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, POST

GET /osImages/remoteFileServers

Use this method retrieve information about all remote file-server profiles.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/osImages/remoteFileServers`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
serverList		Information about each remote file-server profile
address		IP address of the remote file server
keyType		Type of encryption algorithm. This can be one of the following values. • **RSA-2048** • **RSA-4096** • **ECDSA-521-secp521r1**
port		Port number
protocol		Server protocol. This can be one of the following values. • **HTTP** • **HTTPS** • **FTP** • **SFTP**
serverId		Profile ID for the remote file server.
serverPublicKey		XClarity Administrator generated public key.
username		User name to connect to the remote file server.
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "serverList": [{
      "address": "192.168.1.10",
      "keyType": "RSA-2048",
```

```
      "port": 8080,
      "protocol": "SFTP",
      "serverId": "100",
      "serverPublicKey": "KLAJDSLFAKEUIJ387U28379…"
   },
   {
      "address": "192.168.1.20,
      "port" : 80,
      "protocol" : "FTP",
      "serverId" : "101",
      "username" : "admin"
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Informationonly;noactionisrequired.",
         "URL": ""
      },
      "text": "Therequestcompletedsuccessfully."
   }]
}
```


POST /osImages/remoteFileServers

Use this method to create a remote file-server profile.

The public key is returned in the response body. The generated private key is stored in Lenovo XClarity Administrator.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/osImages/remoteFileServers
```

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
address	Required	String	IP address of the remote file server
displayName	Required	String	User-defined name of the remote file server
keyComment	Optional	String	Key comment
keyPassphras	Optional	String	Key passphrase

Attributes	Re-quired / Optional	Type	Description
keyType	Optional	String	Type of encryption algorithm. This can be one of the following values. • **RSA-2048** • **RSA-4096** • **ECDSA-521-secp521r1**
password	Optional	String	Password to connect to the remote file server
port	Required	Integer	Port number
protocol	Required	String	Server protocol. This can be one of the following values. • **HTTP** • **HTTPS** • **FTP** • **SFTP**
serverId	Optional	String	Profile ID for the remote file server If specified, the profile is modified. If not specified, a new profile is created.
username	Optional	String	User name to connect to the remote file server

The following example creates a new remote file-server profile using a security key.

```
{
   "address" : "192.168.1.10",
   "keyPassphrase": "PasswOrd",
   "keyType" : "RSA-2048",
   "port" : 8080,
   "protocol" : "HTTPS"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
address	String	IP address of the remote file server
keySignature	String	SFTP server key signature
port	integer	Port number

Attributes	Type	Description
protocol	String	Server protocol. This can be one of the following values. • **HTTP** • **HTTPS** • **FTP** • **SFTP**
serverId	String	Profile ID for the remote file server
serverPublicKey	String	XClarity Administrator generated public key
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Object	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "address" : "192.168.1.10",
   "keySignature" : "WJILKEKJLKJLKSJ092039230948…",
   "port" : 8080,
   "protocol" : "SFTP",
   "serverId" : "100",
   "serverPublicKey" : "KADKJADSKF94JK9O$#@@5983739AD…",
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```

/osImages/remoteFileServers/*{id}*

Use this REST API to retrieve information about or to delete a specific remote file-server profile.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, DELETE

GET /osImages/remoteFileServers/*{id}*

Use this method retrieve information about a specific remote file-server profile.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/osImages/remoteFileServers/{id}`

where *{id}* is the ID of an remote file-server profile. To obtain the ID, use the GET /osImages/remoteFileServers method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
address	String	IP address of the remote file server
keyType	String	Type of encryption algorithm. This can be one of the following values. • **RSA-2048** • **RSA-4096** • **ECDSA-521-secp521r1**
port	Integer	Port number
protocol	String	Server protocol. This can be one of the following values. • **HTTP** • **HTTPS** • **FTP** • **SFTP**
serverId	String	Profile ID for the remote file server

Attributes	Type	Description
serverPublicKey	String	XClarity Administrator generated public key
username	String	User name to connect to the remote file server.
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "address": "192.168.1.10",
   "keyType": "RSA-2048",
   "port": 8080,
   "protocol": "SFTP",
   "serverId": "100",
   "serverPublicKey": "KLAJDSLFAKEUIJ387U28379…"
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Informationonly;noactionisrequired.",
         "URL": ""
      },
      "text": "Therequestcompletedsuccessfully."
   }]
}
```

DELETE /osImages/remoteFileServers/*{id}*

Use this method delete a specific remote file-server profile.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
DELETE https://{management_server_IP}/osImages/remoteFileServers/{id}
```

where *{id}* is the ID of an remote file-server profile. To obtain the ID, use the GET /osImages/remoteFileServers method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
204	No Content	The request completed successfully, but no response content is returned.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Informationonly;noactionisrequired.",
         "URL": ""
      },
      "text": "Therequestcompletedsuccessfully."
```

```
    }]
}
```

PUT /osImages/remoteFileServers/*{id}*

Use this method to modify a remote file-server profile.

The public key is returned in the response body. The generated private key is stored in Lenovo XClarity Administrator.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/osImages/remoteFileServers/{id}`

where *{id}* is the ID of the remote file-server profile to be modified. To obtain the ID, use the GET /osImages/remoteFileServers method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
address	Required	String	IP address of the remote file server
displayName	Required	String	User-defined name of the remote file server
keyComment	Optional	String	Key comment
keyPassphras	Optional	String	Key passphrase
keyType	Optional	String	Type of encryption algorithm. This can be one of the following values. • **RSA-2048** • **RSA-4096** • **ECDSA-521-secp521r1**
password	Optional	String	Password to connect to the remote file server
port	Required	Integer	Port number
protocol	Required	String	Server protocol. This can be one of the following values. • **HTTP** • **HTTPS** • **FTP** • **SFTP**
serverId	Optional	String	Profile ID for the remote file server If specified, the profile is modified. If not specified, a new profile is created.
username	Optional	String	User name to connect to the remote file server

The following example modifies a remote file-server profile using a user name and password.

```
{
   "address" : "192.168.1.10",
   "password" : "Passw0rd",
   "port" : 8081,
   "protocol" : "HTTPS",
   "username" : "admin"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
address	String	IP address of the remote file server
keySignature	String	SFTP server key signature
port	Integer	Port number
protocol	String	Server protocol. This can be one of the following values. • **HTTP** • **HTTPS** • **FTP** • **SFTP**
serverId	String	Profile ID for the remote file server
serverPublicKey	String	XClarity Administrator generated public key
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Object	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "address" : "192.168.1.10",
   "keySignature" : "WJILKEKJLKJLKSJ092039230948…",
   "port" : 8080,
   "protocol" : "SFTP",
   "serverId" : "100",
   "serverPublicKey" : "KADKJADSKF94JK90$#@@5983739AD…",
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```

Chapter 9. Firmware update

The following resources are available for performing firmware updates functions.

/compliancePolicies

Use this REST API to retrieve basic or detailed information for a specified compliance policy or all policies. You can also use this REST API to create, copy, delete, modify, import or export a firmware-update compliance policy or delete a list of compliance policies.

HTTP methods

GET, PUT, POST, DELETE

GET /compliancePolicies

Use this method to export a firmware-update compliance policy or retrieve basic or detailed information for a specified compliance policy or all policies. The basic information includes the name, last modified, and description. The detailed information includes the target versions and information about the firmware-update packages.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/compliancePolicies`

Query parameters

Parameters	Required / Optional	Description
basic_full=*{type}*	Optional	Returns the specified type of information. This can be one of the following values. • **basic**. Returns basic information for the compliance policy. • **full**. Returns detailed information for the compliance policy.
exportDownload=*{file_name}*	Optional	Downloads the specified compliance policy as a .zip file to your local system
policyname_all=*{policy_name}*	Optional	Returns information about the specified compliance policy. If the value is empty, information is returned for all compliance policies.
refresh=*{Boolean}*	Optional	Indicates whether to refresh the compliance-policy data before returning the results. This can be one of the following values. • **true**. Refreshes the compliance-policy data. • **false**. (default) Does not refresh the compliance policy data.

The following example refreshes the compliance-policy data and then returns basic information about all compliance policies.

```
GET https://{management_server_IP}/compliancePolicies?basic_full=basic
&policyname_all=&refresh=false
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Table 55. Basic information for compliance policies

Attributes	Type	Description
policies	Array	Information about the compliance policy
description	String	Compliance policy description
id	String	Compliance policy ID
inUse	Boolean	Identifies whether the compliance policy is in use. This can be one of the following values. • **true**. The compliance policy is in use. • **false**. The compliance policy is not in use.
filterType	String	Filter type. This can be one of the following values. • **all**. All supported machine types • **managed**. Only managed machine types.
lastAction	String	Last action that was performed on the compliance policy. This can be one of the following values. • **Predefined**. The compliance policy is predefined. • **Created by** *{user_name}*. The user-defined compliance policy was created by the specified user. • **Edited by** *<user_name}*. The user-defined compliance policy was edited by the specified user.
lastEdited	String	Timestamp of the last change to the compliance policy
lastModified	String	Timestamp of the last change to the compliance policy
name	String	Compliance policy name
updateRule	String	Internal use only
userDefined	String	Identifies whether the compliance policy is user-defined. This can be one of the following values. • **yes**. The compliance policy is user-defined. • **no**. The compliance policy is predefined.

This example response is returned if the request is successful when the **basic_full=basic** query parameter is specified and the **policyname_all** query parameter is not specified.

```
{
   "policies":[{
```

```
      "id": "1612876820379",
      "description": "",
      "filterType": "managed",
      "inUse": "true",
      "lastAction": "Created by USER1",
      "lastEdited": "2021-02-09T13:20:20Z",
      "lastModified": "This policy was created by USER1 on 2021-02-09T13:20:20Z",
      "name": "7162-imm2-dsa",
      "updateRule": "",
      "userDefined": "yes"
   }]
}
```

Table 56. Detailed information for compliance policies

Attributes	Type	Description
policies	Array	Information about the compliance policy
id	String	Compliance policy ID
description	String	Compliance policy description
details	Array	Details about each compliance policy
id	String	System type used to identify the CMM. Internal use only
baseVersion	String	For CMMs or switches, this is the fix ID of the package. For servers, the following is returned. `xxxx_utl_uxsp_xxxxxx-1.00_xxxx_32-64`
build	String	Firmware update build number
components	Array	Information about each component in the firmware update package
build	String	Component firmware update build number.
isDefault	String	Indicates whether the component update is the default component (the latest component update). If so, **yes** is returned.
isGA	String	Indicates whether the component update is the GA level version of the update. This can be one of the following values. • **yes**. Component update is the GA level
name	String	Component name
packageExistence	String	Indicates whether the update exists in the firmware-updates repository. This can be one of the following values. • **yes**. Update package exists. • **no**. Update package does not exist.
releaseDate	String	Release date of the component update
rule	String	Rule for raising a non-compliant alert. This can be one of the following values. • **alertIfNotExactMatch**. Show non-compliance when the installed version on device does not exactly match the compliance target. • **alertIfDownlevel**. Show non-compliance when the installed version on device is earlier than the compliance target. • **noAlerting**. Never show non-compliance.
targetVersion	String	Firmware level that is considered to be the baseline for the specified system type

Table 56. Detailed information for compliance policies (continued)

Attributes	Type	Description
type	String	For CMMs or switches, this attribute is empty. For servers, specifies the type of package. This can be one of the following values. • **IMM** • **IMM-Backup** • **UEFI** • **UEFI-Backup**
version	String	Component firmware update version
isDefault	String	Indicates whether the update package is the default package (the latest package). This can be one of the following values. • **yes**. This is the default update package • **no**. This is not the default update package
isDoNotUpdate	String	Indicates whether to not update the firmware for this component. This can be one of the following values. • **Yes**. Do not update firmware on this component. • **No**. Update firmware on this component.
isGA	String	Indicates whether the package is the GA level version of the update
isUXSP	String	Indicates whether this update package is an UpdateXpress System Pack (UXSP). This can be one of the following values. • **yes**. This is a UXSP. • **no**. This is not a UXSP.
name	String	Compliance policy name
packageExistence	String	Indicates whether the update package exists in the firmware-updates repository. This can be one of the following values. • **yes**. Update package exists. • **no**. Update package does not exist.
releaseDate	String	For CMMs or switches, the release date of the update package. If so, **yes** is returned. For servers, this attribute is empty.
rule	String	Rule for raising a non-compliant alert. This can be one of the following values. • **alertIfNotExactMatch**. Show non-compliance when the installed version on device does not exactly match the compliance target. • **alertIfDownlevel**. Show non-compliance when the installed version on device is earlier than the compliance target. • **noAlerting**. Never show non-compliance. • **custom**. Follow the detailed rules of each firmware component.
systemType	String	Type of device for which the policy applies
version	String	Firmware update version
filterType	String	Filter type. This can be one of the following values. • **all**. All supported machine types • **managed**. Only managed machine types.
inUse	Boolean	Identifies whether the compliance policy is in use. This can be one of the following values. • **true**. The compliance policy is in use. • **false**. The compliance policy is not in use.

Table 56. Detailed information for compliance policies (continued)

Attributes	Type	Description
lastAction	String	Last action that was performed on the compliance policy. This can be one of the following values. • **Predefined**. The compliance policy is predefined. • **Created by** *{user_name}*. The user-defined compliance policy was created by the specified user. • **Edited by** *{user_name}*. The user-defined compliance policy was edited by the specified user.
lastEdited	String	Timestamp of the last change to the compliance policy
lastModified	String	Timestamp of the last change to the compliance policy
name	String	Compliance policy name
updateRule	String	Internal use only
userDefined	String	Identifies whether the compliance policy is user-defined. This can be one of the following values. • **yes**. The compliance policy is user-defined. • **no**. The compliance policy is predefined.

This example response is returned if the request is successful when the **basic_full=full** query parameter is not specified and the **policyname_all** query parameter is specified.


```
{
   "policies": [{
      "id": "1612876820379",
      "description": "",
      "details": [{
         "id": "7162",
         "baseVersion": "xxxx_utl_uxsp_xxxxxx-1.00_xxxx_32-64",
         "build": "",
         "components": [{
            "build": "",
            "isDefault": "yes",
            "isGA": "no",
            "name": "Integrated Management Module 2 (IMM2) Update (Backup)",
            "packageExistence": "yes",
            "releaseDate": "",
            "rule": "alertIfDownlevel",
            "targetVersion": "DoNotUpdate_SERVER_IMM2-BACKUP",
            "type": "IMM-Backup",
            "version": ""
         },
         {
            "build": "TCOO75J",
            "isDefault": "yes",
            "isGA": "no",
            "name": "Integrated Management Module 2 (IMM2) Update",
            "packageExistence": "yes",
            "releaseDate": "2020-12-30",
            "rule": "alertIfDownlevel",
            "size": 90447000,
            "targetVersion": "lnvgy_fw_imm2_tcoo75j-9.00_anyos_noarch",
            "type": "IMM",
            "version": "9.00"
         },
         {
            "build": "DSALB5S",
```

```
            "isDefault": "yes",
            "isGA": "no",
            "name": "Lenovo Dynamic System Analysis (DSA) - Preboot Embedded (For AnyOS)",
            "packageExistence": "yes",
            "releaseDate": "2020-10-13",
            "rule": "alertIfDownlevel",
            "size": 241505000,
            "targetVersion": "lnvgy_fw_dsa_dsalb5s-10.8_anyos_32-64",
            "type": "Diagnostics",
            "version": "10.8"
         }],
         "isDefault": "yes",
         "isDoNotUpdate": "no",
         "isGA": "yes",
         "isUXSP": "yes",
         "packageExistence": "yes"
         "name": "Lenovo Flex System x240 Compute Node-7162",
         "releaseDate": "",
         "rule": "alertIfDownlevel",
         "systemType": "7162",
         "version": "",
      }],
      "filterType": "managed",
      "inUse": "true",
      "lastAction": "Created by JBRUNDIDGE",
      "lastModified": "This policy was created by JBRUNDIDGE on 2021-02-09T13:20:20Z",
      "lastEdited": "2021-02-09T13:20:20Z",
      "name": "7162-imm2-dsa",
      "updateRule": "",
      "userDefined": "yes"
   }]
}
```


PUT /compliancePolicies

Use this method to modify or export a firmware-update compliance policy.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/compliancePolicies`

Query parameters

Parameters	Required / Optional	Description
action=*{action}*	Required	Action type. This can be one of the following values. • **edit**. Modifies the specified compliance policy. • **export**. Compresses the specified compliance policy .xml file into a .zip file, and downloads the .zip file to the local system. Use the GET /tasks/*{job_list}* (where *{job_id}* is the job ID) to retrieve the overall job status. If a job was not successfully started, refer to the response code and response body for details. **Note:** A compliance policy that includes packages might take a longer time to import. • **exportWithPackages**. Compresses the specified compliance policy .xml file and the update files used by the policy into a .zip file and downloads the .zip file to the local system. Use the GET /tasks/*{job_list}* (where *{job_id}* is the job ID) to retrieve the overall job status. If a job was not successfully started, refer to the response code and response body for details.

The following example modifies a compliance policy.

```
PUT https://192.0.2.0/compliancePolicies?type=edit
```

Request body

Modify a compliance policy

Attributes	Required / Optional	Type	Description
policy	Required	Object	Information about the compliance policy
action	Required	String	Action to take. This is always **edit**.
description	Optional	String	Compliance policy description
details	Optional	Array of objects	Details about the compliance policy
baseVersion	Optional	String	For CMMs or switches, this is the fix ID of the package. For servers, the following is returned. `xxxx_utl_uxsp_xxxxxx-1.00_xxxx_32-64`
components	Optional	Array of objects	Information about each firmware component
isDefault	Required	String	Specifies if the component update is the default component (the latest component update). This can be one of the following values. • **yes**. This firmware component is the default. • **no**. This firmware component is not the default.
name	Required	String	Component name

Attributes	Re-quired / Optional	Type	Description
rule	Required	String	Rule for raising a non-compliant alert. This can be one of the following values. • **alertIfNotExactMatch**. Show non-compliance when the installed version on device does not exactly match the compliance target. • **alertIfDownlevel**. Show non-compliance when the installed version on device is earlier than the compliance target. • **noAlerting**. Never show non-compliance.
targetVersion	Required	String	Firmware level that is the baseline for the specified device type
type	Required	String	(Servers only) Package type. This can be one of the following values. • **IMM** • **IMM** • **UEFI** • **UEFI-Backup**
id	Optional	String	System type used to identify the CMM. Internal use only
isDefault	Optional	String	Indicates if the update package is the default package (the latest package). This can be one of the following values. • **yes**. This is the default update package • **no**. This is not the default update package
isUXSP	Optional	String	Indicates if this update package is a UXSP package. This can be one of the following values. • **yes**. This is a UXSP package • **no**. This is not a UXSP package
rule	Optional	String	Rule for raising a non-compliant alert. This can be one of the following values. • **alertIfNotExactMatch**. Show non-compliance when the installed version on device does not exactly match the compliance target. • **alertIfDownlevel**. Show non-compliance when the installed version on device is earlier than the compliance target. • **noAlerting**. Never show non-compliance. • **custom**. Follow the detailed rules of each firmware component.
systemType	Optional	String	Type of device for which the policy applies
filterType	Optional	String	Filter type. This can be one of the following values. • **all**. All supported machine types • **managed**. Only managed machine types.
name	Optional	String	Compliance policy name
oldPolicyName	Optional	String	
updateRule	Optional	String	Internal use only
user	Optional	String	Name of the user that created the policy

The following example modifies a compliance policy when the query parameter `action=edit` is specified.

```
{
   "policy": {
      "action": "edit",
      "description": "",
      "details": [{
         "baseVersion": "lnvgy_fw_cmm_1aon12a-1.5.0a_anyos_noarch",
         "components": [],
         "id": "8721_Lenovo",
         "isDefault": "yes",
         "isUXSP": "no",
         "rule": "alertIfDownlevel",
         "systemType": "8721"
      }],
      "filterType": "managed",
      "name": "Test11",
      "oldPolicyName": "Test11",
      "updateRule": "",
      "user": "USERID"
   }
}
```

Export a compliance policy policy with or without packages

Attributes	Required / Optional	Type	Description
export	Required	String	List of names of the compliance policies to be exported, separate by a comma. To obtain a list of compliance policy names, use the GET /compliancePolicies method.

The following example deletes four compliance policies only if those policies are not in the “Assigned” state when the query parameter `action=export` is specified

```
{
   "export": "test, Copy-test, Copy-Copy-test"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Edit a compliance policy

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages) The **result** attribute can be one of the following values. • **informational**. The request completed successfully. • **minor**. The request failed with a minor issue. • **major**. The request failed with a major issue.

The following example is returned if the request is successful.

```
{
   "result": "informational",
   "messages": [{
      "id": "FQXHMUP3006I",
      "text": "Policy operation completed successfully."
   }]
}
```

Export a compliance policy

Attributes	Type	Description
exportURL	String	Zip file name of exported files
result	String	Results of the request. This can be one of the following values. • **informational**. The request completed successfully.
success	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned when compliance policies were exported successfully.

```
{
   "exportURL": "policies2016042517245649.zip",
   "success": "success",
   "result": "informational",
   "messages": [{
      "id": "FQXHMUP3031I",
      "text": "Policy export completed successfully."
   }]
}
```

Export a compliance policy

Attributes	Type	Description
jobid	Integer	Job ID

The following example is returned when compliance policies were exported successfully.

```
{
   "jobid": "1027"
}
```

POST /compliancePolicies

Use this method to create, copy, or import a firmware-compliance policy in Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/compliancePolicies`

Query parameters

Parameters	Required / Optional	Description
action=*{action}*	Required	Action type. This can be one of the following values. • **create**. Add a compliance policy. • **copy**. Copy a compliance policy.

The following example creates a compliance policy.

```
POST https://192.0.2.0/compliancePolicies?action=create
```

Request body

Table 57. Create a compliance policy

Attributes	Required / Optional	Type	Description
policy	Required	Object	Information about the compliance policy
action	Required	String	Action to take. This is always **create**.
description	Optional	String	Compliance policy description
details	Required	Array of objects	Details about the compliance policy
baseVersion	Required	String	For CMMs or switches, this is the fix ID of the package. For servers, the following is returned. `xxxx_utl_uxsp_xxxxxx-1.00_xxxx_32-64`
components	Required	Array of objects	Information about each firmware component
isDefault	Required	String	Specifies if the component update is the default component (the latest component update). This can be one of the following values. • **yes**. This firmware component is the default. • **no**. This firmware component not is the default.
name	Required	String	Component name

Table 57. Create a compliance policy (continued)

Attributes	Required / Optional	Type	Description
rule	Required	String	Rule for raising a non-compliant alert. This can be one of the following values. • **alertIfNotExactMatch**. Show non-compliance when the installed version on device does not exactly match the compliance target. • **alertIfDownlevel**. Show non-compliance when the installed version on device is earlier than the compliance target. • **noAlerting**. Never show non-compliance.
targetVersion	Required	String	Firmware level that is the baseline for the specified device type
type	Required	String	(Servers only) Package type. This can be one of the following values. • **IMM** • **IMM** • **UEFI** • **UEFI-Backup**
id	Required	String	System type used to identify the CMM. Internal use only
isDefault	Required	String	Indicates whether the update package is the default package (the latest package). This can be one of the following values. • **yes**. This is the default update package. • **no**. This is not the default update package.
isDoNotUpdate	Required	String	Indicates whether the policy is set to “do not update.” ++ +This can be one of the following values. • **yes**. The policy is set to “Do not update.” • **no**. The policy is not set to “Do not update.”
isUXSP	Required	String	Indicates whether this update package is a UXSP package. This can be one of the following values. • **yes**. This is a UXSP package. • **no**. This is not a UXSP package.
rule	Required	String	Rule for raising a non-compliant alert. This can be one of the following values. • **alertIfNotExactMatch**. Show non-compliance when the installed version on device does not exactly match the compliance target. • **alertIfDownlevel**. Show non-compliance when the installed version on device is earlier than the compliance target. • **noAlerting**. Never show non-compliance. • **custom**. Follow the detailed rules of each firmware component.
systemType	Required	String	Type of device for which the policy applies
filterType	Required	String	Filter type. This can be one of the following values. • **all**. All supported machine types • **managed**. Only managed machine types.
name	Required	String	Compliance policy name

Table 57. Create a compliance policy (continued)

Attributes		Required / Optional	Type	Description
	oldPolicyName	Required	String	Specify an empty value when creating a compliance policy
	updateRule	Required	String	Internal use only
	user	Required	String	Name of the user that requested to create the policy

The following example creates a new compliance policy when the query parameter `action=create` is specified.

```
{
   "policy": {
      "action": "create",
      "description": "",
      "details": [{
         "baseVersion": "xxxx_utl_uxsp_xxxxxx-1.00_xxxx_32-64",
         "components": [{
            "name": "Integrated Management Module 2 (IMM2) Update (Standby)",
            "rule": "alertIfDownlevel",
            "type": "IMM-Backup",
            "targetVersion": "DoNotUpdate_ibm_fw_imm2_1aoo81a-6.60_anyos_noarch",
            "isDefault": "yes"
         }],
         "id": "8737",
         "isDefault": "no",
         "isDoNotUpdate": "yes",
         "isUXSP": "no",
         "rule": "custom",
         "systemType": "8737",
      }],
      "filterType": "managed",
      "name": "4234234234",
      "oldPolicyName": ""
      "updateRule": "",
      "user": "USERID"
   }
}
```

Table 58. Copy a compliance policy

Attributes	Required / Optional	Type	Description
oldPolicyName	Required	String	Name of policy to be copied
prefix	Required	String	Prefix of copied policy name
user	Required	String	Name of the user that requested to copy the policy

The following example copies an existing policy when the query parameter `action=copy` is specified.

```
{
   "oldPolicyName": "test",
   "user": "USERID",
   "prefix": "Copy"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
307	Temporary Redirect	The URL changed for this REST API. The response header returns the correct URL in the Location attribute. The URL changed for this REST API when **action=import** is specified.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Table 59. Create a compliance policy

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages) The **result** attribute can be one of the following values. • **informational**. The request completed successfully. • **minor**. The request failed with a minor issue. • **major**. The request failed with a major issue.

The following example is returned if the request is successful.

```
{
   "result": "informational",
   "messages": [{
      "id": "FQXHM3006I",
      "text": "Policy operation completed successfully."
   }]
}
```

Table 60. Copy a compliance policy

When the request is successful, the following attributes are returned in the response body. If the request fails, standard message attributes are returned (see Status messages), where the **result** attribute can be one of the following values: **informational**, **minor**, or **major**.

Attributes	Type	Description
description	String	Compliance policy description
filterType	String	Filter type. This can be one of the following values. • **all**. All supported machine types • **managed**. Only managed machine types.
id	String	Compliance policy ID

Table 60. Copy a compliance policy (continued)

Attributes	Type	Description
inUse	String	Identifies whether the compliance policy is in use. This can be one of the following values. • **true**. The compliance policy is in use. • **false**. The compliance policy is not in use.
lastAction	String	Last action that was performed on the compliance policy. This can be one of the following values. • **Predefined**. The compliance policy is predefined. • **Created by** *{user_name}*. The user-defined compliance policy was created by the specified user. • **Edited by** *{user_name}*. The user-defined compliance policy was edited by the specified user.
lastModified	String	Timestamp of the last change to the compliance policy
lastEdited	String	Timestamp of the last change to the compliance policy
name	String	Compliance policy name
updateRule	String	Internal use only
userDefined	String	Identifies whether the compliance policy is user-defined. This can be one of the following values. • **yes**. The compliance policy is user-defined. • **no**. The compliance policy is predefined.

The following example is returned if the request is successful.

```
{
   "description": "",
   "filterType": "all",
   "id": "1624433666597",
   "inUse": false,
   "lastAction": "Created by USERID",
   "lastEdited": "2021-06-23T07:34:26Z",
   "lastModified": "This policy was created by USERID on 2021-06-23T07:34:26Z",
  "name": "Copy1-test",
   "updateRule": "",
   "userDefined": "yes"
}
```

Table 61. Import a compliance policy

Attributes	Type	Description
errorMsg	Object	Information about firmware-compliance policy files that are not valid
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message

Table 61. Import a compliance policy (continued)

Attributes	Type	Description
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
popMsg	Object	Information about firmware-compliance policy files that exist on the management server
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
successMsg	Object	Information about firmware-compliance policy files that were imported successfully
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event

The following example is returned if the request is successful.

```
{
   "errorMsg": {
      "result": "major",
      "messages": [{
         "id": "FQXHMUP3033L",
         "text": "Some files failed to import and are discarded.",
         "explanation": "The following files are invalid and have been discarded: TestB.xml.",
         "recovery": {
            "text": "Please check the contents of files. Ensure that the uploaded files include
                     the correct .xml file."
         }
      }]
```

```
   },
   "popMsg": {
      "result": "warning",
      "messages": [{
         "id": "FQXHMUP3032F",
         "text": "Some files failed to import and are discarded.",
         "explanation": "The following policy files already exist on system and have been
                         discarded: DEFAULT-2015-04-25.xml.",
         "recovery": {
            "text": "Rename or delete the existing compliance policy in the Compliance Policy
                     page, and retry the import."
         }
      }]
   },
   "successMsg": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP3030I",
         "text": "Policy import completed successfully."
      }]
   }
}
```

DELETE /compliancePolicies

Use this method to delete one or more compliance policies.

Important: Only compliance policies that are not in the “Assigned” state are deleted.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/compliancePolicies`

Query parameters

Parameters	Required / Optional	Description
policyName=*{name}*	String	Name of one or more compliance policies to be deleted, separated by a comma
removePackage=*{boolean}*	String	Identifies whether to delete the firmware-update packages that are associated with the specified compliance policies if the packages are not associated with another compliance policy. This can be one of the following values. • **true**. Deletes the firmware-update packages. • **false**. Does not delete the firmware-update packages **Note:** All package files (payload, metadata, readme and history) are deleted.

The following example deletes four compliance policies and deletes the associated firmware-update packages.

```
POST https://192.0.2.0/compliancePolicies?policyName=policy1,policy2,policy3,policy4&removePackage=true
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
success	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "message":[],
   "success":"success"
}
```

/compliancePolicies/applicableFirmware

Use this REST API to retrieve information about applicable firmware.

HTTP methods

GET

GET /compliancePolicies/applicableFirmware

Use this method to return firmware-compliance information for managed devices.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/compliancePolicies/applicableFirmware
```

Query parameters

Parameters	Required / Optional	Description
refresh=*{Boolean}*	Optional	Indicates whether to refresh the firmware-compliance information for each specified device by comparing the compliance policies for each specified device against the latest available firmware repository. This can be one of the following values. • **true**. Refresh the firmware-compliance information for each specified device. • **false**. Return existing firmware-compliance information for each specified device.
uuids=*{uuid_list}*	Optional	Returns firmware-compliance information for one or more specific devices, specified by UUID and separated by a comma To return information for all managed devices, specify **all**. This is the default value.
hasPayload=*{Boolean}*	Optional	Indicates whether to include firmware updates that do not have payload files available in the repository. This can be one of the following values. • **true**. Returns a list of the latest-available, applicable firmware updates in the repository that have downloaded payload files. • **false**. Returns a list of the latest-available, applicable firmware updates in the repository that do not have downloaded payload files. If not specified, this method returns a list of the latest-available, applicable firmware updates in the repository regardless of whether the payload files are downloaded. This is the default behavior.

The following example returns existing compliance information for all managed devices. All applicable firmware updates in the repository are included in the response, regardless of whether the payload files are available in the repository.

```
GET https://192.0.2.0/compliancePolicies/applicableFirmware
```

The following example refreshes and returns the latest firmware-compliance information for two specific managed devices. All applicable firmware updates in the repository are included in the response, regardless of whether the payload files are available in the repository.

```
GET https://192.0.2.0/compliancePolicies/applicableFirmware?refresh=true
&uuids=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
```

The following example returns existing compliance information for all managed devices. Only applicable firmware updates that have payload files that are available in the repository are included in the response.

```
GET https://192.0.2.0/compliancePolicies/applicableFirmware?hasPayload=true
```

The following example returns existing compliance information for all managed devices. Only applicable firmware updates that do not have payload files in the repository are included in the response

```
GET https://192.0.2.0/compliancePolicies/applicableFirmware?hasPayload=false
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
componentTypes	Array of objects	Information for all managed devices
applicableFirmware	Array of objects	Information applicable firmware updates for managed devices
available	Array	Information about the available firmware-update packages
buildNum	String	Package build number
buildType	String	Build type
fixid	String	Fix ID
name	String	Package name
hasPayload	Boolean	Indicates whether the payload files are in the repository. This can be one of the following values. • **true**.Payload files are in the repository. • **false**. Payload file are not in the repository.
releasedate	String	Release date
softwareIDList	Array of strings	List of software IDs
version	String	Version
versionList	Array of strings	List of all versions in the package
category	String	Type of firmware update, such as IMM2, UEFI, Network, and ServeRAID
name	String	Name of firmware update
machineType	String	Machine type of managed device
uuid	String	UUID of managed device

The following example is returned if the request is successful.


```
{
   "componentTypes": [{
      "applicableFirmware": [{
         "available": [{
            "buildNum": "TCOO15M",
            "buildType": "development",
            "fixid": "lnvgy_fw_imm2_tcoo15m-2.50_anyos_noarch",
            "hasPayload": true,
            "name": "Integrated Management Module 2 (IMM2) Update",
            "releasedate": "2016-01-09",
            "softwareIDList": ["IMM2-Backup"],
            "version": "2.50",
            "versionList": ["2.50"]
         }],
         "category": "IMM2-Backup",
         "installedVersion": "1.95",
         "name": "IMM2 (Backup)"
      }],
      "machineType": "5463",
      "uuid": "208C0140DF7F11D4AE0FF3F3F3797979"
   }]
}
```


/compliancePolicies/compareResult

Use this REST API to retrieve information about or assign compliance policies to one or more devices.

HTTP methods

GET, POST

GET /compliancePolicies/compareResult

Use this method to determine whether devices are compliant with the assigned compliance policy using the job or task ID that was returned when the compliance policy was assigned.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/compliancePolicies/compareResult`

Query parameters

Parameters	Required / Optional	Description
jobid=*{job_id}*	Required	Job ID that was returned by POST /compliancePolicies/compareResult
uuid=*{uuid}*	Required	UUID of the device to which the compliance policy was assigned using the specified job ID If the value is null or empty, compliance information is returned for all devices in the job.

The following example returns information about whether a device is compliant with the assigned compliance policy.

```
GET https://192.0.2.0/compliancePolicies/compareResult?jobid=15&uuid=4DE3B51797C311E2B41F3440B5EABAE8
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
assignCount	Integer	Number of assignment requests
failedCount	Integer	Number of failed assignments
failedDevices	Array of objects	Information about devices with a compliance error
originalPolicy	String	ID of the original compliance policy
targetPolicy	String	ID of the target compliance policy that failed to be assigned
uuid	String	Device UUID
successCount	Integer	Number of successful assignments
jobid	String	Job ID
percentage	Integer	Percent complete
result	Array	
endpointCompliant	String	Identifies whether the device is compliant with the policy. This can be one of the following values. • **yes**. The device is compliant. • **no**. The device is not compliant. • **failed**. There is a compliance error.
message	Array of objects	Message that is returned from the assignment of the policy
status	String	Task status (same as the job status)
targetFirmware	Array of objects	Information about each firmware update in the compliance policy
category	String	Firmware-update category
build	String	Firmware-update build

Attributes	Type	Description
compliant	String	Compliance result after the policy is assigned. This can be one of the following values. • **yes**. Compliant. • **no**. Not compliant • **DoNotUpdate**. Do not update this component.
componentID	String	Component ID. For CMMs or switches, this is the UUID. For server components this is specified as server UUID:component name.
componentName	String	Component name
date	String	Firmware update package release date
fixid	String	Firmware-update ID
level	String	Firmware-update level
packageExistence	Boolean	Identifies whether the firmware update package exists in the updates repository. This can be one of the following values. • **yes**. The firmware update exists. • **no**. The firmware update does not exists.
reason	String	Explanation of the result of the compliance check
versionList	Array of strings	Version list of firmware update package (one firmware update package might contain multiple parts)
taskid	String	Task ID
uuid	String	UUID
status	String	Status of the job. This can be one of the following values. • **notstarted** • **inprogress** • **failed** • **finished** • **cancel**

The following example is returned if the request is successful.


```
{
   "assignCount": 23,
   "failedCount": 2,
   "failedDevices": [{
      "originalPolicy": "v3.2.0-2018-10-26-SystemX-Switch-DEV",
      "targetPolicy": "v3.2.0-2018-10-26-SystemX-Switch-DEV",
      "uuid": "4DE3B51797C311E2B41F3440B5EABAE8"
   },
   {
      "originalPolicy": "v3.2.0-2018-10-26-SystemX-Switch-DEV",
      "targetPolicy": "v3.2.0-2018-10-26-SystemX-Switch-DEV",
      "uuid": "4DE3B51797C311E2B41F3440B5EABAE8"
   }],
   "successCount": 21,
   "jobid": "14",
   "percentage": 100,
   "result": [{
      "endpointCompliant": "no"
      "message": [],
      "status": "finished",
      "targetFirmware": [{
         "build": "0708",
         "category": "Swithes",
```

```
            "compliant": "no",
            "componentID": "A3F8482B012B32188E68375DD5FF40EE",
            "componentName": "Demo - 00004X4093",
            "date": "2015-02-13",
            "fixid": "fw_scsw_en4093r-7.8.9.0_anyos_noarch",
            "level": "higher",
            "packageExistence": "yes",
            "reason": "The installed version is down level than the version defined in compliance
                       policy.",
            "versionList": ["7.8.9.0"]
         }],
         "taskid": "0",
         "uuid": "A3F8482B012B32188E68375DD5FF40EE"
      }],
      "status": "finished"
}
```


POST /compliancePolicies/compareResult

Use the method to assign a compliance policy to one or more devices and to return the job ID and task IDs for monitoring the status of the job and tasks.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/compliancePolicies/compareResult`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
compliance	Required	Array of objects	Information about each compliance policy
autoAssign	Optional	Boolean	Indicates whether to automatically assign the specified compliance policy when a new device of the specified type is detected. This can be one of the following values. • **true**. Automatically assign the specified compliance policy. • **false**. (default) Do not automatically assign the specified compliance policy.
keep	Optional	Boolean	Indicates when to return results when monitoring the status of the assignment job or task. This can be one of the following values. • **true**. (default) Wait for the policy assignment to complete before returning the status. • **false**. Return current status immediately even if the assignment is not complete.
policyname	Required	String	Name of the compliance-policy to be assigned To obtain a list of policy names, use GET /compliancePolicies.

Attributes	Re-quired / Optional	Type	Description
type	Required	String	Device type. This can be one of the following values. • **CMM** • **IOSwitch**. Flex switch • **SWITCH** • **SERVER** • **STORAGE**. Rack storage device
uuid	Required	String	UUID of the device to which you want to assign the compliance policy

The following example assigns a compliance policy to a device.

```
{
   "compliance":[{
      "keep":false,
      "policyName":"DEFAULT-2015-04-01",
      "type":"IOSwitch",
      "uuid":"A3F8482B012B32188E68375DD5FF40EE"
   }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

You can use GET /tasks/*{job_list}* to monitor the progress of the compliance-policy assignment job and tasks using the **taskid** and **jobid** response attributes.

Attributes	Type	Description
errorDetail	Array	Error message if an error occurred
errorMessage	String	
message	Array	
jobid	Integer	Job ID for the policy assignment
tasks	Array	Information about each task in the job
taskid	Integer	Task ID

Attributes	Type	Description
uuid	String	Task UUID
status	String	Status of the job. This can be one of the following values. • **success** • **notstarted** • **inprogress** • **failed** • **finished** • **cancel**

The following example is returned if the request is successful.

```
{
   "errorDetail": [],
   "errorMessage": "",
   "message": [{
      "tasks": [{
         "taskid": 0,
         "uuid": "A3F8482B012B32188E68375DD5FF40EE"
      }],
      "jobid": 14
   }],
   "status": "success"
}
```

/compliancePolicies/persistedResult

Use this REST API to retrieve the persisted compare result for servers to which a policy is assigned. You can also use this REST API to unassign compliance policies that are assigned to one or more specific devices.

HTTP methods

GET, POST

GET /compliancePolicies/persistedResult

Use this method to return the persisted compare result for servers to which a compliance policy is assigned.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/compliancePolicies/persistedResult`

Query parameters

If all query parameters are empty or null, all the persisted compliance result are returned.

Parameters	Re-quired / Optional	Description
complexid=*{uuid}*	Optional	Returns the persisted compliance results for only scalable complexes
uuid=*{uuid}*	Optional	Returns the persisted results for only the device specified by the UUID and resource type
type=*{device_type}*	Optional	When the **uuid** query parameter is specified, this query parameter is used to indicate the resource type. • **CHASSIS** • **CMM** • **IOSwitch**. Flex switch • **RACKSWITCH**. RackSwitch switch • **SERVER**. • **STORAGE**. Rack storage device

The following example returns the persisted compliance results for only scalable complexes.

```
GET https://192.0.2.0/compliancePolicies/persistedResult?complexid=C156CA72D6E811E48F0F6EAE8B4BDB07
```

The following example returns the persisted results for only the device specified by the UUID and resource type.

```
GET https://192.0.2.0/compliancePolicies/persistedResult?type=SERVER&uuid=41C8528EDC3E11E6B757C80D4FC25D9F
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
all	Array	
chassis	String	Chassis UUID
cmms		Compliance policy information for each CMM
deviceCompliant	Boolean	Identifies whether the CMM is compliant. This can be one of the following values. • **yes**. The CMM is compliant. • **no**. The CMM is not compliant.

Attributes	Type	Description
message	Array	Error message that is returned if an error occurs
policyName	String	Firmware-compliance policy that is associated with the CMM
supported	Boolean	Identifies whether the CMM is supported. This can be one of the following values. • **true**. The CMM is supported. • **false**. The CMM is not supported.
targetFirmware	Array	Information about firmware
build	String	Update build
category	String	Update category
compliant	String	Indicates whether the CMM firmware is compliant with the policy. This can be one of the following values. • **yes**. Compliant. • **no**. Not compliant. • **DoNotUpdate**. Do not update this component.
componentID	String	For a CMM, this is the CMM UUID
componentName	String	Name of the CMM
date	String	Update date
fixid	String	Update- ID
installedFirmware	Array of objects	Information about each firmware that is installed on the component
build	String	Firmware build level
date	String	Firmware date
name	String	Firmware name
versionList	Array of strings	List of versions that were installed
level	String	Update level
packageExistence	String	Identifies whether the update package exists in the firmware-updates repository. This can be one of the following values. • **yes**. The update package exists. • **no**. The update package does not exist.
reason	String	Explanation for the result of the compliance check
versionList	Strings	Update package version
uuid	String	CMM UUID
racklist	Object	If there are racks managed, and you queried for all persisted compliance results, return those results
deviceCompliant	Boolean	Identifies whether the CMM is compliant. This can be one of the following values. • **yes**. The CMM is compliant. • **no**. The CMM is not compliant.
message	Array	Error message that is returned if an error occurs
policyName	String	Firmware-compliance policy that is associated with the CMM

Attributes	Type	Description
supported	Boolean	Identifies whether the CMM is supported. This can be one of the following values. • **true**. The CMM is supported. • **false**. The CMM is not supported.
targetFirmware	Array	Information about firmware
category	String	Update category
build	String	Update build
compliant	String	Indicates whether the CMM firmware is compliant with the policy. This can be one of the following values. • **yes**. Compliant. • **no**. Not compliant. • **DoNotUpdate**. Do not update this component.
componentID	String	For a CMM, this is the CMM UUID
componentName	String	Name of the CMM
date	String	Update date
fixid	String	Update- ID
installedFirmware	Array of objects	Information about each firmware that is installed on the component
build	String	Firmware build level
date	String	Firmware date
name	String	Firmware name
versionList	Array of strings	List of versions that were installed
level	String	Update level
packageExistence	String	Identifies whether the update package exists in the firmware-updates repository. This can be one of the following values. • **yes**. The update package exists. • **no**. The update package does not exist.
reason	String	Explanation for the result of the compliance check
versionList	Strings	Update package version
uuid	String	CMM UUID.
rackswitchlist	Object	Compliance policy information for each managed RackSwitch switch
deviceCompliant	String	Identifies whether the RackSwitch switch is compliant. This can be one of the following values. • **yes**. The switch is compliant. • **no**. The switch is not compliant.
message	Array	Error message if an error occurs for this RackSwitch switch
policyName	String	Firmware-compliance policy that is associated with the RackSwitch switch

Attributes	Type	Description
supported	String	Identifies whether the RackSwitch switch is supported. This can be one of the following values. • **true**. The RackSwitch switch is supported. • **false**. The RackSwitch switch is not supported.
targetFirmware	Array	Information about firmware
build	String	Update build
category	String	Type of firmware update
compliant	String	Indicates whether the RackSwitch switch firmware is compliant with the firmware-compliance policy. This can be one of the following values. • **yes**. Compliant. • **no**. Not compliant. • **DoNotUpdate**. Do not update this component.
componentID	String	RackSwitch switch UUID
componentName	String	RackSwitch switch name
date	String	Update date
fixid	String	Update ID
installedFirmware	Array of objects	Information about each firmware that is installed on the component
build	String	Firmware build level
date	String	Firmware date
name	String	Firmware name
versionList	Array of strings	List of versions that were installed
level	String	Update level
packageExistence	String	Identifies whether the update package exists in the firmware-updates repository. This can be one of the following values. • **yes**. The update package exists. • **no**. The update package does not exist.
reason	String	Explanation for the result of the compliance check
versionList	Array of string	Update package version
uuid	String	RackSwitch switch UUID
storagelist	Object	Compliance policy information for each managed storage device
deviceCompliant	String	Identifies whether the storage device is compliant. This can be one of the following values. • **yes**. The storage device is compliant. • **no**. The storage device is not compliant.
message	String	Error message if an error occurs for this storage device
policyName	String	Firmware-compliance policy that is associated with the storage device

Attributes	Type	Description
supported	String	Identifies whether the storage device is supported. This can be one of the following values. • **true**. The storage device is supported. • **false**. The storage device is not supported.
targetFirmware	Array	Information about firmware
build	String	Update build
category	String	Type of firmware update
compliant	String	Indicates whether the storage device firmware is compliant with the firmware-compliance policy. This can be one of the following values. • **yes**. Compliant. • **no**. Not compliant. • **DoNotUpdate**. Do not update this component.
componentID	String	Storage device UUID
componentName	String	Storage device name
date	String	Update date
fixid	String	Update ID
installedFirmware	Array of objects	Information about each firmware that is installed on the component
build	String	Firmware build level
date	String	Firmware date
name	String	Firmware name
versionList	Array of strings	List of versions that were installed
level	String	Update level
packageExistence	String	Identifies whether the update package exists in the firmware-updates repository. This can be one of the following values. • **yes**. The update package exists. • **no**. The update package does not exist.
reason	String	Explanation for the result of the compliance check
versionList	Array of strings	Update package version
uuid	String	Storage device UUID
switches	Object	Compliance policy information for each Flex System switch
deviceCompliant	String	Identifies whether the switch is compliant. This can be one of the following values. • **yes**. The Flex System switch is compliant. • **no**. The Flex System switch is not compliant.
message	Array	Error message if an error occurs for this Flex System switch
policyName	String	Firmware-compliance policy that is associated with the Flex System switch

Attributes	Type	Description
supported	String	Identifies whether the Flex System switch is supported. This can be one of the following values. • **true**. The Flex System switch is supported. • **false**. The Flex System switch is not supported.
targetFirmware	Array	Information about firmware
build	String	Update build
category	String	Type of firmware update, such as IMM2, UEFI, Network, and ServeRAID
compliant	String	Indicates whether the Flex System switch firmware is compliant with the policy. This can be one of the following values. • **yes**. Compliant. • **no**. Not compliant. • **DoNotUpdate**. Do not update this component.
componentID	String	For a Flex System switch, this is the switch UUID
componentName	String	Flex System switch name
date	String	Update date
fixid	String	Update ID
installedFirmware	Array of objects	Information about each firmware that is installed on the component
build	String	Firmware build level
date	String	Firmware date
name	String	Firmware name
versionList	Array of strings	List of versions that were installed
level	String	Update level
packageExistence	String	Identifies whether the update package exists in the firmware-updates repository. This can be one of the following values. • **yes**. The update package exists. • **no**. The update package does not exist.
reason	String	Explanation for the result of the compliance check
versionList	Strings	Update package version
uuid	String	Flex System switch UUID
xITEs	Object	Compliance policy information for each server
message	Array	Error message that is returned if an error occurs
deviceCompliant	Boolean	Identifies whether the server is compliant. This can be one of the following values. • **yes**. The server is compliant. • **no**. The server is not compliant.
policyName	String	Firmware-compliance policy that is associated with the server
supported	Boolean	Identifies whether the server is supported. This can be one of the following values. • **true**. The server is supported. • **false**. The server is not supported.

Attributes	Type	Description
targetFirmware	Array	Information about firmware
build	String	Update build
category	String	Update category
compliant	String	Indicates whether the server firmware is compliant with the policy. This can be one of the following values. • **yes**. • **no**.
componentID	String	For servers, this is returned as server UUID:component name
componentName	String	Component name
date	String	Update date
fixid	String	Update ID
level	String	Update level
installedFirmware	Array of objects	Information about each firmware that is installed on the component
build	String	Firmware build level
date	String	Firmware date
name	String	Firmware name
versionList	Array of strings	List of versions that were installed
packageExistence	String	Identifies whether the update package exists in the firmware-updates repository. This can be one of the following values. • **yes**. The update package exists. • **no**. The update package does not exist.
reason	String	Explanation for the result of the compliance check
versionList	Strings	Update package version
uuid	String	Server UUID
message	Array	Error message that is returned if an error occurs

The following example is returned if the request is successful.

```
{
   "all": [
   {
      "chassis": "FBEF740B178F4EFAA846E7225EE256DC",
      "cmms": [{
         "deviceCompliant": ""."message": [],
         "policyName": "",
         "supported": "true",
         "targetFirmware": [],
         "uuid": "387E51D69EC311E0A4C8E87E4D6C0479"
      }]
      "switches": [{
         "deviceCompliant": "no",
         "message": [],
         "policyName": "DEFAULT-2015-04-25",
         "supported": "true",
         "targetFirmware": [{
```

```
            "build": "0802",
            "category": "Switches",
            "compliant": "no",
            "componentID": "1B33D6C57ECB04C14567A897DC604900",
            "componentName": "IO Module 02",
            "date": "2015-04-22",
            "fixid": "lnvgy_fw_scsw_si4093-8.2.1.0_anyos_noarch",
            "installedFirmware": [{
               "build": "",
               "date": "2014-05-20",
               "name": "Boot ROM",
               "versionList": ["7.8.3.15"]
            },
            {
               "build": "",
               "date": "2014-05-20",
               "name": "Main Application 1",
               "versionList": ["7.8.3.15"]
            },
            {
               "build": "" ,
               "name": "Main Application 2",
               "date": "2014-05-20",
               "versionList": ["7.8.3.15"]
            }],
            "level": "higher",
            "packageExistence": "yes",
            "reason": "The installed version is down level than the version defined in compliance policy.",
            "versionList": ["8.2.1.0"]
         }],
         "uuid": "1B33D6C57ECB04C14567A897DC604900"
      }],
      "xITEs": [{
         "deviceCompliant": "",
         "message": [],
         "policyName": "",
         "supported": "true",
         "targetFirmware": [],
         "uuid": "69BDF8912E5211E4998B40F2E99033F0"
      }]
   }
   {
      "racklist": [{
         "policyName": "",
         "endpointCompliant": "",
         "targetFirmware": [],
         "message": [],
         "uuid": "200B8108289D11E3878E000AF725674C"
      }]
   },
   {
      "complexlist": []
   },
   {
      "rackswitchlist": []
   },
   {
      "storagelist": []
   }]
}
```

POST /compliancePolicies/persistedResult

Use this method to unassign compliance policies that are assigned to one or more specific devices.

This method unassigns one or more compliance policies that are assigned to specific devices, updates the persisted result on the disk drive, and caches in memory that is related to this policies and devices.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/compliancePolicies/persistedResult`

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
unassign	Required	Array of objects	List of managed devices for which you want to retrieve compare results
uuid	Required	String	Unique ID of the managed device

The following example unassigns the compliance policy from the device with UUID `C156CA72D6E811E48F0F6EAE8B4BDB07`.

```
{
   "unassign":[{
      "uuid":"C156CA72D6E811E48F0F6EAE8B4BDB07"
   }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
failedCount	Integer	Number of failed unassignments
failedDevices	Array of objects	Information about devices with failed compliance
originalPolicy	String	ID of the original compliance policy
uuid	String	Device UUID
successCount	Integer	Number of successful unassignments
unassignCount	Integer	Number of unassignment requests
success	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier
originalPolicy	String	ID of the compliance policy that was unassigned
uuid	String	Device UUID

The following example is returned if the request is successful.


```
{
   "failedCount": 0,
   "failedDevices": [],
   "unassignCount": 29,
   "successCount": 27,
   "messages": [{
      "explanation": "",
      "id": "FQXHMUP2000I",
      "recovery": [],
      "text": "The command completed successfully."
      "originalPolicy": "v2.2.0-2018-10-26-SystemX-Switch-DEV"
      "uuid": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
   }]
}
```


/files/compliancePolicies?action=import

Use this REST API to import a zip file containing firmware-compliance policies into Lenovo XClarity Administrator.

HTTP methods

POST

POST /files/compliancePolicies?action=import

Use this method to import a zip file containing firmware-compliance policies into Lenovo XClarity Administrator.

A job is created to import the compliance policy. Use the GET /tasks/*{job_list}* (where *{job_id}* is the job ID) to retrieve the overall job status. If a job was not successfully started, refer to the response code and response body for details.

Note: A compliance policy that includes update packages might take a longer time to import.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/files/compliancePolicies?action=import
```

Query parameters

Parameters	Required / Optional	Description
action=import	Required	Imports firmware-compliance policies

The following example imports a compliance policy (with or without update packages)

```
POST https://192.0.2.0/files/compliancePolicies?action=import
```

Request body

Use the "multipart/form-data" media type to import the update package. Use the attributes in the following table as the multipart name in the body. For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage.

The following example imports a zip file containing firmware-compliance policies.

HTTP Header

```
Content-Type: multipart/form-data; boundary=AaB03x
```

Request body

```
--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]"; filename="policies2018103122275762.zip"
   Content-Type: application/x-zip-compressed

 --AaB03x
  Content-Disposition: form-data; name="uploadedfiles[]"; filename="policies2018102523335745.zip"
   Content-Type: application/x-zip-compressed

--AaB03x--
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
413	Request Entity Too Large	Clients might impose limitations on the length of the request URI, and the request URI is too long to be handled. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
jobid	Integer	Job ID
status	String	Import status. This can be one of the following values. • **success**. The request completed successfully. • **error**. The request failed. A descriptive error message is returned.
errorMsg	Object	Information about firmware-compliance policy files that are not valid
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
popMsg	Object	Information about firmware-compliance policy files that exist on the management server
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages

Attributes	Type	Description
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event

The following example is returned if the request is successful.

```
{
   "jobid": 127,
   "status": "success",
   "errorMsg": {
      "result": "major",
      "messages": [{
         "id": "FQXHMUP3033L",
         "text": "Some files failed to import and are discarded.",
         "explanation": "The following files are invalid and have been discarded: TestB.xml.",
         "recovery": {
            "text": "Please check the contents of files. Ensure that the uploaded files include
                     the correct .xml file."
         }
      }]
   },
   "popMsg": {
      "result": "warning",
      "messages": [{
         "id": "FQXHMUP3032F",
         "text": "Some files failed to import and are discarded.",
         "explanation": "The following policy files already exist on system and have been
                         discarded: DEFAULT-2015-04-25.xml.",
         "recovery": {
            "text": "Rename or delete the existing compliance policy in the Compliance Policy
                     page, and retry the import."
         }
      }]
   },
   "successMsg": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP3030I",
         "text": "Policy import completed successfully."
      }]
   }
}
```

/files/updateRepositories/firmware/import

Use this REST API to import a firmware update or UpdateXpress System Pack (UXSP) in to the repository.

HTTP methods

POST

POST /files/updateRepositories/firmware/import

Use this method to import a firmware update or UpdateXpress System Pack (UXSP) to the updates repository.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/files/updateRepositories/firmware/import
```

Query parameters

Parameters	Required / Optional	Description
jobid={jobID}	Required	ID of the job that was created to import file using the last POST /files/updateRepositories/firmware/import method

The following example import a firmware update or UpdateXpress System Pack (UXSP) to the updates repository.

```
GET https://192.0.2.0/files/updateRepositories/firmware/import?jobid=11
```

Request body

Use the "multipart/form-data" media type to import the update package. Use the attributes in the following table as the multipart name in the body. For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage. For example:

HTTP Header

```
Content-Type: multipart/form-data; boundary=AaB03x
```

Request body

```
--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]"; filename="fwfiles2018103122275762.zip"
   Content-Type: application/x-zip-compressed

--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]"; filename="fwfiles2018102523335745.zip"
   Content-Type: application/x-zip-compressed

--AaB03x--
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
current	String	
downloadedsize	Integer	
downloadednum	Integer	
progress	Integer	Job progress, where `100` is complete, and less than `100` is in progress
state	String	State of the import process. This can be one of the following values. • **success**. The request completed successfully. • **error**. The request failed. A descriptive error message is returned.
total	Integer	
totalsize	Integer	
updates	Array	
popMsg	Array	Indicates that some files are not applicable for virtual-appliance updates repository
result	String	Result of the request. This can be one of the following values. • **warning**
messages	Object	Information about one or more messages
id	String	Message identifier of a returned message
explanation	String	
recovery	Array	
text	String	
text	String	Message text that is associated with the message identifier
errorMsg	Array	Information about one or more messages
result	String	Result of the request. This can be one of the following values. • **informational**. The request completed successfully.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text that is associated with the message identifier

The following example is returned if the request is successful.

```
{
   "current": "",
   "downloadednum": 0
   "downloadedsize": 0,
   "progress": 0,
```

```
   "state": "success",
   "total": 0,
   "totalsize": 1,
   "updates": [],
   "popMsg": {
      "result": "warning",
      "messages": [{
         "id": "FQXHMUP2512F",
         "text": "Import complete",
         "explanation": "The following files are not applicable to the updates
                         process; they have been discarded: newFile.txt.",
         "recovery": {
            "text": "Discarded packages are not referenced by any .xml file
                     currently in Firmware Updates Repository. Ensure your
                     uploaded files include the correct .xml file."
         }
      }]
   },
   "errorMsg": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   },
}
```


/files/updateRepositories/firmware/import/validation

Use this REST API to check the file size before importing a firmware update or UpdateXpress System Pack (UXSP) in to the repository to ensure that there is enough file space to store them.

HTTP methods

POST

POST /files/updateRepositories/firmware/import/validate

Use this method to check the file size before importing a firmware update or UpdateXpress System Pack (UXSP) in to the repository to ensure that there is enough file space to store them and reserve part of file space for the import operation.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/files/updateRepositories/firmware/import/validate`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
file	Required	Array	
index	Optional	String	Array index
name	Required	String	File name
size	Required	Long	File size
type	Optional	String	File type. This can be one of the following values. • **text** • **binary**

The following example check the file size before importing.

```
{
   "files": [{
      "index": 0,
      "name": "filename.txt",
      "size": 8192,
      "type": "text/plain"
   }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
current	String	
downloadednum	Integer	
downloadedsize	Integer	
jobid	Integer	Job ID
progress	Integer	Job progress, where `100` is complete, and less than `100` is in progress
state	String	This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned.

Attributes	Type	Description
total	Integer	
totalsize	Integer	
updates	Array	
errorMsg	Array	Information about one or more messages
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned. • **informational**.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text that is associated with the message identifier

The following example is returned if the request is successful.


```
{
   "current": "",
   "downloadednum": 0,
   "downloadedsize": 0,
   "jobid": 96,
   "progress": 0,
   "state": "success",
   "total": 0,
   "totalsize": 0,
   "updates": [],
   "errorMsg": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```


/updateRepositories/firmware

Use this REST API to retrieve or modify information about firmware updates and UpdateXpress System Packs (UXSPs) in the firmware-updates repository

HTTP methods

GET, PUT

GET /updateRepositories/firmware

Use this method to return information about firmware in the firmware-updates repository or export firmware-update files to the local system.

To export firmware-update files, complete the following steps.

1. Export (collect) the firmware updates as a. zip file using the PUT /updateRepositories/firmware?action=export method. The response body returns the job (task) ID in the **taskid** parameter.
2. Ensure that the job for creating the .zip file completed and retrieve the name of the zip file using the GET /updateRepositories/firmware/status?tasktype=EXPORTREPOSITORY&taskid=*{job_id}* method, where

{job_id} is the job (task) ID that is returned in the previous step. The response body returns the name of the .zip file in the **current** parameter.

3. Download the zip file using the GET /updateRepositories/firmware?action=export&exportRepoFilename=<*file_name}* method, where *{file_name}* is the name of the ZIP file that is returned in the previous step.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/updateRepositories/firmware
```

Query parameters

Table 62. Export firmware update files

Parameters	Required / Optional	Description
key=export	Required	Downloads a ZIP file that contains the firmware-update and UXSP files to the local system. Use PUT /updateRepositories/firmware?action=export&filetype={type} to export (collect) the files as a. zip file that you can download using this method.
exportRepoFilename={name}	Required	Name of the .zip file To obtain the file name, use the GET /updateRepositories/firmware/status?tasktype=EXPORTREPOSITORY&taskid={job_id} method. The name of the ZIP file is returned by the **current** parameter in the response body.

The following example downloads a zip file of firmware updates to the local system.

```
GET https://192.0.2.0/updateRepositories/firmware?key=export
&exportRepoFilename=repository20181217142307.zip
```

Table 63. Return all information about firmware updates in the repository

Parameters	Required / Optional	Description
updates	Required	Returns all information about firmware updates that are in the repository

The following example returns all information about firmware updates.

```
GET https://192.0.2.0/updateRepositories/firmware?updates
```

Table 64. Return specific information about firmware updates in the repository

Parameters	Required / Optional	Description
key=*{key}*	Required	Returns specific information about firmware updates that are in the repository. This can be one of the following values. • **importDir**. Returns the import directory for the repository. • **importedUxsps**. Returns information about all UXSPs in the repository. • **isUpdating**. Returns the whether the firmware repository is being updated. • **lastRefreshed**. Returns the timestamp of the last repository refresh. • **publicKeys**. Returns the supported keys (actions) for this attribute. • **size**. Returns the repository size. • **supportedMts**. Returns a list of all device types for which the firmware-updates function is supported. • **updates**. Returns information about all firmware updates in the repository. • **updatesByMt**. Returns information about firmware updates organized by device type. • **updatesByMtByComp**. Returns the information about firmware updates, organized by device type and UXSP. • **updatesInUXSPByMt**. Returns the information about firmware updates, organized by device type and UXSP.
mt=*{type_list}*	Optional	Returns information for one or more specific device types, separated by a comma. **Note:** This attribute is applicable only when key is set to **updates**, **updatesByMt**, **updatesByMTByComp**, or **updatesInUXSPByMt**.
with=*{scope}*	Optional	Returns information about the firmware-update versions. This can be one of the following values. • **all**. (default) Returns information about all versions of firmware updates. • **latest**. Returns information about the most current version of firmware updates. **Note:** This attribute is applicable only when key is set to **updates**, **updatesByMt**, **updatesByMTByComp**, or **updatesInUXSPByMt**.
payload=*{boolean}*	Optional	Returns information about the firmware-updates. This can be one of the following values. • **true**. Returns information about only downloaded firmware updates. • **false**. (default) Returns information about all firmware updates. **Note:** This attribute is applicable only when key is set to **updates**, **updatesByMt**, **updatesByMTByComp**, or **updatesInUXSPByMt**.
managedOnly=*{boolean}*	Optional	Returns information about the device types. This can be one of the following values. • **true**. Returns a list of all managed device types. • **false**. (default) Returns a list of all device types for which the firmware-updates function is supported. **Note:** This attribute is applicable only when key is set to **supportedMts**.

The following example returns information about all UXSPs that are in the repository.

```
GET https://192.0.2.0/updateRepositories/firmware?key=importedUxsps
```

The following example returns a list of machine types that are supported by the firmware-update function.

```
GET https://192.0.2.0/updateRepositories/firmware?key=supportedMts
```

The following example returns information about the latest firmware updates in the repository.

```
GET https://192.0.2.0/updateRepositories/firmware?key=updates&with=latest
```

The following example returns information about the firmware updates for specific devices in USXPs in the repository.

```
GET https://192.0.2.0/updateRepositories/firmware?key=updaesInUXSPByMt&mt=7X21,7X15
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The following parameters are returned when the **updates** query parameter is specified.

A subset of parameters is returned when the **key** query parameter is specified. The object that is returned matches the key value that is specified. For example, if you specify **?key=size**, only the **size** parameter is returned.

Attributes	Type	Description
importDir	String	Import directory for the repository
importedUxsps	Array of objects	Information about UXSPs in the repository
category	String	Device category. This can be one of the following values. • **chassis** • **server** • **rackswitch** • **storage** • **switch**
displayType	String	Machine type that displays in the web interface
inventoryMT	String	Indicates whether devices with this machine type are currently managed by XClarity Administrator. This can be one of the following values. • **true** • **false**
name	String	Device name

Attributes	Type	Description
supportDownload	String	Indicate whether download from Lenovo XClarity Support website is supported. This can be one of the following values. • **true** • **false**
type	String	Device type
uxsp	Array of strings	List of UXSPs in the repository that are associated with the device type
isUpdating	String	Identifies whether the firmware repository is being updated. This can be one of the following values. • **true**. The firmware repository is being updated. The repository is locked until the update is complete. • **false**. The firmware repository is not being updated. Other actions can be performed on the repository.
lastRefreshed	String	Timestamp of the last catalog refresh operation.
publicKeys	Object	Public keys that are used in this repository for update packages
size	Object	Information about the size of the firmware-updates repository
allotment	Long	Amount of space that is available
freeSpace	Long	Amount of free space
firmwareRepoUsage	Long	Amount of used space, in bytes, in the firmware updates repository
highusage	String	Used capacity. This can be one of the following values. • **high**. 85% capacity or higher • **medium**. 50% capacity or higher • **low**. 49% or lower
selfRepoUsage	Long	Amount of used space, in bytes, in the updates repository
upperLimitSpace	Long	Maximum amount of space, in GB, that can be allocated to the updates repository (including firmware, OS device drivers, and management server updates) The minimum size is 50 GB. The maximum size is dependent on the amount of disk space on the local system.
usedSpace	Long	Amount of used space
windowsDriverRepoUsage	Long	Amount of used space, in bytes, in the Windows device-drivers repository
supportedMts	Object	Information about each device type for which the firmware-updates function is supported
category	String	Device category. This can be one of the following values. • **chassis** • **server** • **rackswitch** • **storage** • **switch**
comp	Array of strings	List of components that are associated with the firmware update (for example, XCC, UEFI, and LXPM)
displayType	String	Device type that displayed in the web interface

Attributes	Type	Description
inventoryMT	Boolean	Indicates whether devices with this machine type are currently managed by XClarity Administrator. This can be one of the following values. • **true** • **false**
name	String	Device name
supportDownload	String	Indicate whether the firmware update can be downloaded from the Lenovo XClarity Support website. This can be one of the following values. • **true** • **false**
type	String	Device type
uxsp	Array of strings	List of UXSPs in the repository that are associated with the device type
updates	Array of objects	Information about the updates.
applyable	String	Indicates whether the update can be applied. This can be one of the following values. • **true** • **false**
buildNumber	String	The update build number, if applicable and available.
buildType	String	Specifies that this update is a GA-level update
change	String	Indicates whether the change log file exists in the repository for this firmware update. This can be one of the following values. • **true** • **false**
comp	Array of strings	List of components that are associated with the firmware update (for example, XCC, UEFI, and LXPM)
downloadedsize	Integer	Size of the firmware-update file that is currently downloaded. After the download is complete, the download size is the same as the total size.
errorMsg	String	Not used
fixid	String	Firmware update UUID
latest	String	Indicates whether the firmware update is the latest version. This can be one of the following values. • **true**. This is the latest version. • **false**. This is not the latest version.
name	String	Not used
OperatingSystemList	Array of strings	List of operating systems that are associated with the firmware update
origin	String	Firmware update file name
payload	String	Indicates whether the payload file exists in the repository for this firmware update. This can be one of the following values. • **true**. The payload file is downloaded. • **false**. The payload file is not downloaded.
payloadFilename	String	Name of the payload file

Attributes	Type	Description
percentage	Integer	Percentage of the firmware update that is downloaded. If the download is complete, the value is set to **100**.
prereq	Array of strings	List of IDs of prerequisite firmware updates
readableName	String	Name of the readme file
readme	String	Indicates whether the readme file exists in the repository for this firmware update. This can be one of the following values. • **true**. The readme file is downloaded. • **false**. The readme file is not downloaded.
rebootRequired	String	Indicates whether the device must be rebooted after installing this firmware update. This can be one of the following values. • **true**. The update requires a reboot. • **false**. The update does not require a reboot.
releasedate	String	Update release date
releasedinterval	Integer	Number of months since the firmware update was released
severity	Integer	Update severity. This can be one of the following values. • **0**. Initial release of the update. • **1**. Critical update release. • **2**. Suggested update release. • **3**. Noncritical update release.
state	String	Not used
supportDownload	String	Indicate whether download from Lenovo XClarity Support website is supported. • **true** • **false**
totalsize	Integer	Total size of the update
uxsp	Array of strings	ID of the UXSP in the repository that is associated with the firmware update
version	String	Update version
updatesByMt	Object	Information about updates by device type
current	String	Not used
downloadednum	Integer	Number of updates that are downloaded
downloadedsize	Integer	Size of downloaded updates
jobid	Integer	Job ID that currently is running
progress	Double	Job progress. This can be one of the following values. • **0**. Created • **50**. Incomplete • **100**. Done
state	String	Job status. This can be one of the following values. • **complete**
total	Integer	Total number of updates
totalsize	Integer	Total size of updates
updates	Array of objects	Information about the firmware update

Attributes	Type	Description
inventoryMT	String	Indicates whether devices with this machine type are currently managed by XClarity Administrator. This can be one of the following values. • **true** • **false**
mt	String	Machine type
updates	Array of objects	Information about each firmware update
updatesByMtByComp	Object	Update information organized by machine type and component name
parameter		
value		
comp		
category		
displayType		
inventoryMT		Indicates whether devices with this machine type are currently managed by XClarity Administrator. This can be one of the following values. • **true** • **false**
name	String	
supportDownload		
type	String	
uxsp		
updatesInUXSPByMt	Object	Information about firmware updates, organized by device type and UXSP
current	Integer	
downloadednum	Integer	
downloadedsize	Integer	
jobid	Integer	
progress	Integer	
state	Integer	
total	Integer	
totalsize	Integer	
updates	Array of objects	
status	Object	Information about one or more messages
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about each message

Attributes	Type	Description
id	String	Message ID
text	String	Message text associated with the ID

The following example returns the import directory for the repository (**?key=importDir**).).

```
{
   "importDir": "\/opt\/lenovo\/lxca\/data\/updates\/repository",
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```

The following example returns information about all UXSPs that are in the repository (**?key=importedUxsps**).

```
{
   "importedUxsps": [{
      "category": "server",
      "displayType": "4259",
      "inventoryMT": "false",
      "name": "IBM Flex System x280\/x480\/x880 X6 Compute Node",
      "supportDownload": "true",
      "type": "4259",
      "uxsp": "[ibm_utl_uxsp_n2ib06p-2.30_sles_32-64, ibm_utl_uxsp_n2ib03p-2.50_sles11_32-64]"
   },
   {
      "category": "server",
      "displayType": "8738",
      "inventoryMT": "false",
      "name": "IBM Flex System x240 Compute Node",
      "supportDownload": "true",
      "type": "8738",
      "uxsp": "[ibm_utl_uxsp_b2ib04p-2.50_sles11_32-64, ibm_utl_uxsp_b2ib05p-2.30_sles_32-64]"
   },
   ...,
   {
      "category": "server",
      "displayType": "7X99",
      "inventoryMT": "false",
      "name": "Lenovo ThinkSystem SR590 Server",
      "supportDownload": "true",
      "type": "7X99",
      "uxsp": "[]"
   }],
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```

The following examples returns information about whether the firmware repository is being updated (**?key=isUpdating**).

```
{
```

```
   "isUpdating": "false"
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   },
}
```


The following example returns the timestamp when repository was refresh last (**?key=lastRefreshed**).


```
{
   "lastRefreshed": "2018-10-31T15:26:52Z",
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```


The following examples returns information about the size of the firmware-updates repository (**?key=size**).


```
{
   "size": {
      "allotment": 53687091200,
      "firmwareRepoUsage": 34685248291,
      "freeSpace": 11407376384,
      "highusage": "high",
      "selfRepoUsage": 97299561694,
      "upperLimitSpace": 158230491136,
      "usedSpace": 133804243686,
      "windowsDriverRepoUsage": 1819433701
   },
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```


The following examples returns a list of machine types that are supported by the firmware-update function (**?key=supportedMts**).


```
{
   "supportedMts": [{
      "category": "server",
      "comp": "[Emulex HBA (LPe1600x) Firmware Update for Linux, Online Qlogic NetXtreme II Firmware
      Utility, IBM Online SAS\/SATA Hard Disk Drive Update Program - contains Lenovo Drives, Emulex
      OCe14xxx UCNA Firmware Update for Linux, Diagnostics, Online Broadcom NetXtreme I Linux Firmware
      Utility, Firmware Update for ServeRAID M5115 PSoC3, IBM Flex System FC3172 2-port 8Gb FC
      Multiboot Update Package, IMM2, ServeRAID 6GB SAS\/SATA Controller Firmware Update, IBM Online
      SAS\/SATA Hard Disk Drive Update Program For Legacy, Mellanox Firmware Update, UEFI, ServeRAID
      M1210e SAS\/SATA Controller Firmware Update, Emulex OCe11xxx UCNA Firmware Update for Linux,
      QLogic BR series BootCode Update for 16G FC 10G CNA and 4\/8G FC HBA, IBM Flex System FC5172
      2-port 16Gb FC Multiboot Update Package, Emulex HBA (LPe1205\/LPe1200x) Firmware Update for
      Linux]",
      "displayType": "7903",
      "inventoryMT": "true",
```

```
      "name": "IBM Flex System x280\/x480\/x880 X6 Compute Node",
      "supportDownload": "true",
      "type": "7903",
      "uxsp": "[ibm_utl_uxsp_n2ib06p-2.30_sles_32-64, ibm_utl_uxsp_n2ib03p-2.50_sles11_32-64]"
   },
   {
      "category": "server",
      "comp": "[Online Qlogic NetXtreme II Firmware Utility, Emulex HBA (LPe1600x) Firmware Update for
      Linux, LSI 2004 SAS Controller BIOS and Firmware Update for IBM Flex x440 Compute Node, IBM Online
      SAS\/SATA Hard Disk Drive Update Program - contains Lenovo Drives, Emulex OCe14xxx UCNA Firmware
      Update for Linux, Diagnostics, Online Broadcom NetXtreme I Linux Firmware Utility, Firmware Update
      for ServeRAID M5115 PSoC3, IBM Flex System FC3172 2-port 8Gb FC Multiboot Update Package, IMM2,
      ServeRAID 6GB SAS\/SATA Controller Firmware Update, IBM Online SAS\/SATA Hard Disk Drive Update
      Program For Legacy, Mellanox Firmware Update, UEFI, QLogic BR series BootCode Update for 16G FC
      10G CNA and 4\/8G FC HBA, Emulex OCe11xxx UCNA Firmware Update for Linux, IBM Flex System FC5172
      2-port 16Gb FC Multiboot Update Package, Emulex HBA (LPe1205\/LPe1200x) Firmware Update for Linux]",
      "displayType": "7917",
      "inventoryMT": "true",
      "name": "IBM Flex System x440 Compute Node",
      "supportDownload": "true",
      "type": "7917",
      "uxsp": "[ibm_utl_uxsp_cnib06p-3.20_sles_32-64, ibm_utl_uxsp_cnib03p-3.30_sles_32-64]"
   },
   ...,
   {
      "category": "server",
      "comp": "[BIOS and Firmware Update for ThinkSystem 430-x SAS\/SATA 12Gb HBA(06.02.00.02), Broadcom NX-1
               Ethernet Firmware Update for Linux, Emulex OCe14xxx UCNA Firmware Update for Linux, Intel
             v23.2 Network FW Update Release for Linux, QLogic FastLinQ Ethernet Adapter Firmware Update
             for Linux, ThinkSystem RAID 530-x Adapters update BIOS and Firmware for windows and linux,
             Firmware Update for ThinkSystem 1610-4P NVMe Switch Card, LXPM, Emulex HBA (LPe3100x) Firmware
             Update for Linux, DRVLN, ThinkSystem RAID 930-x xGB Flash PCIe 12Gb Adapters2Gb Adapters update
             BIOS and Firmware for windows and linux, ThinkSystem 810-4p NVMe Switch Card Firmware, Lenovo
             Online SAS\/SATA Hard Disk Drive Update Program, UEFI, QLogic Fibre Channel HBA Firmware Update
             for ThinkSystem, XCC, DRVWN, Emulex HBA (LPe1205\/LPe1200x) Firmware Update for Linux, Broadcom
             NX-E Ethernet Firmware Update for Linux, ThinkSystem RAID 730-8i XGB Cache\/Flash PCIe 12Gb
             Adapter Update BIOS and Firmware, ThinkSystem M.2 with Mirroring Enablement Kit Firmware Update
             For Anyos]",
      "displayType": "7X99",
      "inventoryMT": "false",
      "name": "Lenovo ThinkSystem SR590 Server",
      "supportDownload": "true",
      "type": "7X99",
      "uxsp": "[]"
   }],
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```


The following example returns information about the latest firmware updates in the repository (for example, **?key=updates&with=latest**).


```
{
   "updates": [{
      "applyable": "true",
      "buildNumber": "1AON20A",
      "buildType": "production",
```

```
    "change": "true",
    "comp": "CMM",
    "downloadedsize": 0,
    "errorMsg": "",
    "fixid": "lnvgy_fw_cmm_1aon20a-1.8.0_anyos_noarch",
    "latest": "false",
    "name": "",
    "OperatingSystemList": [],
    "origin": null,
    "payload": "false",
    "payloadFilename": "",
    "percentage": 0,
    "prereq": ["lnvgy_fw_cmm_1aon16b-1.6.1_anyos_noarch"],
    "readableName": "Lenovo Chassis Management Module 2 [CMM2] Firmware  1.8.0  [1AON20A]
                    18A GA",
    "readme": "true",
    "rebootRequired": "true",
    "releasedate": "2018-06-05",
    "releasedinterval": 5,
    "severity": 2,
    "state": "",
    "supportDownload": "true",
    "totalsize": 80617000,
    "uxsp": [],
    "version": "1.8.0"
},
...,
{
    "applyable": "true",
    "buildNumber": "",
    "buildType": "production",
    "change": "true",
    "comp": "Broadcom NX-E Ethernet Firmware Update for Linux",
    "downloadedsize": 0,
    "errorMsg": "",
    "fixid": "brcm-lnvgy_fw_nic_nxe-20.06.04.02a_linux_x86-64",
    "latest": "true",
    "name": "",
    "OperatingSystemList": [],
    "origin": null,
    "payload": "false",
    "payloadFilename": "",
    "percentage": 0,
    "prereq": [],
    "readableName": "Broadcom NetXtreme-E Ethernet Adapter Firmware Utility for Linux",
    "readme": "true",
    "rebootRequired": "true",
    "releasedate": "2017-08-04",
    "releasedinterval": 15,
    "severity": 0,
    "state": "",
    "supportDownload": "true",
    "totalsize": 5571000,
    "uxsp": [],
    "version": "nxe-20.06.04.02a"
}],
"status": {
    "result": "informational",
    "messages": [{
       "id": "FQXHMUP2500I",
       "text": "Repository operation completed successfully."
```

```
      }]
   }
}
```

The following examples returns information about firmware updates, organized by device type (**?key=updatesByMt**).


```
{
   "updatesByMt": {
      "current": "",
      "downloadednum": 0,
      "downloadedsize": 1,
      "jobid": -1,
      "progress": 100,
      "state": "complete",
      "total": 0,
      "totalsize": 1,
      "updates": [{
         "inventoryMT": "true",
         "mt": "7917",
         "updates": [{
            "applyable": "true",
            "buildNumber": "",
            "buildType": "production",
            "change": "true",
            "comp": "Emulex OCe14xxx UCNA Firmware Update for Linux",
            "downloadedsize": 0,
            "errorMsg": "",
            "fixid": "elx_fw_cna_15a-oc14-10.3.148.0-1_linux_32-64",
            "latest": "true",
            "name": "",
            "OperatingSystemList": [],
            "origin": null,
            "payloadFilename": "",
            "percentage": 0,
            "prereq": [],
            "payload": "false",
            "readableName": "Emulex OCe14xxx UCNA Firmware Update for Linux",
            "readme": "true",
            "rebootRequired": "true",
            "releasedate": "2016-11-22",
            "releasedinterval": 23,
            "severity": 0,
            "state": "",
            "supportDownload": "true",
            "totalsize": 20640000,
            "uxsp": [],
            "version": "oc14-10.3.148.0-1"
         },
         ...,
         {
            "applyable": "true",
            "buildNumber": "1.20.02",
            "buildType": "production",
            "change": "true",
            "comp": "LSI 2004 SAS Controller BIOS and Firmware Update for IBM Flex x440 Compute Node",
            "downloadedsize": 0,
            "errorMsg": "",
            "fixid": "ibm_fw_mpt2sas_x440-1.20.02_linux_32-64",
            "latest": "true",
            "name": "",
            "OperatingSystemList": [],
```

```
            "origin": null,
            "payload": "false",
            "payloadFilename": "",
            "percentage": 0,
            "prereq": [],
            "readableName": "LSI 2004 SAS Controller BIOS and Firmware Update for IBM Flex x440 Compute Node",
            "readme": "true",
            "rebootRequired": "true",
            "releasedate": "2015-12-03",
            "releasedinterval": 35,
            "state": "",
            "severity": 2,
            "supportDownload": "true",
            "totalsize": 1436000,
            "uxsp": [],
            "version": "1.20.02",
         }]
      }]
   },
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```


The following example returns information about firmware updates, organized by component and device type (for example, **?updatesByMtByComp**).


```
{
   "updatesByMtByComp": {
      "parameter": "MTS",
      "value": [{
         "comp": "[Emulex HBA (LPe1600x) Firmware Update for Linux, Emulex OCe14xxx UCNA
                  Firmware Update for Linux, Lenovo Online SAS\/SATA Hard Disk Drive Update
                  Program, Intel v22.9 Network FW Update Release for Linux, Diagnostics, Online
                  Broadcom NetXtreme I Linux Firmware Utility, BIOS and Firmware Update for ServeRAID
                  M5200 Series SAS\/SATA Controllers, IMM2, Emulex HBA (LPe1205\/LPe1200x) Firmware
                  Update for Linux, BIOS and Firmware Update for ServeRAID M1200 Series SAS\/SATA
                  Controllers(24.21.0-0016), Emulex HBA (LPe3100x) Firmware Update for Linux]",
         "category": "server",
         "displayType": "3633",
         "inventoryMT": "false",
         "name": "Lenovo System x3250 M6",
         "supportDownload": "true",
         "type": "3633",
         "uxsp": "[]",
      },
      {
         "category": "server",
         "comp": "[Online Qlogic NetXtreme II Firmware Utility, Emulex HBA (LPe1600x)
                  Firmware Update for Linux, Emulex OCe14xxx UCNA Firmware Update for Linux,
                  Diagnostics, Online Broadcom NetXtreme I Linux Firmware Utility, BIOS and
                  Firmware Update for ServeRAID M5200 Series SAS\/SATA Controllers, IMM2,
                  Emulex HBA (LPe3100x) Firmware Update for Linux, Mellanox Firmware Update
                  (17B), Lenovo Online SAS\/SATA Hard Disk Drive Update Program, Intel v22.9
                  Network FW Update Release for Linux,QLogic Fibre Channel HBA Firmware Update
                  for ThinkSystem, Emulex OCe11xxx UCNA Firmware Update for Linux, Emulex HBA
                  (LPe1205\/LPe1200x) Firmware Update for Linux,BIOS and Firmware Update for
                  ServeRAID M1200 Series SAS\/SATA Controllers(24.21.0-0016), ServeRAID 6gb
```

```
                    SAS\/SATA Controller Firmware Update]",
         "displayType": "6241",
         "inventoryMT": "false",
         "name": "Lenovo System x3850 \/ x3950 X6",
         "supportDownload": "true",
         "type": "6241",
         "uxsp": "[]",
      }]
   },
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```


The following example returns information about firmware updates, organized by device type and UXSP (**?key=updatesInUXSPByMt**).


```
{
   "updatesInUXSPByMt": {
      "current": "",
      "downloadednum": 0,
      "downloadedsize": 1,
      "jobid": -1,
      "progress": 100,
      "state": "complete",
      "total": 0,
      "totalsize": 1,
      "updates": [{
         "inventoryMT": "false",
         "mt": "3633",
         "updates": [{
            "applyable": "true",
            "buildNumber": "SAS-1.27.08",
            "buildType": "production",
            "change": "true",
            "comp": "Lenovo Online SAS\/SATA Hard Disk Drive Update Program",
            "downloadedsize": 220516907,
            "errorMsg": "",
            "fixid": "lnvgy_fw_hdd_sas-1.27.08_linux_x86-64",
            "latest": "true",
            "name": "",
            "OperatingSystemList": [],
            "origin": null,
            "payload": "true",
            "payloadFilename": "lnvgy_fw_hdd_sas-1.27.08_linux_x86-64.bin",
            "percentage": 100,
            "prereq": [],
            "readableName": "Lenovo Online SAS\/SATA Hard Disk Drive Update Program",
            "readme": "true",
            "rebootRequired": "false",
            "releasedate": "2018-10-09",
            "releasedinterval": 1,
            "severity": 2,
            "state": "",
            "supportDownload": "true",
            "totalsize": 220516907,
            "uxsp": [],
            "version": "sas-1.27.08"
```

```
         },
         ...,
         ]
      ...,
      }]
   },
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```

PUT /updateRepositories/firmware

Use this method to modify information about firmware updates in the updates repository.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/updateRepositories/firmware`

Query parameters

Parameters	Required / Optional	Description
action=*{action}*	Required	Action to take. This can be one of the following values. • **read**. Reloads the repository files. The clears the update information in cache and reads the update file again from the repository. • **refresh**. Retrieves information about firmware updates from the Lenovo XClarity Support website, and stores the information to the updates repository. You must specify the **mt**, **os**, and **type** request attributes. • **refreshThenAcquire**. Retrieves information about latest available firmware updates from the Lenovo XClarity Support website, stores the information to the updates repository, and downloads the updates that are not already downloaded. **Important:** You must specify the **mt** and **os** request attributes. • **acquire**. Downloads the specified firmware updates from Lenovo XClarity Support website, and stores the updates to the updates repository. You must specify the **fixids**, **mt**, and **type** request attributes. • **delete**. Deletes the specified firmware updates from the updates repository. You must specify the **fixids** request attribute. • **export**. Compresses the specified firmware updates from the updates repository into a ZIP file, and downloads the ZIP file to your local system. A job is created to export files into the .zip file. Use the GET /updateRepositories/firmware/status?taskid=*{task_id}* method (where *{task_id}* is the subtask ID) to retrieve the subtask status and file name, or use GET /tasks/*{job_id}* (where *{job_id}* is the job ID) to retrieve the overall job status. If a job was not successfully started, refer to the response code and response body for details.
filetypes=*{type}*	Optional	When **action=delete** is specified, this query parameter is used. You can specify one of the following values. • **all**. Deletes selected update-package files (payload, change history, readme, and metadata files) • **payloads**. Deletes only the selected payload (image) files
with=*{scope}*	Optional	Scope of the action. This can be one of the following values. • **all**. (default) – When **action=refresh** query parameter is specified, this query parameter returns information about all versions of all firmware updates that are available for all supported devices. – When **action= refreshThenAcquire** query parameter is specified, this query parameter retrieves information about all versions of all firmware updates for the specified machine types, then downloads the firmware updates that are not already downloaded – When **action=export** query parameter is specified, it compresses all firmware updates into a .zip file • **latest**. – When **action=refresh** query parameter is specified, this query parameter returns information about the most current version of all firmware updates for all supported devices. – When **action= refreshThenAcquire** query parameter is specified, this query parameter retrieves information about the most current version of all firmware updates for the specified

Parameters	Re-quired / Optional	Description
		machine types, then downloads the updates that are not already downloaded. – When **action=export** query parameter is specified, it compresses latest firmware based on list of machine types into ZIP file. You must specify the **mt** request attribute • **payloads**. – When **action=acquire** query parameter is specified, this query parameter returns information about specific firmware updates. – When **action=export** query parameter is specified, it compresses firmware updates based on list of fix IDs into ZIP file. You must specify the **fixids** request attribute.

The following example retrieves information about the latest available firmware updates and downloads the updates that are not already downloaded.

```
PUT https://192.0.2.0/updateRepositories/firmware?action=refreshThenAcquire&with=latest
```

The following example downloads information about the latest version of each firmware update.

```
PUT https://192.0.2.0/updateRepositories/firmware?action=refresh&with=latest
```

The following example downloads the specified firmware-update files.

```
PUT https://192.0.2.0/updateRepositories/firmware?action=acquire&with=payload
```

The following example deletes the payload (image files) from the updates repository for the specified firmware update.

```
PUT https://192.0.2.0/updateRepositories/firmware?action=delete&filetypes=payloads
```

The following example deletes the payload (image), change history, readme, and metadata files from the updates repository for the specified firmware update.

```
PUT https://192.0.2.0/updateRepositories/firmware?action=delete&filetypes=all
```

Request body

Attributes	Required / Optional	Type	Description
fixids	Required if **action** is “acquire”, “export”, or “delete”	Array of strings	List of firmware-update IDs to be downloaded or deleted
mt	Required if **action** is “refresh”, “refreshThe-nAcquire”, or “acquire”	Array of strings	List of machine types for which firmware updates are to be refreshed or downloaded.
os	Required if **action** is “refresh” or “refresh”,	String	Operating system to be refreshed. For firmware updates, this value must be empty (for example, `"os":""`).
type	Required if **action** is “refresh” or “acquire”	String	If **action=refresh**, this value must be “catalog.” If **action=acquire**, set this value to “latest.”

The following example retrieves information about and downloads the latest available firmware updates that are applicable to ThinkSystem SR530 servers when `?action=refreshThenAcquire&with=latest` is specified.

```
{
   "mt": ["7X07,7X08"],
   "os": "",
}
```

The following examples retrieves information about the latest available firmware updates for ThinkSystem SR530 servers when `?action=refresh&with=latest` is specified.

```
{
   "mt": ["7X07,7X08"],
   "os": "",
   "type": "catalog"
}
```

The following examples downloads the latest firmware updates for specific fixes when `?action=acquire&with=payloads` is specified.

```
{
   "fixids": [
      "brcd_fw_bcsw_nos5.0.1_anyos_noarch",
      "brcd_fw_cna_3.2.4.0_linux_32-64",
      "brcd_fw_cna_3.2.3.0_linux_32-64",
      "lenovo_fw_dsa_dsyte2f-9.61_anyos_32-64"
   ],
   "mt": ["0000"],
   "type": "latest"
}
```

The following examples deletes a specific firmware-update package when `?action=delete` is specified.

```
{
   "fixids":["nvgy_utl_lxce_ux01h_2.3.0_windows_i386"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

A subset of the following attributes are returned, depending on the specified query parameters.

Attributes	Type	Description
jobid	String	Job ID
taskid	String	Subtask ID

Attributes	Type	Description
tasktype	String	Action that was performed. This can be one of the following values. • **EXPORTREPOSITORY**. The type of export action. • **ACQUIRECATALOG**. The type of refresh action. • **ACQUIREPAYLOAD**. The type of acquire action. • **DELETEPAYLOAD**. The type of delete action.
status	String	This can be one of the following values when the **action** query parameter is “export.”. • **success**. The request completed successfully. Started to compress repository successfully. • **error**. The request failed. A descriptive error message is returned.
result	String	This can be one of the following values when the **action** query parameter is “read,” “refresh,” “acquire.” • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message is returned.
errorMsg	Array of objects	Information about one or more messages
messages	Array of objects	Information about a specific message
id	String	Message identifier of a returned message
text	String	Message identifier of a returned message
result	String	The results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned. • **informational**

The following example returns the job and task ID of read action when **?action=read** is specified.

```
{
   "jobid": "515",
   "taskid": "14",
   "result": "success",
   "errorMsg": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2508I",
         "text": "The repository operation has started successfully."
      }]
   }
}
```

The following example returns the task of export action and job ID when **?action=export** is specified.

```
{
   "tasktype": "EXPORTREPOSITORY",
   "taskid": "11",
   "status": "success",
   "errorMsg": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```

/updateRepositories/firmware/status

Use this REST API to retrieve the status for a repository task.

HTTP methods

GET

GET /updateRepositories/firmware/status

Use this method to return the status for a repository task.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/updateRepositories/firmware/status`

Query parameters

Parameters	Required / Optional	Description
taskType=EXPORTREPOSITORY	Required	Type of repository task for which to retrieve status. This can be the following value. • **EXPORTREPOSITORY**. Returns status for an export task.
taskid=*{task_id}*	Required	Job (task) ID that is returned by the PUT /updateRepositories/firmware?action=export method for collecting (exporting) firmware updates and UpdateXpress System Packs (UXSPs) in a .zip file. If `0` is specified, the status for all running tasks is returned.

The following example returns the status for a specific export job.

```
GET https://192.0.2.0/updateRepositories/firmware/status?tasktype=EXPORTREPOSITORY&taskid=12
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
current	String	Name of the ZIP file
downloadednum	Integer	Number of firmware-update and UXSPs that is currently exported After the export is complete, the download number is the same as the total.
downloadedsize	Integer	Size of the .zip file that is currently exported After the export is complete, the download size is the same as the total size.
progress	Integer	Percentage complete of the bulk management job. This can be one of the following values • **0**. Created. • **50**. In progress. • **100.** Complete.
state	String	This can be one of the following values. • **canceled**. The request was canceled. • **complete**. The request completed successfully. • **error**. The request encountered an error.
taskIds	String	ID of the task that collected the files.
total	Integer	Total number of firmware-update and UXSPs in the .zip file
totalsize	Integer	Total size of the .zip file
updates	Array	
errorMsg	Array	Information about one or more messages.
messages	Array	Message.
id	String	The message identifier of a returned message.
text	String	Message text associated with the message identifier.
result	String	The results of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned. • **informational**

The following example is returned if the request is successful.

```
{
   "current": "repository20181112011742.zip",
   "downloadednum": 0,
   "downloadedsize": 8298,
   "progress": 100,
   "state": "complete",
   "taskIds": "",
   "total": 0,
   "totalsize": 8298,
   "updates": [],
   "errorMsg": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```

/updateRepositories/firmware/uxsps

Use this REST API to retrieve information about and modify all UpdateXpress System Packs (UXSPs) in the repository (for firmware updates and OS device drivers.

HTTP methods

GET, PUT

GET /updateRepositories/firmware/uxsps

Use this method to return information about all UpdateXpress System Packs (UXSPs) in the repository (for firmware updates and OS device drivers.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/updateRepositories/firmware/uxsps
```

Query parameters

Table 65. Export UXSP files

Parameters	Required / Optional	Description
key=export	Required	Downloads a ZIP file that contains the UXSP files to the local system. You must specify **filetypes** query parameter. Use PUT /updateRepositories/firmware/uxsp?action=export&filetype=<*type}* to export (collect) the files as a. zip file that you can download using this method.
exportRepoFilename=*{name}*	Required	Name of the .zip file To obtain the file name, use the GET /updateRepositories/firmware/status?tasktype=EXPORTREPOSITORY&taskid=*{job_id}* method. The name of the ZIP file is returned by the **current** parameter in the response body.

The following example downloads a zip file of UXSPs to the local system.

```
GET https://192.0.2.0/updateRepositories/firmware/uxsps?key=export
&exportRepoFilename=repository20181217142307.zip
```

Table 66. Return specific information about UXSPs in the repository

Parameters	Re-quired / Optional	Description
key=*{key}*	Required	Action to take. This can be one of the following values. • **uxsps**. Returns the UXSPs for specified device types if the UXSP is available in firmware repository. • **uxspsByMt**. Returns information about UXSP for the specified device types.
mt=*{type_list}*	Optional	Returns information for one or more specific device types, separated by a comma. If not specified, information about all device types is returned.
with=*{scope}*	Optional	UXSP versions. This can be one of the following values. • **all**. (default) Returns information about all versions of UXSPs. • **latest**. Returns information about the most current version of UXSP.

The following example returns information about the most current UXSPs by device type.

```
PUT https://192.0.2.0/updateRepositories/firmware/uxsps?key=uxsps&with=latest
```

The following example returns information about UXSPs for specific devices.

```
PUT https://192.0.2.0/updateRepositories/firmware/uxsps?key=uxspsByMt&mt=7X21,7X15
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

A subset of the following Attributes are displayed, depending on the specified query parameters.

Attributes	Type	Description
uxsps	Object	Information about the UXSPs
uxspsByMt	Object	Information about UXSPs by device type

Attributes	Type	Description
current	String	Not used
downloadednum	Integer	Not used
downloadedsize	Integer	Not used
progress	Double	This can be one of the following values. • **0**. Created • **50**. Incomplete • **100**. Done
state	String	This can be one of the following values. • **complete**
totalsize	Integer	Not used
uxsps	Array of objects	Information about the UXSPs
mt	String	Machine type.
updates	Array of objects	Information about each update in the UXSP
applyable	Boolean	• **true** • **false**
buildNumber	String	Update build number, if applicable and available
buildType	String	Specifies that this update is a GA-level update
change	Boolean	• **true** • **false**
comp	String	Update component name
child	Array of strings	Updates fix IDs that belongs to this UXSP
errorMsg	String	Not used
fixid	String	Update UUID
origin	String	Origin file name
latest	Boolean	• **true** • **false**
name	String	Not used
payload	Boolean	This can be one of the following values. • **true** • **false**
payloadFilename	String	Name of the update payload
percentage	Integer	Percentage of the update that is downloaded. If the download is complete, the value is set to **100**.
readableName	String	Name of the README file
readme	Boolean	This can be one of the following values. • **true** • **false**
rebootRequired	Boolean	This can be one of the following values. • **true** • **false**

Attributes	Type	Description
releasedate	String	Update release date
releasedinterval	Integer	Number of months since the firmware update was released
severity	Integer	Update severity. This can be one of the following values. • **0**. Initial release of the update. • **1**. Critical update release. • **2**. Suggested update release. • **3**. Noncritical update release.
supportDownload	String	Indicate whether download from Lenovo XClarity Support website is supported. • **true** • **false**
state	String	Not used
totalsize	Integer	Total size of the update
version	String	Version of the update
downloadedsize	Integer	Size of the downloaded update. After the download is complete, this will be the same as totalsize.

The following examples returns firmware-update information for the supported machine types (for example, ?key=uxspsByMt&with=all&payload=&mt=7X21,7X15).


```
{
   "uxspsByMt": {
      "current": "",
      "downloadednum": 0
      "downloadedsize": 1,
      "progress": 100,
      "state": "complete",
      "total": 0,
      "totalsize": 1,
      "uxsps": [{
         "mt": "7X25",
         "updates": [{
            "applyable": "false",
            "buildNumber": "0709",
            "buildType": "production",
            "change": "true",
            "comp": "",
            "child": ["lnvgy_fw_hdd_sas-1.26.05_linux_x86-64",
                      "brcm-lnvgy_fw_cna_18b-oc14-12.0.1141.7-1_linux_x86-64",
                      "elx-lnvgy_fw_fc_18a-lp3x-11.4.329.13-6_linux_x86-64",
                      "qlgc-lnvgy_fw_nic_ah-8.35.04-4_linux_x86-64",
                      "lnvgy_fw_mpt35sas_430-06.01.00.07_linux_x86-64",
                      "brcm-lnvgy_fw_nic_nxe-212.0.112.0-a_linux_x86-64",
                      "intc-lnvgy_fw_nic_6.01-3.3d-1.1892.0-b_linux_x86-64",
                      "mlnx-lnvgy_fw_nic_4.3-1.0.1.0.3_linux_x86-64",
                      "lnvgy_fw_m2raid_2.3.10.1095_anyos_noarch",
                      "elx-lnvgy_fw_fc_18a-2.10x6-8_linux_x86-64",
                      "qlgc-lnvgy_fw_fc_1.90.48-2690-2742.e_linux_x86-64",
                      "lnvgy_fw_xcc_tei326q-1.80_anyos_noarch",
                      "lnvgy_fw_uefi_tee124n-1.40_anyos_32-64",
                      "lnvgy_fw_lxpm_pdl114n-1.30_anyos_noarch"],
            "downloadedsize": 37374651,
            "errorMsg": "",
            "fixid": "lnvgy_utl_uxsp_tesp05p-2.50_platform_32-64",
            "latest": "true",
```

```
      "name": "",
      "origin": null,
      "payload": "true",
      "payloadFilename": "lnvgy_utl_uxsp_tesp05p-2.50_platform_32-64.zip",
      "percentage": 100,
      "readableName": "Lenovo UpdateXpress System Pack",
      "readme": "true",
      "rebootRequired": "true",
      "releasedate": "2018-11-18",
      "releasedinterval": 9,
      "severity": 2,
      "state": "",
      "supportDownload": "true",
      "totalsize": 37374651,
      "version": "2.50"
   }]
},
{
   "mt": "7917"
   "updates": [{
      "applyable": "true",
      "buildType": "production",
      "buildNumber": "",
      "change": "true",
      "comp": "",
   "child": ["lnvgy_fw_hdd_sas-1.26.05_linux_x86-64",
             "brcm-lnvgy_fw_cna_18b-oc14-12.0.1141.7-1_linux_x86-64",
             "elx-lnvgy_fw_fc_18a-lp3x-11.4.329.13-6_linux_x86-64",
             "qlgc-lnvgy_fw_nic_ah-8.35.04-4_linux_x86-64",
             "lnvgy_fw_mpt35sas_430-06.01.00.07_linux_x86-64",
             "brcm-lnvgy_fw_nic_nxe-212.0.112.0-a_linux_x86-64",
             "intc-lnvgy_fw_nic_6.01-3.3d-1.1892.0-b_linux_x86-64",
             "mlnx-lnvgy_fw_nic_4.3-1.0.1.0.3_linux_x86-64",
             "lnvgy_fw_m2raid_2.3.10.1095_anyos_noarch",
             "elx-lnvgy_fw_fc_18a-2.10x6-8_linux_x86-64",
             "qlgc-lnvgy_fw_fc_1.90.48-2690-2742.e_linux_x86-64",
             "lnvgy_fw_xcc_tei326q-1.80_anyos_noarch",
             "lnvgy_fw_uefi_tee124n-1.40_anyos_32-64",
             "lnvgy_fw_lxpm_pdl114n-1.30_anyos_noarch"],
      "downloadedsize": 21828067,
      "errorMsg": "",
      "fixid": "lnvgy_utl_uxsp_w8sp04p-2.50_platform_32-64",
      "latest": "true"
      "name": "",
      "origin": null,
      "payload": "true",
      "payloadFilename": "lnvgy_utl_uxsp_w8sp04p-2.50_platform_32-64.zip",
      "percentage": 100,
      "readableName": "Lenovo UpdateXpress System Pack",
      "readme": "true",
      "rebootRequired": "true",
      "releasedate": "2018-08-29",
      "releasedinterval": 9,
      "severity": 2,
      "state": "",
      "supportDownload": "true",
      "totalsize": 21828067,
      "version": "2.50",
   }
   ]
}]
```

```
    }
}
```

PUT /updateRepositories/firmware/uxsps

Use this method to modify information about UpdateXpress System Packs (UXSPs) in the updates repository.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/updateRepositories/firmware/uxsps`

Query parameters

Table 67. Export UXSP files

Parameters	Required / Optional	Description
action=export	Required	Compresses the specified UXSPs (firmware updates and device driver files) from the repository into a ZIP file, and downloads the ZIP file to your local system. A job is created to complete this request. Use the GET /tasks/*{job_list}* method to retrieve the job status and file name. If a job was not successfully started, refer to the response code and response body for details. When the job is complete, use GET /updateRepositories/firmware?action=export to download the zip file to the local system.
filetype=*{type}*	Required	Types of files to export. This can be one of the following values. • **all**. Exports all files (payload, change history, readme, and metadata files) for the selected UXSPs • **payloads**. Exports only payload (image) files for the selected UXSPs

The following example downloads a zip file of UXSP payload files to the local system.

`PUT https://192.0.2.0/updateRepositories/firmware/uxsps?action=export&filetypes=payload`

Table 68. Manage UXSPs in the repository

Parameters	Re-quired / Optional	Description
action=*{action}*	Required	Action to take. This can be one of the following values. • **read**. Reloads the information in the user interface. The clears the information in cache and reads the UXSP information again from the repository. • **refresh**. Retrieves information about UXSPs from the Lenovo XClarity Support website, and stores the information to the updates repository. You must specify the **mt**, **os**, and**type** request parameters. • **refreshThenAcquire**. Retrieves information about latest available UXSPs from the Lenovo XClarity Support website, stores the information to the updates repository, and downloads the UXSPs that are not already downloaded. **Important:** You must specify the **mt** and **os** request attributes. • **acquire**. Downloads the specified UXSPs files (firmware updates and device driver) from Lenovo XClarity Support website, and stores the files in the repository. You must specify the **fixids**, **mt**, and**type** request parameters.
with=*{scope}*	Optional	Scope of the action. This can be one of the following values. • **all**. (default) – When **action=refresh** is specified, this parameter returns information about all versions of all UXSPs that are available for all supported devices. Use the **fixids**, **mt**, and**type** request parameters to narrow the scope. – When **action= refreshThenAcquire** query parameter is specified, this query parameter retrieves information about all versions of all UXSPs for the specified machine types, then downloads the UXSPs that are not already downloaded • **latest**. – When **action=refresh** is specified, this parameter returns information about the most current version of all UXSPs for all supported devices. Use the **fixids**, **mt**, and **type** request parameters to narrow the scope. – When **action= refreshThenAcquire** query parameter is specified, this query parameter retrieves information about the most current version of all UXSPs for the specified machine types, then downloads the firmware UXSPs that are not already downloaded. • **payloads**. – When **action=acquire** is specified, this parameter returns information about the specified UXSPs (using the **fixids** request parameter).

The following example retrieves information about the latest available UXSPs and downloads the UXSPs that are not already downloaded.

```
PUT https://192.0.2.0/updateRepositories/firmware?action=refreshThenAcquire&with=latest
```

The following example reloads the web interface with information about the current repository.

```
PUT https://192.0.2.0/updateRepositories/firmware/uxsps?action=read
```

The following example refreshes the catalog with information about all of the most current UXSPs on the Lenovo XClarity Support website.

```
PUT https://192.0.2.0/updateRepositories/firmware/uxsps?action=refresh&with=latest
```

The following example downloads all files for the specified UXSPs from the Lenovo XClarity Support website.

```
PUT https://192.0.2.0/updateRepositories/firmware/uxsps?action=acquire
```

The following example downloads only payload files for the specified UXSPs on the Lenovo XClarity Support website.

```
PUT https://192.0.2.0/updateRepositories/firmware/uxsps?action=acquire&with=payloads
```

Request body

Attributes	Required / Optional	Type	Description
fixids	Required if **action** is “acquire”	Array of strings	List of IDs, separated by a comma, for UXSPs and firmware-updates to be acquired.
mt	Required if **action** is “refresh”, “refreshThenAcquire”, or “acquire”	Array of strings	List of machine types for which updates are to be refreshed or acquired.
os	Required if **action** is “refresh” or “refreshThenAcquire”	String	Operating system to be refreshed For UXSPs, this value must be empty (for example, `"os":""`).
type	Required if **action** is “refresh” or “acquire”	String	If **action=refresh**, this value must be **catalog**. If **action=acquire**, this value must be **latest**.

The following example retrieves information about and downloads the latest available firmware updates that are applicable to ThinkSystem SR530 servers when `?action=refreshThenAcquire&with=latest` is specified.

```
{
   "mt": ["7X07,7X08"],
   "os": "",
}
```

The following examples retrieves information about the latest available OS device drivers for Lenovo ThinkSystem SR530 servers when `?action=refresh&with=latest` is specified.

```
{
   "mt": ["7X07,7X08"]
```

```
   "os": "",
   "type": "catalog"
}
```

The following examples downloads the latest firmware-update and OS device-driver payload files for Lenovo ThinkSystem SR530 servers in the specified UXSPs when `?action=acquire&with=payloads` is specified.

```
{
   "fixids": [
      "lnvgy_utl_uxsp_c6sp03p-1.40_platform_32-64",
      "lnvgy_utl_uxsp_c5sp03p-1.40_platform_32-64"
   ],
   "mt": "7X07,7X08",
   "type": "latest"
}
```

The following examples downloads the latest firmware updates for specific fixes when `?action=acquire&with=payloads` is specified.

```
{
   "fixids": [
      "brcd_fw_bcsw_nos5.0.1_anyos_noarch",
      "brcd_fw_cna_3.2.4.0_linux_32-64",
      "brcd_fw_cna_3.2.3.0_linux_32-64",
      "lenovo_fw_dsa_dsyte2f-9.61_anyos_32-64"
   ],
   "mt": ["7X07,7X08"],
   "type": "latest"
}
```

The following examples export the latest firmware updates for specific device types when `?action=export&with=latest` is specified.

```
{
   "mt": ["7167", "7X05"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/updateRepositories/firmware/uxsps/*{id_list}*

Use this REST API to delete one or more UpdateXpress System Packs (UXSPs) from the repository.

HTTP methods

DELETE

DELETE /updateRepositories/firmware/uxsps/*{id_list}*

Use this method to delete one or more UpdateXpress System Packs (UXSPs) from the repository.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/updateRepositories/firmware/uxsps/{id_list}`

where *{id_list}* is list of one or more UXSP IDs, separated by a comma (comma (for example, lnvgy_utl_uxsp_c5sp03p-1.40_platform_32-64, lnvgy_utl_uxsp_c6sp03p-1.40_platform_32-64). To obtain the UXSP IDs, use GET /updateRepositories/firmware/uxsps method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
413	Request Entity Too Large	Clients might impose limitations on the length of the request URI, and the request URI is too long to be handled. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/updatableComponents

Use this REST API to start, apply, or cancel a firmware update on target devices and retrieve the status and progress of firmware updates.

HTTP methods

GET, PUT

GET /updatableComponents

Use this method to return the status of firmware updates that are in progress or retrieve a list of devices and components that can be updated..

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/updatableComponents
```

Query parameters

Parameters	Required / Optional	Description
action=*{data}*	Optional	The data to return. This can be one of the following values. • **getComponents**. Returns a list of devices and components that can be updated. • **applyStatus**. (default) Returns the status of firmware updates that are in progress

The following example returns a list of updatable devices and components.

```
GET https://192.0.2.0/updatableComponents?action=getComponents
```

The following example returns the status of firmware update jobs.

```
GET https://192.0.2.0/updatableComponents
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Table 69. Returns a list of devices and components that can be updated

Attributes	Type	Description
DeviceList	Array of objects	List of devices that are being updated
CMMList	Array of objects	List of CMM components
componentName	String	CMM component name
uuid	String	CMM component UUID
ServerList	Array of objects	List of server components
componentName	Array	Server component name
uuid	String	Server component UUID
StorageList	Array of objects	List of storage components
componentName	Array	Storage component name
uuid	String	storage component UUID
SwitchList	Array of objects	List of switch components
componentName	Array	switch component name
uuid	String	switch component UUID

Table 70. Returns the status of firmware updates that are in progress

Attributes	Type	Description
DeviceList	Array of objects	List of devices that are being updated
CMMList	Object	List of CMMs
UpdateStatus	Array	Status of the firmware update
JobID	Integer	
PercentComplete	Integer	

Table 70. Returns the status of firmware updates that are in progress (continued)

Attributes	Type	Description
Phase	String	Update phase. This can be one of the following values. • **Activating** • **Applying** • **Canceling** • **Complete** • **Completing** • **Initializing** • **Entering** • **Executing** • **Extracting** • **Pending** • **Performing** • **Preparing** • **Processing** • **Queued** • **Restarting** • **Starting** • **Transferring** • **Unknown** • **Validating** • **Waiting**
StartTime	String	
State	String	Update state. This can be one of the following values. • **Blocked** • **Cancel** • **Complete** • **Inprogress** • **Notstarted** • **Return**
Status	String	Update status. This can be one of the following values. • **Active** • **Inactive**
TaskID	Integer	
UUID	String	CMM UUID
ServerList	Object	List of servers
Components	Object	List of server components
Component	String	
UpdateStatus	Array	
JobID	Integer	
PercentComplete	Integer	

Table 70. Returns the status of firmware updates that are in progress (continued)

Attributes	Type	Description
Phase	String	Update phase. This can be one of the following values. • **Activating** • **Applying** • **Canceling** • **Complete** • **Completing** • **Initializing** • **Entering** • **Executing** • **Extracting** • **Pending** • **Performing** • **Preparing** • **Processing** • **Queued** • **Restarting** • **Starting** • **Transferring** • **Unknown** • **Validating** • **Waiting**
State	String	Update state. This can be one of the following values. • **Blocked** • **Cancel** • **Complete** • **Inprogress** • **Notstarted** • **Return**
Status	String	Update status. This can be one of the following values. • **Active** • **Canceled** • **Failed** • **Hardware_Not_Present** • **Skip_Already_Applied** • **Skip_Already_Compliant** • **Skip_Do_Not_Update** • **Queued** • **Succeed**
TaskID	Integer	
UpdateStatus	Array	
CurrentComponent	Array	
Component	String	This can be one of the following values. • **Queued**
PercentComplete	Integer	
State	String	This can be one of the following values. • **Blocked** • **Cancel** • **Complete** • **Inprogress** • **Notstarted** • **Return**

Table 70. Returns the status of firmware updates that are in progress (continued)

Attributes	Type	Description
Status	String	This can be one of the following values. • **Active** • **Inactive**
TotalComponents	Integer	Total number of components to be updated
TotalComplete	Integer	Total number of completed updates
Weight	Integer	
UUID	String	Switch UUID
StorageList	Array of objects	List of switches
UpdateStatus	Array	Status of the firmware update
JobID	Integer	
PercentComplete	Integer	
Phase	String	This can be one of the following values. • **Activating** • **Applying** • **Canceling** • **Complete** • **Completing** • **Initializing** • **Entering** • **Executing** • **Extracting** • **Pending** • **Performing** • **Preparing** • **Processing** • **Queued** • **Restarting** • **Starting** • **Transferring** • **Unknown** • **Validating** • **Waiting**
State	String	This can be one of the following values. • **Blocked** • **Cancel** • **Complete** • **Inprogress** • **Notstarted** • **Return**
Status	String	This can be one of the following values. • **Active** • **Inactive**
TaskID	Integer	
UUID	String	Storage device UUID
SwitchList	Array of objects	List of switches

Table 70. Returns the status of firmware updates that are in progress (continued)

Attributes	Type	Description
ReadinessCheck	Object	
ElapsedTime	String	
ElapsedTimeFormatted	String	
EndTime	String	
JobID	Integer	Job ID
PercentComplete	Integer	
Phase	String	This can be one of the following values. • **Activating** • **Applying** • **Canceling** • **Complete** • **Completing** • **Initializing** • **Entering** • **Executing** • **Extracting** • **Pending** • **Performing** • **Preparing** • **Processing** • **Queued** • **Restarting** • **Starting** • **Transferring** • **Unknown** • **Validating** • **Waiting**
StartTime	String	
State	String	This can be one of the following values. • **Blocked** • **Cancel** • **Complete** • **Inprogress** • **Notstarted** • **Return**
Status	String	This can be one of the following values. • **Active** • **Inactive**
TaskID	Integer	Subtask ID
Message	Object	
result	String	Result of the request. This can be one of the following values. • **informational**. The request completed successfully.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text that is associated with the message identifier

Table 70. Returns the status of firmware updates that are in progress (continued)

Attributes	Type	Description
explanation	String	
UpdateStatus	Array	Status of the firmware update
EndTime	String	
JobID	Integer	
PercentComplete	Integer	
Phase	String	This can be one of the following values. • **Activating** • **Applying** • **Canceling** • **Complete** • **Completing** • **Initializing** • **Entering** • **Executing** • **Extracting** • **Pending** • **Performing** • **Preparing** • **Processing** • **Queued** • **Restarting** • **Starting** • **Transferring** • **Unknown** • **Validating** • **Waiting**
State	String	This can be one of the following values. • **Blocked** • **Cancel** • **Complete** • **Inprogress** • **Notstarted** • **Return**
Status	String	This can be one of the following values. • **Active** • **Inactive**
TaskID	Integer	
Message	Object	
result	String	Result of the request. This can be one of the following values. • **informational**. The request completed successfully.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text that is associated with the message identifier
explanation	String	
UUID	String	Switch UUID

Table 70. Returns the status of firmware updates that are in progress (continued)

Attributes	Type	Description
UpdateStatusMetrics	Array	
TotaldeviceUpdates	Integer	
TotaldeviceUpdatesActive	Integer	
TotaldeviceUpdatesComplete	Integer	
TotaldeviceUpdatesInProgress	Integer	
TotalJobs	Integer	Total number of jobs
TotalJobsComplete	Integer	Number of completed jobs
TotalJobsInProgress	Integer	
TotalJobsPercentComplete	Integer	
TotalSupportTasks	Integer	
TotalSupportTasksActive	Integer	
TotalTasks	Integer	Total number of tasks
TotalTasksBlocked	Integer	
TotalTasksCanceled	Integer	
TotalTasksComplete	Integer	
TotalTasksFailed	Integer	
TotalTasksInProgress	Integer	
TotalTasksSuccess	Integer	
TotalUpdateTasksActive	Integer	
TotalUpdateTasks	Integer	
result	String	Request results. This can be one of the following values. • **informational**. The request completed successfully.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text that is associated with the message identifier

The following example is returned if you specify **query=status**.

```
{
   "DeviceList": [{
      "CMMList": [{
         "UpdateStatus": {
            "JobID": 1,
            "PercentComplete": 1,
            "Phase": "Applying",
            "StartTime": "2015-04-13 12:50:31.077",
            "State": "InProgress",
            "Status": "Active",
            "TaskID": 1,
```

```
      },
      "UUID": "6134AFCEA91311E199A5A45AC8953137"
   }]
},
{
   "ServerList": [{
      "UUID": "8BFBADCC33CB11E499F740F2E9903640",
      "Components": [{
         "Component": "System Prerequisites",
         "UpdateStatus": {
            "JobID": 1,
            "PercentComplete": 0,
            "Phase": "Queued",
            "State": "Blocked",
            "Status": "Queued",
            "TaskID": 4,
         },
         "Weight": 1
      },
      ...,
      {
         "Component": "ITE",
         "UpdateStatus": {
            "CurrentComponent": {
               "Component": "Queued"
            },
            "PercentComplete": 0,
            "State": "NotStarted",
            "Status": "Active",
            "TotalComplete": 0,
            "TotalComponents": 32
         }
      }]
   },
   ...,
   {
      "UUID": "0CDF130FDFC211E392806CAE8B704250",
      "Components": [{
         "Component": "System Prerequisites""UpdateStatus": {
            "JobID": 1,
            "PercentComplete": 0,
            "Phase": "Queued",
            "State": "Blocked",
            "Status": "Queued",
            "TaskID": 64
         },
         "Weight": 1,

      },
      ...,
      {
         "Component": "ITE",
         "UpdateStatus": {
            "CurrentComponent": {
               "Component": "Queued"
            },
            "PercentComplete": 0,
            "State": "NotStarted",
            "Status": "Active",
            "TotalComplete": 0,
            "TotalComponents": 30
```

```
         }
      }]
   }]
},
{
   "SwitchList": [{
      "ReadinessCheck": {
         "ElapsedTime": "00:00:00:01.509",
         "ElapsedTimeFormatted": "1 second 509 milliseconds",
         "EndTime": "2016-04-07 23:44:10.366",
         "JobID": 1,
         "PercentComplete": 100,
         "Phase": "Complete",
         "StartTime": "2016-04-07 23:44:08.857",
         "State": "Complete",
         "Status": "Failed",
         "TaskID": 1,
         "Message": {
            "result": "informational",
            "messages": [{
               "id": "FQXHMUP1000I",
               "text": "The command completed successfully."
            },
            ...,
            {
               "id": "FQXHMUP4545L",
               "text": "The device is not ready for an update.",
               "explanation": "The device did not pass validation for firmware updates..",
               "recovery": {
                  "text": "Correct the issues discovered by validation checks."
               }
            }]
         }
      },
      "UpdateStatus": {
         "EndTime": "2016-04-07 23:44:10.869",
         "JobID": 1,
         "PercentComplete": 100,
         "Phase": "Complete",
         "State": "Complete",
         "Status": "Canceled",
         "TaskID": 3,
         "Message": {
            "result": "warning",
            "messages": [{
               "id": "FQXHMUP4086F",
               "text": "The RackSwitch G7052 xHMCUpdates task was canceled.",
               "explanation": "The task was canceled because the required task RackSwitch G7052
                               xHMCUpdates (10.243.1.152): READINESSCHECK: (jobid_1-taskid_1)
                           that this task depends on did not complete successfully.",
               "recovery": {
                  "text": "Try to perform the update again. If the problem persists, please
                           contact Customer Support."
               }
            }]
         }
      },
      "UUID": "0b0f5101bb8844b8b2d1c1aaeb24f446"
   }]
}],
"UpdateStatusMetrics": {
```

```
      "TotaldeviceUpdates": 6,
      "TotaldeviceUpdatesActive": 6,
      "TotaldeviceUpdatesComplete": 0,
      "TotaldeviceUpdatesInProgress": 1,
      "TotalJobs": 1,
      "TotalJobsComplete": 0,
      "TotalJobsInProgress": 1,
      "TotalJobsPercentComplete": 0,
      "TotalSupportTasks": 18,
      "TotalSupportTasksActive": 18,
      "TotalTasks": 93,
      "TotalTasksBlocked": 92,
      "TotalTasksCanceled": 0,
      "TotalTasksComplete": 0,
      "TotalTasksFailed": 0,
      "TotalTasksInProgress": 1,
      "TotalTasksSuccess": 0,
      "TotalUpdateTasks": 75,
      "TotalUpdateTasksActive": 72
   },
   "result": "informational",
   "messages": [{
      "id": "FQXHMUP4091I",
      "text": "Update Status was obtained successfully."
   }]
}
```


PUT /updatableComponents

Use this method to start, apply or cancel a firmware update on target devices.

The request body differs depending on the action that you want to perform. You can use this PUT method to perform the following management actions.

- Applying or canceling a firmware
- Modifying the power state

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/updatableComponents`

Query parameters

Parameters	Required / Optional	Description
action=*{action}*	Optional	Action to take. This can be one of the following values. • **apply**. (default) Applies the firmware updates to the specified components using applicable update packages. • **applyBundle**. Applies firmware updates to all components of specified ThinkSystem SR635 and SR655 devices according to the assigned firmware-compliance policy using a bundled image that contain all applicable firmware packages. **Attention:** Before using the bundled-update function, review important information regarding ThinkSystem SR635 and SR655 devices and the bundle-update function limitations (see Firmware update considerations in the Lenovo XClarity Administrator online documentation). • **cancelApply**. Cancels the firmware update request for the specified components. • **powerState**. Performs a power operation on the specified device.
activationMode=*{mode}*	Optional	Indicates when to activate the update. This can be one of the following values. • **immediate**. (default) During the update process, the target device might be automatically restarted multiple times until the entire process is complete. Ensure that you quiesce all applications on the target device before you proceed. • **prioritized**. Firmware updates on the baseboard management controller are activated immediately; all other firmware updates are firmware updates are activated the next time the device is restarted. Additional restarts are then performed until the update operation completes. This rule is supported only for servers. • **delayed**. Some but not all update operations are performed. The target device must be restarted manually to continue the update process. Additional restarts are then performed automatically until the update operation completes. This rule is supported only for servers and rack switches.
forceUpdateMode=*{mode}*	Optional	Indicates whether to apply the update if firmware is already compliant. This can be one of the following values. • **true**. Applies the firmware update to the selected devices even if the firmware is compliant. • **false**. (default) Skips the firmware update on the selected devices if the firmware is already compliant.
functionType=*{type}*	Optional	Indicates the function that applies to the power action. This can be one of the following values. • **firmwareUpdates**. (default) • **osDriverUpdates**. **Note:** This query parameter is used only when the **action=powerState** query parameter is specified.
installPrereq=*{Boolean}*	Optional	Indicates whether to install firmware prerequisites. This can be one of the following values. • **true**. (default) Installs all firmware prerequisites, if needed. • **false**. Do not install firmware prerequisites.

Parameters	Required / Optional	Description
memoryTest={*Boolean*}	Optional	Indicates whether to run a memory test after the update firmware completes. This can be one of the following values. • **true**. (default) Run a memory test. • **false**. Do not run a memory test. **Note:** This option is applicable only when **activationMode** is **immediate** and the server is rebooted during the firmware update.
onErrorMode={*mode*}	Optional	Indicates how to handle errors during the firmware update. This can be one of the following values. • **stopOnError**. Stops all firmware updates within the selected devices if an error is encountered. • **stopdeviceOnError**. Stops all firmware updates on a specific device if an error is encountered and continues with the other devices. • **continueOnError**. (default) Ignores errors and continues firmware updates on the devices.

The following example applies firmware updates, including firmware prerequisite, to a server using prioritized activation.

```
PUT https://192.0.2.0/updatableComponents?action=apply&functionType=firmwareUpdates
&activationMode=prioritized
```

Request body

Table 71. Applying or canceling a firmware update

Attributes	Required / Optional	Type	Description
DeviceList	Required	Array of objects	List of devices
CMMList	Optional	Array of objects	List of CMMs
Components	Required	Array of strings	List of components in the CMM
Component	Required	String	Component name To obtain the component name, use the GET /updateRepositories/firmware method.
Fixid	Optional	String	Firmware-update ID of the target package to be applied to the component. Specify if this attribute if the update is not driven by the firmware-compliance policy. Do not specify if the update is driven by the policy. To obtain the firmware-update IDs, use the GET /updateRepositories/firmware method.
UUID	Required	String	UUID of the chassis CMM
ServerList	Optional	Array of objects	List of servers
Components	Required	Array of objects	List of components in the server

Table 71. Applying or canceling a firmware update (continued)

Attributes	Re-quired / Optional	Type	Description
Component	Required	String	Component name To obtain the component name, use the GET /updateRepositories/firmware method.
Fixid	Optional	String	Firmware-update ID of the target package to be applied to the component. Specify if this attribute if the update is not driven by the firmware-compliance policy. Do not specify if the update is driven by the policy. To obtain the firmware-update IDs, use the GET /updateRepositories/firmware method.
UUID	Required	String	UUID of the server
StorageList	Optional	Array of objects	List of storage devices
Components	Required	Array of objects	List of components in the storage device
Component	Required	String	Component name To obtain the component name, use the GET /updateRepositories/firmware method.
Fixid	Optional	String	Firmware-update ID of the target package to be applied to the component. Specify if this attribute if the update is not driven by the firmware-compliance policy. Do not specify if the update is driven by the policy. To obtain the firmware-update IDs, use the GET /updateRepositories/firmware method.
UUID	Required	String	WWNN of the storage device
SwitchList	Optional	Array of objects	List of switches
Components	Required	Array of objects	List of components in the switch
Component	Required	String	Component name To obtain the component name, use the GET /updatableComponents method.
Fixid	Optional	String	Firmware-update ID of the target package to be applied to the component. Specify if this attribute if the update is not driven by the firmware-compliance policy. Do not specify if the update is driven by the policy. To obtain the firmware-update IDs, use the GET /updateRepositories/firmware method.
UUID	Required	String	UUID of the switch

The following example applies firmware updates to multiple devices and components.

```
{
   "DeviceList": [{
      "ServerList": [{
         "UUID": "8BFBADCC33CB11E499F740F2E9903640",
         "Components": [{
            "Fixid": "lnvgy_fw_imm2_tcoo17g-3.00_anyos_noarch",
```

```
            "Component": "IMM2 (Backup)"
         },
         {
            "Fixid": "lnvgy_fw_imm2_tcoo17g-3.00_anyos_noarch",
            "Component": "IMM2 (Primary)"
         }]
      }]
   },
   {
      "CMMList": [{
         "UUID": "8BFBADCC33CB11E499F740F2E9903640",
         "Components": [{
            "Fixid": "lnvgy_fw_imm2_tcoo17g-3.00_anyos_noarch",
            "Component": "CMM")"
         }]
      }]
   },
   {
      "SwitchList": [{
         "UUID": "8BFBADCC33CB11E499F740F2E9903640",
         "Components": [{
            "Fixid": "lnvgy_fw_scsw_en4093r-8.3.9.0_anyons_noarch",
            "Component": "Main Application"
         }]
      }]
   },
   {
      "StorageList": [{
         "UUID": "8BFBADCC33CB11E499F740F2E9903640",
         "Components": [{
            "Fixid": "lnvgy_fw_storage_1.1.1",
            "Component": "Controller a"
         }]
      }]
   }]
}
```


Table 72. Modifying the power state

Attributes	Required / Optional	Type	Description
DeviceList	Required	Array of objects	List of devices
CMMList	Optional	Array of objects	List of CMMs
PowerState	Required	String	Performs a power operation on the CMM. This can be one of the following values. • **reset**. Restart the CMM.
UUID	Required	String	UUID of the chassis CMM
ServerList	Optional	Array of objects	List of servers

Table 72. Modifying the power state (continued)

Attributes	Required / Optional	Type	Description
PowerState	Required	String	Performs a power operation on the device. This can be one of the following values: • **powerOn**. Powers on the server • **powerOff**. Powers off the server • **powerCycleSoft**. Immediately restarts the server • **powerCycleSoftGrace**. Restarts the server gracefully (shuts down the operating system where applicable) • **powerOffHard**. Immediately powers off the operating system, and shut down the server • **powerOffHardGrace**. Powers off the server gracefully (shuts down the operating system where applicable)
UUID	Required	String	UUID of the server
StorageList	Optional	Array of objects	List of storage devices
PowerState	Required	String	Performs a power operation on the device. This can be one of the following values. • **powerOff**. Power off the storage device • **powerCycleSoft**. Restart the storage device
UUID	Required	String	WWNN of the storage device
SwitchList	Optional	Array of objects	List of switches
PowerState	Required	String	Performs a power operation on the switch. This can be one of the following values. • **powerOn**. Power on the switch • **powerOff**. Power off the switch • **powerCycleSoft**. Restart the switch
UUID	Required	String	UUID of the switch

The following example performs power actions on multiple devices.

```
{
   "DeviceList": [{
      "CMMList": [{
         "PowerState": "reset",
         "UUID": "8BFBADCC33CB11E499F740F2E9972457"
      }]
   },
   {
      "ServerList": [{
         "PowerState": "powerOn",
         "UUID": "8BFBADCC33CB11E499F740F2E9936841"
      }]
   },
   {
      "StorageList": [{
         "PowerState": powerCycleSoft,
         "UUID": "8BFBADCC33CB11E499F740F2E9927945"
      }]
   },
   {
      "SwitchList": [{
```

```
         "PowerState": powerCycleSoft,
         "UUID": "8BFBADCC33CB11E499F740F2E9932769"
      }]
   }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response body provides information about the success or failure of the request. The attributes in the response body differ depending on the specified request attributes.

Note: A response body is not returned for some requests.

The following example is returned when modifying the power state for multiple devices.

```
{
   "DeviceList": [{
      "CMMList": [{
         "UUID": "8BFBADCC33CB11E499F740F2E9972457",
         "PowerStatus": {
            "PowerRequest": "reset",
            "Status": "Success",
            "Message”: {
               result: "informational",
               messages: []
            }
         }
      }]
   },
   {
      "ServerList": [{
         "UUID": "8BFBADCC33CB11E499F740F2E9936841",
         "PowerStatus": {
            "PowerRequest": "powerOn",
            "Status": "Success",
            "Message”: {
               result: "informational",
               messages: []
            }
         }
      }]
   },
```

```
   {
      "StorageList": [{
         "UUID": "8BFBADCC33CB11E499F740F2E9927945",
         "PowerStatus": {
            "PowerRequest": "powerCycleSoft",
            "Status": "Success",
            "Message": {
               result: "informational",
               messages: []
            }
         }
      }]
   },
   {
      "SwitchList": [{
         "UUID": "8BFBADCC33CB11E499F740F2E9932769",
         "PowerStatus": {
            "PowerRequest": "powerCycleSoft",
            "Status": "Success",
            "Message": {
               result: "informational",
               messages: []
            }
         }
      }]
   }]
}
```

Chapter 10. Management-server update

The following resources are available for performing management-server update functions.

/authCodes

Use this REST API to return a list of authorization code, add one or more license-authorization codes in Lenovo XClarity Administrator, fetch redeemed licenses key from the Features on Demand web portal, manage license keys for one or more authorization codes, or modify customer information.

Note: This REST API requires Lenovo XClarity Administrator v3.5.0 or later.

HTTP methods

GET, POST, PUT, PATCH

GET /authCodes

Use this method to return a list of authorization codes in Lenovo XClarity Administrator.

Note: This REST API requires Lenovo XClarity Administrator v3.5.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/authCodes`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
authCodes	Array of objects	Information about each license-authorization code
authCode	String	License-authorization code ID
errorMsg	String	Message description
featureCode	String	License feature code
featureDescription	String	License feature description
keysRedeemed	Integer	Number of redeemed license-activation keys
keysRemaining	Integer	Number of available (not redeemed) license-activation keys
lenovoCustomerNumber	String	Lenovo customer number
licenseKeys	Array of objects	Information about each license-activation key
customerNumber	String	Lenovo customer number associated with the license-activation key
licenseKeyId	String	License-activation key ID
quantity	Integer	Number of redeemed licensees
state	String	License-activation key state. This can be one of the following values. • **installed**. The license-activation key is installed in XClarity Administrator. • **not installed**. The license-activation key is not installed.
partNumber	String	License part number
purchaseOrder	String	License purchase-order number
salesOrder	String	License sales-order number
startDate	String	Date when the authorization code was created and the license validation period starts This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
customerInfo	Object	Information about the customer that is associated with the license-authorization codes
companyNameInEnglish	String	Customer company name in English
companyNameInLocalLanguage	String	Customer company name in local language
contactPhoneNumber	String	Customer phone number
contactEmailAddress	String	Customer email address
customerAddress	String	Customer physical address
customerCity	String	Customer city
customerRegionStateOrProvince	String	Customer state or region
customerPostalCode	String	Customer postal code
country	String	Customer country code For a complete list of country codes, use GET /licenseCountries.

Attributes		Type	Description
	firstName	String	Customer given name
	lastName	String	Customer family name
	preferredLanguage	String	Language code of the preferred language For a complete list of language codes, use GET /licenseCountries.

The following example is returned if the request is successful.


```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V11OOAID2K4",
      "errorMsg": "",
      "featureCode": "1341 contact",
      "featureDescription": "Lenovo XClarity Pro, Per Managed Endpoint w/5 Yr SW S&S",
      "keysRedeemed": 50,
      "keysRemaining ": 0,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [],
      "partNumber": "5641PX5",
      "purchaseOrder": "OOOOOOOO",
      "salesOrder": "999999999",
      "startDate": "2020-06-02",
   },
   {
      "authCode": "YYA7BQ2V37V11OOAID2K5",
      "errorMsg": "",
      "featureCode": "1341 contact",
      "featureDescription": "Lenovo XClarity Pro, Per Managed Endpoint w/5 Yr SW S&S",
      "keysRedeemed": 50,
      "keysRemaining ": 0,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "OOOO1",
         "quantity": 20,
         "state": "installed"
      },
      {
         "customerNumber": "1234567890",
         "licenseKeyId": "OOOO3",
         "quantity": 30,
         "state": "installed"
      },
      ...],
      "partNumber": "5641PX5",
      "purchaseOrder": "OOOOOOOO",
      "salesOrder": "999999999",
      "startDate": "2020-06-02"
   }],
   "customerInfo": {
      "companyNameInEnglish": "Some Company",
      "companyNameInLocalLanguage": " Some Company ",
      "contactPhoneNumber": "9995551212",
      "contactEmailAddress": "jane.doe@somecompany.com",
      "customerAddress": "10 Main Street",
      "customerCity": "Rockville",
      "customerRegionStateOrProvince": "NY",
      "customerPostalCode": "12345",
      "country": "US",
```

```
      "firstName": "Jane",
      "lastName": "Doe",
      "preferredLanguage": "EN"
   }
}
```

POST /authCodes

Use this method to add one or more license-authorization codes in Lenovo XClarity Administrator by retrieving authorization-code data from the Features on Demand web portal and, if the authorization code has already been redeemed, retrieve its license-activation keys.

Note: This REST API requires Lenovo XClarity Administrator v3.5.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/authCodes`

Query parameters

None

Request body

- **Add a single authorization code**

Attributes	Required / Optional	Type	Description
authCode	Required	String	License-authorization code ID
lenovoCustomerNumber	Required if **authCode** is not specified	String	Lenovo customer number You can specify either **authCode** or **lenovoCustomerNumber**, but not both.
retrieveKeys	Optional	Boolean	Indicates whether to retrieve license-activation keys. This can be one of the following values. – **true**. Retrieve license-activation keys. – **false**. (default) Do not retrieve license-activation keys.

The following example adds an authorization code to XClarity Administrator but does not retrieve the license-activation keys for that code.

```
{
   "authCode": "YYA7BQ2V37V11OOAID2K4"
}
```

The following example adds an authorization code to XClarity Administrator and retrieves license-activation keys for that code.

```
{
   "authCode": "YYA7BQ2V37V11OOAID2K4"
   "retrieveKeys": true
}
```

The following example retrieves license-activation keys for that all authorization codes associated with the specified Lenovo customer number.

```
{
   "lenovoCustomerNumber": "1234567890",
   "retrieveKeys": true
}
```

- **Add multiple authorization codes**Use the “multipart/form-data” content type to import a CSV file that contains one or more authorization codes, separated by a comma (for example, WWGDISQHE24UQK05MVM1P9,WWMEHFI7SNL7K9L59T6OBT,WWTRPECTK9OFNHR8RJUPVT). For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage.

  The following example imports a CVS file that contains the authorization codes.

  Request Header

  ```
  Content-Type: multipart/form-data; boundary=AaB03x
  ```

  Request body

  ```
  --AaB03x
      Content-Disposition: form-data; name="fileUpload"; filename="auth_codes.csv"
      Content-Type: application/octet-stream
  --AaB03x--
  ```

- **Retrieve license-activation keys**

Attributes	Required / Optional	Type	Description
authCode	Required	Object	Information about the authorization code for which you want to retrieve license-activation keys
authCode	Required	String	License-authorization code ID If you specify a Lenovo customer number, specify an empty string for the authorization code.
lenovoCustomerNumber	Optional	String	Lenovo customer number If you specify an authorization code, specify an empty string for the Lenovo customer number.
retrieveKeys	Optional	Boolean	Indicates whether to retrieve license-activation keys. This value is always **true**.

The following example fetches the redeemed license-activation keys for a specific authorization code.

```
{
   "authCode": {
      "authCode": "YYA7BQ2V37V1100AID2K4",
      "retrieveKeys": true
   }
}
```

The following example fetches the redeemed license-activation keys for all authorization codes that are associated with a specific Lenovo customer number.

```
{
   "authCode": {
      "authCode": "",
      "lenovoCustomerNumber": "1234567890",
      "retrieveKeys": true
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
authCodes	Array of objects	Information about each license-authorization code
authCode	String	License-authorization code ID
errorMsg	String	Message description
featureCode	String	License feature code
featureDescription	String	License feature description
keysRedeemed	Integer	Number of redeemed license-activation keys
keysRemaining	Integer	Number of available (not redeemed) license-activation keys
lenovoCustomerNumber	String	Lenovo customer number
licenseKeys	Array of objects	Information about each license-activation key
customerNumber	String	Lenovo customer number associated with the license-activation key
licenseKeyId	String	License-activation key ID
quantity	Integer	Number of redeemed licensees
state	String	License-activation key state. This can be one of the following values. • **installed**. The license-activation key is installed in XClarity Administrator. • **not installed**. The license-activation key is not installed.
partNumber	String	License part number
purchaseOrder	String	License purchase-order number
salesOrder	String	License sales-order number
startDate	String	Date when the authorization code was created and the license validation period starts This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
customerInfo	Object	Information about the customer that is associated with the license-authorization codes

Attributes		Type	Description
	companyNameInEnglish	String	Customer company name in English
	companyNameInLocalLanguage	String	Customer company name in local language
	contactPhoneNumber	String	Customer phone number
	contactEmailAddress	String	Customer email address
	customerAddress	String	Customer physical address
	customerCity	String	Customer city
	customerRegionStateOrProvince	String	Customer state or region
	customerPostalCode	String	Customer postal code
	country	String	Customer country code For a complete list of country codes, use GET /licenseCountries.
	firstName	String	Customer given name
	lastName	String	Customer family name
	preferredLanguage	String	Language code of the preferred language For a complete list of language codes, use GET /licenseCountries.

The following example is returned if the request is successful when a CSV file is used to create multiple license authorization codes.


```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V11OOAID2K4",
      "errorMsg": "",
      "featureCode": "1341 contact",
      "featureDescription": "Lenovo XClarity Pro, Per Managed Endpoint w/5 Yr SW S&S",
      "keysRedeemed": 0,
      "keysRemaining ": 50,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [],
      "partNumber": "5641PX5",
      "purchaseOrder": "OOOOOOOO",
      "salesOrder": "999999999",
      "startDate": "2020-06-02",
   },
   {
      "authCode": "YYA7BQ2V37V11OOAID2K5",
      "errorMsg": "",
      "featureCode": "1341 contact",
      "featureDescription": "Lenovo XClarity Pro, Per Managed Endpoint w/5 Yr SW S&S",
      "keysRedeemed": 0,
      "keysRemaining ": 50,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [],
      "partNumber": "5641PX5",
      "purchaseOrder": "OOOOOOOO",
      "salesOrder": "999999999",
      "startDate": "2020-06-02"
   }],
   "customerInfo": {
      "companyNameInEnglish": "Some Company",
```

```
      "companyNameInLocalLanguage": " Some Company ",
      "contactEmailAddress": "jane.doe@somecompany.com",
      "contactPhoneNumber": "9995551212",
      "customerAddress": "10 Main Street",
      "customerCity": "Rockville",
      "customerRegionStateOrProvince": "NY",
      "customerPostalCode": "12345",
      "country": "US",
      "firstName": "Jane",
      "lastName": "Doe",
      "preferredLanguage": "EN"
   }
}
```

The following example is returned if the request is successful when the **authCode** attribute in the JSON request body is used to create a single license authorization code and when license keys are fetched (**keyState = retrieve**).

```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V11OOAID2K5",
      "errorMsg": "",
      "featureCode": "1341 contact",
      "featureDescription": "Lenovo XClarity Pro, Per Managed Endpoint w/5 Yr SW S&S",
      "keysRedeemed": 0,
      "keysRemaining ": 50,
      "lenovoCustomerNumber": "123456789O",
      "licenseKeys": [{
      "licenseKeyFile": "OOOO1",
         "customerNumber": "123456789O",
         "licenseKeyId": "OOOO1",
         "quantity": 20,
         "state": "installed"
      },
      {
         "customerNumber": "123456789O",
         "licenseKeyId": "OOOO3",
         "quantity": 30,
         "state": "installed"
      },
      ...],
      "partNumber": "5641PX5",
      "purchaseOrder": "OOOOOOOO",
      "salesOrder": "999999999",
      "startDate": "2020-06-02"
   }],
   "customerInfo": {
      "companyNameInEnglish": "Some Company",
      "companyNameInLocalLanguage": " Some Company ",
      "contactEmailAddress": "jane.doe@somecompany.com",
      "contactPhoneNumber": "9995551212",
      "customerAddress": "10 Main Street",
      "customerCity": "Rockville",
      "customerRegionStateOrProvince": "NY",
      "customerPostalCode": "12345",
      "country": "US",
      "firstName": "Jane",
      "lastName": "Doe",
      "preferredLanguage": "EN"
   }
}
```

PUT /authCodes

Use this method to redeem licenses from one or more authorization codes, fetch redeemed license-activation keys, and modify customer information.

You can perform the following management tasks.

- **Redeem licenses for one or more authorization codes**

  Lenovo XClarity Administrator sends a request to the Features on Demand web portal to redeem the licenses. The web portal creates a license-key file for each authorization code and downloads the files to the management server. Each license-key file contains the set of redeemed licenses for a specific authorization code. You can then use the license-key file to apply licenses to the current XClarity Administrator, or you can import and install the downloaded license key file into another XClarity Administrator that might not have access to the Features on Demand web portal.

  If you specify a single authorization code, you can redeem all or a subset of licenses by specifying the **keysRedeemQty** request attribute. You must also specify the **authCode** attribute, **lenovoCustomerNumber** attribute, and set **licenseKeys.state** to “not installed.”

  If you specify a multiple authorization code, all remaining licenses for the specified authorization codes are redeemed. Use the **authCode** attribute to identify the license authorization code, and set **licenseKeys.state** to “not installed.”

  When you redeem licenses for authorization codes, the license-activation keys are retrieved automatically.

- **Retrieve license keys for one or more authorization codes**

  You can manually retrieve license-activation keys from the Features on Demand web portal for a license-authorization code that has redeemed licenses. You must also specify either authorization code or Lenovo customer number set the **retrieveKeys** attribute to “true.” If a single license-activation keys is selected, the key is saved as a .KEY file on the local system. If multiple license-activation keys are selected, the license-activation key files are compressed into a ZIP file that is saved on the local system. The file location is returned in the “Location” field in the response header.

  After retrieving keys, you can then import and install the keys in XClarity Administrator using POST /quantityLicense.

- **Modifying customer information**

  You can set new values for customer information by using the **customerInfo** attributes.

Note: This REST API requires Lenovo XClarity Administrator v3.5.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/authCodes`

Query parameters

None

Request body

This request updates the entire resource. If an optional attribute is set to an empty string, that attribute is not changed. If an idempotent (unchangeable) attribute is modified, an error is thrown.

Attributes	Re-quired / Optional	Type	Description
authCodes	Required	Array of objects	Information about each license-authorization code
authCode	Required	String	License-authorization code ID
errorMsg	Required	String	Message description This attribute is idempotent (cannot be changed).
featureCode	Required	Integer	License feature code This attribute is idempotent (cannot be changed).
featureDescription	Required	String	License feature description This attribute is idempotent (cannot be changed).
keysRedeemed	Required	Integer	Number of redeemed license-activation keys This attribute is idempotent (cannot be changed).
keysRedeemQty	Required	Integer	Number of redeemed license-activation keys
keysRemaining	Required	Integer	Number of available (not redeemed) license-activation keys This attribute is idempotent (cannot be changed).
lenovoCustomerNumber	Required	String	Lenovo customer number
licenseKeys	Required	Array of objects	Information about each license-activation key
customerNumber	Required	String	Lenovo customer number associated with the license-activation key
licenseKeyId	Required	String	License-activation key ID This attribute is idempotent (cannot be changed).
quantity	Required	Integer	Number of redeemed licenses
state	Required	String	License-activation key state This attribute cannot be changed.
partNumber	Required	String	License part number This attribute is idempotent (cannot be changed).
purchaseOrder	Required	String	License purchase-order number This attribute is idempotent (cannot be changed).
retrieveKeys	Required	Boolean	Indicates whether to retrieve license-activation keys. This can be one of the following values. • **true**. Retrieve license-activation keys. • **false**. (default) Do not retrieve license-activation keys.
salesOrder	Required	String	License sales-order number This attribute is idempotent (cannot be changed).
startDate	Required	String	Date when the authorization code was created and the license validation period starts This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage. This attribute is idempotent (cannot be changed).
customerInfo	Required	Object	Information about the customer that is associated with the license-authorization codes

Attributes	Required / Optional	Type	Description
companyNameInEnglish	Required	String	Customer company name in English
companyNameInLocalLanguage	Required	String	Customer company name in local language
contactPhoneNumber	Required	String	Customer phone number
contactEmailAddress	Required	String	Customer email address
customerAddress	Required	String	Customer physical address
customerCity	Required	String	Customer city
customerRegionStateOrProvince	Required	String	Customer state or region
customerPostalCode	Required	String	Customer postal code
country	Required	String	Customer country code
firstName	Required	String	Customer given name
lastName	Required	String	Customer family name
preferredLanguage	Required	String	Preferred language

The following example redeems ten of the remaining licenses in an authorization code.

```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V11OOAID2K4",
      "errorMsg": "",
      "featureCode": "",
      "featureDescription": "",
      "keysRedeemed": null,
      "keysRedeemQty": "10",
      "keysRemaining ": null,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "",
         "quantity": 10,
         "state": "not installed",
      }],
      "partNumber": "",
      "purchaseOrder": "",
      "retrieveKeys": false,
      "salesOrder": "",
      "startDate": "",
   }],
   "customerInfo": {
      "companyNameInEnglish": "",
      "companyNameInLocalLanguage": "",
      "contactPhoneNumber": "",
      "contactEmailAddress": "",
      "customerAddress": "",
      "customerCity": "",
      "customerRegionStateOrProvince": "",
      "customerPostalCode": "",
      "country": "",
      "firstName": "",
```

```
      "lastName": "",
      "preferredLanguage": ""
   }
}
```

The following example redeems all remaining licenses for two authorization codes.

```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V11OOAID2K4",
      "errorMsg": "",
      "featureCode": "",
      "featureDescription": "",
      "keysRedeemed": null,
      "keysRedeemQty": null,
      "keysRemaining ": null,
      "lenovoCustomerNumber": "",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "",
         "quantity": null,
         "state": "not installed",
      }],
      "partNumber": "",
      "purchaseOrder": "",
      "retrieveKeys": false,
      "salesOrder": "",
      "startDate": "",
   },
   {
      "authCode": "YYA7BQ2V37V11OOAID2K5",
      "errorMsg": "",
      "featureCode": "",
      "featureDescription": "",
      "keysRedeemed": null,
      "keysRedeemQty": null,
      "keysRemaining ": null,
      "lenovoCustomerNumber": "",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "",
         "quantity": null,
         "state": "not installed",
      }],
      "partNumber": "",
      "purchaseOrder": "",
      "retrieveKeys": false,
      "salesOrder": "",
      "startDate": "",
   }],
   "customerInfo": {
      "companyNameInEnglish": "",
      "companyNameInLocalLanguage": "",
      "contactPhoneNumber": "",
      "contactEmailAddress": "",
      "customerAddress": "",
      "customerCity": "",
      "customerRegionStateOrProvince": "",
      "customerPostalCode": "",
      "country": "",
      "firstName": "",
      "lastName": "",
```

```
      "preferredLanguage": ""
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
authCodes	Array of objects	Information about each license-authorization code
authCode	String	License-authorization code ID
errorMsg	String	Message description
featureCode	String	License feature code
featureDescription	String	License feature description
keysRedeemed	Integer	Number of redeemed license-activation keys
keysRemaining	Integer	Number of available (not redeemed) license-activation keys
lenovoCustomerNumber	String	Lenovo customer number
licenseKeys	Array of objects	Information about each license-activation key
customerNumber	String	Lenovo customer number associated with the license-activation key
licenseKeyId	String	License-activation key ID
quantity	Integer	Number of redeemed licensees
state	String	License-activation key state. This can be one of the following values. • **installed**. The license-activation key is installed in XClarity Administrator. • **not installed**. The license-activation key is not installed.
partNumber	String	License part number
purchaseOrder	String	License purchase-order number
salesOrder	String	License sales-order number

Attributes	Type	Description
startDate	String	Date when the authorization code was created and the license validation period starts This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
customerInfo	Object	Information about the customer that is associated with the license-authorization codes
companyNameInEnglish	String	Customer company name in English
companyNameInLocalLanguage	String	Customer company name in local language
contactPhoneNumber	String	Customer phone number
contactEmailAddress	String	Customer email address
customerAddress	String	Customer physical address
customerCity	String	Customer city
customerRegionStateOrProvince	String	Customer state or region
customerPostalCode	String	Customer postal code
country	String	Customer country code For a complete list of country codes, use GET /licenseCountries.
firstName	String	Customer given name
lastName	String	Customer family name
preferredLanguage	String	Language code of the preferred language For a complete list of language codes, use GET /licenseCountries.

The following example is returned if the request is successful when ten of the remaining licenses in a single authorization code are redeemed


```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V11O0AID2K4",
      "errorMsg": "",
      "featureCode": "1341 contact",
      "featureDescription": "Lenovo XClarity Pro, Per Managed Endpoint w/5 Yr SW S&S",
      "keysRedeemed": 35,
      "keysRemaining ": 15,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "00001",
         "quantity": null,
         "state": "not installed",
      },
      {
         "customerNumber": "1234567890",
         "licenseKeyId": "00002",
         "quantity": null,
         "state": "not installed",
      }],
      "partNumber": "5641PX5",
      "purchaseOrder": "00000000",
```

```
      "salesOrder": "999999999",
      "startDate": "2020-06-02",
   }],
   "customerInfo": {
      "companyNameInEnglish": "Some Company",
      "companyNameInLocalLanguage": " Some Company ",
      "contactPhoneNumber": "9995551212",
      "contactEmailAddress": "jane.doe@somecompany.com",
      "customerAddress": "10 Main Street",
      "customerCity": "Rockville",
      "customerRegionStateOrProvince": "NY",
      "customerPostalCode": "12345",
      "country": "US",
      "firstName": "Jane",
      "lastName": "Doe",
      "preferredLanguage": "EN"
   }
}
```

The following example is returned if the request is successful when all remaining licenses for two authorization codes are redeemed.

```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V1100AID2K4",
      "errorMsg": "",
      "featureCode": "1341 contact",
      "featureDescription": "Lenovo XClarity Pro, Per Managed Endpoint w/5 Yr SW S&S",
      "keysRedeemed": 50,
      "keysRemaining ": 0,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "00001",
         "quantity": null,
         "state": "not installed"
      },
      {
         "customerNumber": "1234567890",
         "licenseKeyId": "00002",
         "quantity": null,
         "state": "not installed"
      }],
      "partNumber": "5641PX5",
      "purchaseOrder": "00000000",
      "salesOrder": "999999999",
      "startDate": "2020-06-02",
   },
   {
      "authCode": "YYA7BQ2V37V1100AID2K5",
      "errorMsg": "",
      "featureCode": "1341 contact",
      "featureDescription": "Lenovo XClarity Pro, Per Managed Endpoint w/5 Yr SW S&S",
      "keysRedeemed": 50,
      "keysRemaining ": 0,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "00113",
         "quantity": null,
         "state": "not installed"
      },
```

```
      {
         "customerNumber": "1234567890",
         "licenseKeyId": "00114",
         "quantity": null,
         "state": "not installed"
      }],
      "partNumber": "5641PX5",
      "purchaseOrder": "00000000",
      "salesOrder": "999999999",
      "startDate": "2020-06-02"
   }],
   "customerInfo": {
      "companyNameInEnglish": "Some Company",
      "companyNameInLocalLanguage": " Some Company ",
      "contactEmailAddress": "jane.doe@somecompany.com",
      "contactPhoneNumber": "9995551212",
      "customerAddress": "10 Main Street",
      "customerCity": "Rockville",
      "customerRegionStateOrProvince": "NY",
      "customerPostalCode": "12345",
      "country": "US",
      "firstName": "Jane",
      "lastName": "Doe",
      "preferredLanguage": "EN"
   }
}
```

PATCH /authCodes

Use this method to install or download license-activation keys for one or more authorization codes.

Note: This REST API requires Lenovo XClarity Administrator v3.5.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PATCH https://{management_server_IP}/authCodes`

Query parameters

None

Request body

- **Install license-activation keys in Lenovo XClarity Administrator**

Attributes	Required / Optional	Type	Description
authCodes	Optional	Array of objects	Information about each authorization code
authCode	Optional	String	License-authorization code ID
licenseKeys	Optional	Array of objects	Information about each license-activation key
licenseKeyId	Optional	String	License-key ID This attribute is idempotent (cannot be changed).

Attributes	Re-quired / Optional	Type	Description
customerNumber	Optional	String	Lenovo customer number associated with the license-activation key
quantity	Optional	Integer	Number of redeemed licenses
state	Optional	String	License-key state. This is always **installed**.

The following example install four license keys in Lenovo XClarity Administrator.

```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V11OOAID2K4",
      "licenseKeys": [{
         "licenseKeyId": "OOOO2",
         "state": "installed"
      },
      {
         "licenseKeyId": "OOOO3",
         "state": "installed"
      }]
   },
   {
      "authCode": "YYA7BQ2V37V11OOAID2K5",
      "licenseKeys": [{
         "licenseKeyId": "OOO25",
         "state": "installed"
      },
      {
         "licenseKeyId": "OOO32",
         "state": "installed"
      }]
   }]
}
```

- **Download license-activation keys to the local system**

Attributes	Re-quired / Optional	Type	Description
authCodes	Optional	Array of objects	Information about each authorization code
authCode	Optional	String	License-authorization code ID
licenseKeys	Optional	Array of objects	Information about each license key
licenseKeyId	Optional	String	License-key ID This attribute is idempotent (cannot be changed).
state	Optional	String	License-key state. This is always **downloaded**. The name and path of the license-activation keys file on the local system is returned in the "Location" field in the response header.

The following example downloads four license keys to the local system.

```
{
   "authCodes": [{
```

```
        "authCode": "YYA7BQ2V37V11OOAID2K4",
        "licenseKeys": [{
           "licenseKeyId": "OOOO2",
           "state": "downloaded"
        },
        {
           "licenseKeyId": "OOOO3",
           "state": "downloaded"
        }]
     },
     {
        "authCode": "YYA7BQ2V37V11OOAID2K5",
        "licenseKeys": [{
           "licenseKeyId": "OOO25",
           "state": "downloaded"
        },
        {
           "licenseKeyId": "OOO32",
           "state": "downloaded"
        }]
     }]
  }
```


Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

When **licenseKyes.state=downloaded**, a link to the license authorization-keys file is returned in the **Location** attribute in the response header.

```
Location: https://192.0.2.0/filename.zip
```

Response body

Attributes	Type	Description
response	Array of objects	Information about each license-activation key
result	String	Request status for the key
filename	String	File name for the license-activation keys

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "response": [{
      "result": "OK",
      "filename": "lnvgy_fod_0038_7777777777_anyos_noarch_00000011_1337.key"
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "explanation": "",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      }
   }]
}
```

/authCodes/*{code}*

Use this REST API to manage licenses for a specific license authorization code or modify customer information.

Note: This REST API requires Lenovo XClarity Administrator v3.5.0 or later.

HTTP methods

PUT, PATCH

PUT /authCodes/*{code}*

Use this method to redeem licenses from a single authorization code.

Lenovo XClarity Administrator sends a request to the Features on Demand web portal to redeem the licenses. The web portal creates a license-key file for each authorization code and downloads the files to the management server. Each license-key file contains the set of redeemed licenses for a specific authorization

code. You can then use the license-key file to apply licenses to the current XClarity Administrator, or you can import and install the downloaded license key file into another XClarity Administrator that might not have access to the Features on Demand web portal.

You can redeem all or a subset of licenses by specifying the **keysRedeemQty** request attribute. You must also specify the **authCode** attribute, **lenovoCustomerNumber** attribute, and ensure that **licenseKeys.state** is set to “not installed.”.

Note: This REST API requires Lenovo XClarity Administrator v3.5.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/authCodes/{code}`

where *{code}* is the authorization code ID which was sent to you in an *electronic proof of entitlement* email when you purchased the licenses.

Query parameters

None

Request body

This request updates the entire resource. If an optional attribute is set to an empty string, that attribute is not changed. If an idempotent (unchangeable) attribute is modified, an error is thrown.

Attributes	Required / Optional	Type	Description
authCodes	Optional	Object	Information about a single license-authorization code
authCode	Optional	String	License-authorization code ID
errorMsg	Optional	String	Message description This attribute is idempotent (cannot be changed).
featureCode	Optional	String	License feature code This attribute is idempotent (cannot be changed).
featureDescription	Optional	String	License feature description This attribute is idempotent (cannot be changed).
keysRedeemed	Optional	Integer	Number of redeemed license-activation keys This attribute is idempotent (cannot be changed).
keysRedeemQty	Optional	Integer	Number of redeemed license-activation keys
keysRemaining	Optional	Integer	Number of available (not redeemed) license-activation keys This attribute is idempotent (cannot be changed).
lenovoCustomerNumber	Optional	String	Lenovo customer number
licenseKeys	Optional	Array of objects	Information about each license-activation key
customerNumber	Optional	String	Lenovo customer number associated with the license-activation key

Attributes	Re-quired / Optional	Type	Description
licenseKeyId	Optional	String	License-activation-key ID This attribute is idempotent (cannot be changed).
quantity	Optional	Integer	Number of redeemed licenses
state	Optional	String	License-activation key state This attribute cannot be changed.
partNumber	Optional	String	License part number This attribute is idempotent (cannot be changed).
purchaseOrder	Optional	String	License purchase-order number This attribute is idempotent (cannot be changed).
retrieveKeys	Optional	Boolean	Indicates whether to retrieve license-activation keys. This can be one of the following values. • **true**. Retrieve license-activation keys. • **false**. (default) Do not retrieve license-activation keys.
salesOrder	Optional	String	License sales-order number This attribute is idempotent (cannot be changed).
startDate	Optional	String	Date when the authorization code was created and the license validation period starts This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage. This attribute is idempotent (cannot be changed).

The following example redeems ten of the remaining licenses in an authorization code.

```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V1100AID2K4",
      "errorMsg": "",
      "featureCode": "",
      "featureDescription": "",
      "keysRedeemed": null,
      "keysRedeemQty": "10",
      "keysRemaining ": null,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "",
         "quantity": null,
         "state": "not installed",
      }],
      "partNumber": "",
      "purchaseOrder": "",
      "retrieveKeys": false,
      "salesOrder": "",
      "startDate": "",
   }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
authCodes	Array of objects	Information about each license-authorization code
authCode	String	License-authorization code ID
errorMsg	String	Message description
featureCode	String	License feature code
featureDescription	String	License feature description
keysRedeemed	Integer	Number of redeemed license-activation keys
keysRemaining	Integer	Number of available (not redeemed) license-activation keys
lenovoCustomerNumber	String	Lenovo customer number
licenseKeys	Array of objects	Information about each license-activation key
customerNumber	String	Lenovo customer number associated with the license-activation key
licenseKeyId	String	License-activation key ID
quantity	Integer	Number of redeemed licensees
state	String	License-activation key state. This can be one of the following values. • **installed**. The license-activation key is installed in XClarity Administrator. • **not installed**. The license-activation key is not installed.
partNumber	String	License part number
purchaseOrder	String	License purchase-order number
salesOrder	String	License sales-order number
startDate	String	Date when the authorization code was created and the license validation period starts This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
customerInfo	Object	Information about the customer that is associated with the license-authorization codes

Attributes		Type	Description
	companyNameInEnglish	String	Customer company name in English
	companyNameInLocalLanguage	String	Customer company name in local language
	contactPhoneNumber	String	Customer phone number
	contactEmailAddress	String	Customer email address
	customerAddress	String	Customer physical address
	customerCity	String	Customer city
	customerRegionStateOrProvince	String	Customer state or region
	customerPostalCode	String	Customer postal code
	country	String	Customer country code For a complete list of country codes, use GET /licenseCountries.
	firstName	String	Customer given name
	lastName	String	Customer family name
	preferredLanguage	String	Language code of the preferred language For a complete list of language codes, use GET /licenseCountries.

The following example is returned if the request is successful.


```
{
   "authCodes": [{
      "authCode": "YYA7BQ2V37V11OOAID2K4",
      "errorMsg": "",
      "featureCode": "1341 contact",
      "featureDescription": "Lenovo XClarity Pro, Per Managed Endpoint w/5 Yr SW S&S",
      "keysRedeemed": 50,
      "keysRemaining ": 0,
      "lenovoCustomerNumber": "1234567890",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "00001",
         "quantity": null,
         "state": "not installed",
      },
      {
         "customerNumber": "1234567890",
         "licenseKeyId": "00002",
         "quantity": null,
         "state": "not installed",
      }],
      "partNumber": "5641PX5",
      "purchaseOrder": "00000000",
      "salesOrder": "999999999",
      "startDate": "2020-06-02",
   }],
   "customerInfo": {
      "companyNameInEnglish": "Some Company",
      "companyNameInLocalLanguage": " Some Company ",
      "contactPhoneNumber": "9995551212",
      "contactEmailAddress": "jane.doe@somecompany.com",
      "customerAddress": "10 Main Street",
      "customerCity": "Rockville",
```

```
      "customerRegionStateOrProvince": "NY",
      "customerPostalCode": "12345",
      "country": "US",
      "firstName": "Jane",
      "lastName": "Doe",
      "preferredLanguage": "EN"
   }
}
```

PATCH /authCodes/*{code}*

Use this method to install or download license-activation keys for a specific authorization code.

Note: This REST API requires Lenovo XClarity Administrator v3.5.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PATCH https://{management_server_IP}/authCodes/{code}/licenseKeys`

where *{code}* is the authorization code ID which was sent to you in an *electronic proof of entitlement* email when you purchased the licenses.

Query parameters

None

Request body

- **Install license-activation keys in Lenovo XClarity Administrator**

Attributes	Required / Optional	Type	Description
authCodes	Optional	Object	Information about each authorization code
authCode	Optional	String	License-authorization code ID
licenseKeys	Optional	Array of objects	Information about each license key
customerNumber	Optional	String	Lenovo customer number associated with the license-activation key
licenseKeyId	Optional	String	License-key ID This attribute is idempotent (cannot be changed).
quantity	Optional	Integer	Number of redeemed licenses
state	Optional	String	License-key state. This is always **installed**.

The following example install four license keys in Lenovo XClarity Administrator

```
{
   "authCodes": {
      "authCode": "YYA7BQ2V37V1100AID2K4",
      "licenseKeys": [{
         "customerNumber": "1234567890",
         "licenseKeyId": "00002",
```

```
            "quantity": 10,
            "state": "installed"
         },
         {
            "customerNumber": "1234567890",
            "licenseKeyId": "00003",
            "quantity": 10,
            "state": "installed"
         }
      }]
}
```

- **Download license-activation keys to the local system**

Attributes	Re-quired / Optional	Type	Description
authCodes	Optional	Object	Information about each authorization code
authCode	Optional	String	License-authorization code ID
licenseKeys	Optional	Array of objects	Information about each license key
licenseKeyId	Optional	String	License-key ID This attribute is idempotent (cannot be changed).
state	Optional	String	License-key state. This is always **downloaded**. The name and path of the license-activation keys file on the local system is returned in the "Location" field in the response header.

The following example downloads four license keys to the local system.

```
{
   "authCodes": {
      "authCode": "YYA7BQ2V37V1100AID2K4",
      "licenseKeys": [{
         "licenseKeyId": "00002",
         "state": "downloaded"
      },
      {
         "licenseKeyId": "00003",
         "state": "downloaded"
      }]
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Information about each license-activation key
result	String	Request status for the key
filename	String	File name for the license-activation keys
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "response": [{
      "result": "OK",
      "filename": "lnvgy_fod_0038_7777777777_anyos_noarch_00000011_1337.key"
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "explanation": "",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      }
   }]
}
```

/files/managementServer/updates?action=import&jobid=*{job_id}*

Use this REST API to import a management-server update into the updates repository.

HTTP methods

POST

POST /files/managementServer/updates?action=import&jobid={job_id}

Use this method to import a management-server update to the updates repository. Only the user that created the job has the permission to import the update using the job ID that was returned from that method.

Before you can import an update, you must first create an import job using the POST /managementServer/updates?action=import method.

You can monitor the status of the import request using the GET /tasks/*{job_list}* method.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/files/managementServer/updates?action=import&jobid={job_id}
```

Query parameters

Parameters	Required / Optional	Description
jobid=*{job_id}*	Required	The ID of the job that was created to import images using the last POST /managementServer/updates?action=import method

The following example imports a management-server update using job ID 1.

```
POST https://192.0.2.0/files/managementServer/updates?action=import&jobid=1
```

Request body

Use the "multipart/form-data" media type to import the update package. Use the attributes in the following table as the multipart name in the body. For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage.

Attributes	Required / Optional	Type	Description
fileSize	Optional	String	Size of the update file to be imported (in bytes)
uploadedfile	Required	Object	Information about the image being imported
fileName	Required	String	Name of the update file

The following example imports a management-server update.

HTTP Header

```
Content-Type: multipart/form-data; boundary=AaB03x
```

Request body

```
--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                        filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.chg"
   Content-Type: application/octet-stream
```

```
--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                        filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.tgz"
   Content-Type: application/x-compressed

--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                         filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.txt"
   Content-Type: text/plain

--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                         filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.xml"
   Content-Type: text/xml

--AaB03x--
```

Response codes

Code	Description	Comments
201	Created	One or more new resources were successfully created.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful. You can use the GET /tasks/*{job_list}* resource to monitor the progress of the deployment.

```
{
   "result": "success",
   "messages":[]
}
```

The following example is returned if the request is not successful (such as a response code of 409).

```
{
   "result": "failed",
   "errorMsg": {
      "result": "major",
      "messages": [{
         "explanation": "The operation failed for an unknown reason.  The network connection
                         might have gone down",
         "id": "FQXHMUP2502L",
         "recovery": {
            "text": "Check the network connection.  Retry the operation."
         },
         "text": "The repository operation failed."
      }]
   }
}
```

/files/stgupdates/repository/import/SELF

Use this REST API to import a management-server update into the updates repository without using a job.

HTTP methods

POST

POST /files/stgupdates/repository/import/SELF

Use this method to import a management-server update to the updates repository without using a job.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/files/stgupdates/repository/import/SELF`

Query parameters

None

Request body

Use the "multipart/form-data" media type to import the update package. Use the attributes in the following table as the multipart name in the body. For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage. For example:

HTTP Header

```
Content-Type: multipart/form-data; boundary=AaB03x
```

Request body

```
--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                         filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.chg"
   Content-Type: application/octet-stream

--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                        filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.tgz"
   Content-Type: application/x-compressed
```

```
--AaBO3x
   Content-Disposition: form-data; name="uploadedfiles[]";
                        filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.txt"
   Content-Type: text/plain

--AaBO3x
   Content-Disposition: form-data; name="uploadedfiles[]";
                        filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.xml"
   Content-Type: text/xml

--AaBO3x--
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
current	String	
downloadedsize	Integer	
downloadednum	Integer	
progress	Integer	Job progress, where `100` is complete, and less than `100` is in progress
state	String	State of the import process. This can be one of the following values. • **success**. The request completed successfully. • **error**. The request failed. A descriptive error message is returned.
total	Integer	
totalsize	Integer	
updates	Array	
popMsg	Array	Indicates that some files are not applicable for virtual-appliance updates repository
result	String	Result of the request. This can be one of the following values. • **warning**
messages	Object	Information about one or more messages
id	String	Message identifier of a returned message
explanation	String	
recovery	Array	
text	String	
text	String	Message text that is associated with the message identifier

Attributes	Type	Description
errorMsg	Array	Information about one or more messages
result	String	Result of the request. This can be one of the following values. • **informational**. The request completed successfully.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text that is associated with the message identifier

The following example is returned if the request is successful.

```
{
   "current": "",
   "downloadednum": 0
   "downloadedsize": 0,
   "progress": 0,
   "state": "success",
   "total": 0,
   "totalsize": 1,
   "updates": [],
   "popMsg": {
      "result": "warning",
      "messages": [{
         "id": "FQXHMUP2512F",
         "text": "Import complete",
         "explanation": "The following files are not applicable to the updates
                         process; they have been discarded: newFile.txt.",
         "recovery": {
            "text": "Discarded packages are not referenced by any .xml file
                     currently in Firmware Updates Repository. Ensure your
                     uploaded files include the correct .xml file."
         }
      }]
   },
   "errorMsg": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   }
}
```

/files/stgupdates/repository/import/validate/SELF

Use this REST API to verify that Lenovo XClarity Administrator has sufficient disk space to import management-server update files.

HTTP methods

POST

POST /files/stgupdates/repository/import/validate/SELF

Use this method to verify that Lenovo XClarity Administrator has sufficient disk space to import management-server update files.

If you specify this attribute, this method starts a job that runs in the background to perform the operation. The response body includes the ID of the job that was created to perform this request. Use POST /files/stgupdates/repository/import/SELF?jobid=*{job_id}* to start the import job.. If a job was not successfully started, refer to the response code and response body for details.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/files/stgupdates/repository/import/validate/SELF`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
files	Required	Array of objects	Information about each file to import
index	Optional	String	Array index
name	Required	String	File name
size	Required	Long	File size
type	Optional	String	File type. This can be one of the following values. • **text** • **binary**

The following example check the file size before importing updates.

```
{
    "files": [{
        "index": 0,
        "name": "filename.txt",
        "size": 8192,
        "type": "text/plain"
    }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
current	String	
downloadednum	Integer	
downloadedsize	Integer	
progress	Integer	Job progress, where `100` is complete, and less than `100` is in progress
state	String	This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned.
total	Integer	
totalsize	Integer	
updates	Array	
errorMsg	Array	Information about one or more messages
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned. • **informational**.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text that is associated with the message identifier

The following example is returned if the request is successful.

```
{
    "current": "",
    "downloadednum": 0
    "downloadedsize": 0,
    "progress": 0,
    "state": "success",
    "total": 0,
    "totalsize": 0,
    "updates": [],
    "errorMsg": {
        "result": "informational",
        "messages": [{
            "id": "FQXHMUP2500I",
            "text": "Repository operation completed successfully."
        }]
    }
}
```

/files/stgupdates/repository/import/SELF?jobid={*job_id*}

Use this REST API to import a management-server update to the updates repository. Only the user that created the job has the permission to import the update using the job ID that was returned from that method.

HTTP methods

POST

POST /files/stgupdates/repository/import/SELF?jobid=*{job_id}*

Use this method to import a management-server update to the updates repository. Only the user that created the job has the permission to import the update using the job ID that was returned from that method.

Before you can import an update, you must first create an import job using the POST /files/stgupdates/repository/import/validate/SELF method.

You can monitor the status of the import request using the GET /tasks/*{job_list}* method.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/files/stgupdates/repository/import/SELF?jobid={job_id}
```

Query parameters

Parameters	Required / Optional	Description
jobid=*{job_id}*	Required	ID of the job that was created to import images using the last POST /files/stgupdates/repository/import/validate/SELF method

The following example imports a management-server update using job ID 1.

```
POST https://192.0.2.0/files/stgupdates/repository/import/SELF?jobid=1
```

Request body

Use the "multipart/form-data" media type to import the update package. Use the attributes in the following table as the multipart name in the body. For more information about the multipart/form-data media type, see Returning Values from Forms: multipart/form-data webpage.

Attributes	Required / Optional	Type	Description
fileSize	Optional	String	Size of the update file to be imported (in bytes)
uploadedfile	Required	Object	Information about the image being imported
fileName	Required	String	Name of the update file

The following example imports a management-server update.

HTTP Header

```
Content-Type: multipart/form-data; boundary=AaB03x
```

Request body

```
--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                         filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.chg"
   Content-Type: application/octet-stream

--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                        filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.tgz"
```

```
   Content-Type: application/x-compressed

--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                        filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.txt"
   Content-Type: text/plain

--AaB03x
   Content-Disposition: form-data; name="uploadedfiles[]";
                        filename="lnvgy_sw_lxca_serverrepo2-1.1.1_anyos_noarch.xml"
   Content-Type: text/xml

--AaB03x--
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
current	String	
downloadednum	Integer	
downloadedsize	Integer	
progress	Integer	Job progress, where `100` is complete, and less than `100` is in progress
state	String	This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned.
total	Integer	
totalsize	Integer	
updates	Array	
errorMsg	Array	Information about one or more messages
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned. • **informational**.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text that is associated with the message identifier

The following example is returned if the request is successful.

```
{
    "current": "",
    "downloadednum": 0
```

```
    "downloadedsize": 0,
    "progress": 0,
    "state": "success",
    "total": 0,
    "totalsize": 0,
    "updates": [],
    "errorMsg": {
        "result": "informational",
        "messages": [{
            "id": "FQXHMUP2500I",
            "text": "Repository operation completed successfully."
        }]
    }
}
```


/licenseCompliance

Use this REST API to retrieve information about whether Lenovo XClarity Administrator is license compliant.

HTTP methods

GET

GET /licenseCompliance

Use this method to return information about whether Lenovo XClarity Administrator is license compliant.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/licenseCompliance`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
response	Array of objects	Information about compliance for each license
compliant	Integer	Indicates whether XClarity Administrator is compliant with installed licenses. This can be one of the following values. • **0**. XClarity Administrator is not compliant. • **1**. XClarity Administrator is compliant. • **2**. XClarity Administrator is registered.
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "response": [{
      "compliant": 1
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```

/licenseCountries

Use this REST API to return a list of countries and languages that can be for customer information associated with licenses.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

HTTP methods

GET

GET /licenseCountries

Use this REST API to return a list of countries and languages that can be for customer information associated with licenses.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/licenseCountries
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
countries	Array of objects	Information about each country
desc	String	Country description
value	String	Country code
languages	Array of objects	Information about each language
desc	String	Language description
value	String	Language code

The following example is returned if the request is successful.

```
{
   "countries" :[
```

```
      { "desc": "China", "value": "CN" },
      { "desc": "UnitedKingdom", "value": "GB" }
      ...,
   ],
   "languages" :[
      { "desc": "Chinese-traditional", "value": "ZN" },
      { "desc": "English", "value": "EN" },
      ...,
   ]
}
```

/registration

Use this REST API to return information about the Lenovo XClarity Administrator registration status, register XClarity Administrator, or import the registration token.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

HTTP methods

GET, POST, PUT

GET /registration

Use this method to return information about the Lenovo XClarity Administrator registration status.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/registration`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
company	String	Company name
country	String	Country code for the location of the management server To obtain the country code, use GET /registration/countries.
deviceCount	Integer	Number of managed devices
status	Integer	Indicates status information about whether the system has free license registered • **0**. Not registered • **1**. Registered
token	String	Registration token If a token is not installed, this value is null.

The following example is returned if the request is successful.

```
{
   "company": "Some Company",
   "country": "us",
   "deviceCount": 250,
   "status": 1,
   "token": "ODF4-0110-E231"
}
```

POST /registration

Use this method to send a registration request to the Lenovo eSupport website and return the registration status and token.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/registration`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
company	Required	String	Company name
country	Required	String	Country code for the location of the management server To obtain the country codes, use GET /utils/countries.
deviceCount	Required	Integer	Number of managed devices

The following example registers a company for a free license.

```
{
   "company": "Some Company",
```

```
   "country": "us",
   "deviceCount": 250
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
408	Request Timeout	The orchestrator server did not receive a required request in a specific amount of time. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

PUT /registration

Use this method to import the registration token in the management server.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/registration`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
token	Required	String	Free-license registration token If you registered Lenovo XClarity Administrator using the REST API, this token is returned by POST /registration. If you registered using the Lenovo XClarity Registration web portal, the token is returned when you complete the registration.

The following example installs the free-license registration token.

```
{
   "token": "ODF4-0110-E231"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/registration/countries

Use this REST API to return a list of country and region codes that can be used during the registration process.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

HTTP methods

GET

GET /registration/countries

Use this method to return a list of country and region codes that can be used during the registration process.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/registration/countries`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
message	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
body	Array of objects	Information about each country or region
Text	String	Country or region name
Value	String	Two-letter ISO 3166 code for the country or region

The following example is returned if the request is successful.

```
{
   "message": "succeed",
   "body": [{
      "Text": "ANGOLA",
      "Value": "AO"
   },
   {
      "Text": "ARGENTINA",
       "Value": "AR"
   },
   ...,
   {
      "Text": "ZAMBIA",
      "Value": "ZM"
   },
   {
      "Text": "ZIMBABWE",
      "Value": "ZW"
   }]
}
```

/registration/details

Use this REST API to return information about the registration settings.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

HTTP methods

GET

GET /registration/details

Use this method to return information about the registration settings.

Note: This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/registration/details`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
compliant	Integer	Indicates whether XClarity Administrator is compliant with installed licenses. This can be one of the following values. • **0**. XClarity Administrator is not compliant. • **1**. XClarity Administrator is compliant. • **2**. XClarity Administrator is registered.
freeOfWarning	Integer	Indicates whether XClarity Administrator is registered and license warnings are suppressed. This can be one of the following values. • **0**. XClarity Administrator is not registered. License warnings are displayed. • **1**. XClarity Administrator is registered. Licenses warnings are suppressed.

The following example is returned if the request is successful.

```
{
   "compliant": 2,
   "freeOfWarning": 1
}
```

/managementServer/updates

Use this REST API to retrieve information about all updates in the management-server updates repository, retrieve status for all management-server updates that are in progress, or manage management-server updates in the repository or to apply an update to the management server.

HTTP methods

GET, POST, PUT

GET /managementServer/updates

Use this method to return information about all updates in the management-server updates repository.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/managementServer/updates
```

Query parameters

Parameters	Required / Optional	Description
key=*{value}*	Optional	Returns the specified type of information for all management-server update-related tasks that are in progress. This can be one of the following values. • **all**. (default) Returns all information. • **currentVersion**. Returns the current version of XClarity Administrator. • **history**. Returns the history of management-server updates. • **importDir**. Returns the directory for the management-server updates repository. • **size**. Returns the repository size (in bytes). • **updates**. Returns information about all updates packages. • **updatedDate**. Returns the date when the last update was performed.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
history	Object	Information about the management-server update history
buildNumber	String	Update build number
dateApplied	String	Timestamp when the update was applied
description	String	Short description of the update
detailInfo	String	Detailed description of the update
fileName	String	Update file name

Attributes	Type	Description
flavor	String	Type of update. This can be one of the following values. • **base install**. The initial installation of XClarity Administrator code changes. • **license enablement**. License for full-function entitlement. • **patch**. XClarity Administrator code changes, including new releases and fix packs • **supplemental pack**. Firmware-update repository packs, which contain firmware update packages for all manageable devices. When imported and applied, the firmware updates are added in the firmware-updates repository.
installationFailedDate	String	Timestamp when the update was applied and failed
version	String	XClarity Administrator version
importDir	String	Directory of the management-server updates repository
size	Object	Information about the size of the management-server updates repository
allotment	Long	Amount of space that is reserved for the repository
firmwareRepoUsage	Long	Amount of used space, in bytes, in the firmware updates repository
highusage	String	Used capacity. This can be one of the following values. • **high**. 85% capacity or higher • **medium**. 50% capacity or higher • **low**. 49% or lower
selfRepoUsage	Long	Amount of used space, in bytes, in the XClarity Administrator updates repository
upperLimitSpace	Long	Maximum amount of space, in GB, that can be allocated to the updates repository (including firmware, OS device drivers, and management server updates) The minimum size is 50 GB. The maximum size is dependent on the amount of disk space on the local system.
usedSpace	Long	Amount of used space
windowsDriverRepoUsage	Long	Amount of used space, in bytes, in the Windows device-drivers repository
updatedDate	String	Timestamp for the last applied update
updates	Array of objects	Information about the latest applied update
applied	String	Applied status. This can be one of the following values. • **applied**. The update was successfully applied. • **not applied**. The update was not applied.
buildNumber	String	Update build number
fixid	String	ID of the update package

Attributes	Type	Description
flavor	String	Type of update. This can be one of the following values. • **base install**. The initial installation of XClarity Administrator code changes. • **license enablement**. License for full-function entitlement. • **patch**. XClarity Administrator code changes, including new releases and fix packs • **supplemental pack**. Firmware-update repository packs, which contain firmware update packages for all manageable devices. When imported and applied, the firmware updates are added in the firmware-updates repository.
id	Integer	ID of the update
payload	String	File name of the update package
readableName	String	Detailed description of the update
rebootRequired	Boolean	Identifies whether the update requires the management server to be rebooted. This can be one of the following values. • **true**. The update requires a reboot. • **false**. The update does not require a reboot.
releasedate	String	Date when the update was released
size	Long	Size of the update package file
status	String	Update-package status. This can be one of the following values. • **acquired**. The entire update package is stored in the repository. • **not acquired**. The update package was not downloaded to the repository.
title	String	Name of the update
version	String	Version of the update
version	String	Version of the currently installed updated

The following example is returned if the request is successful.


```
{
   "history": [{
      "buildNumber": "173",
      "dateApplied": "06-16-2016-19:04",
      "description": "base install",
      "detailInfo": "Base Install",
      "fileName": "Base Install",
      "flavor": "base install",
      "installationFailedDate": "06-16-2016-19:04",
      "version": "1.2.0"
   },
   {
      "buildNumber": "SWITCH-01",
      "dateApplied": "06-16-2016-19:21",
      "description": "TBD",
      "detailInfo": "Lenovo XClarity Administrator Repository Pack for Flex CMM and Switches",
      "fileName": "lnvgy_sw_lxca-fw-cmm-switch-repository-pack_1-1.2.0_anyos_noarch",
      "flavor": "supplement pack",
      "installationFailedDate": "06-16-2016-19:21",
      "version": "Version 1.2.0-[SWITCH-01-1.2.0]-"
   }],
   "importDir": "\/opt\/lenovo\/lxca\/data\/updates\/self",
```

```
   "size": {
      "allotment": 53687091200,
      "firmwareRepoUsage": 34685248291,
      "highusage": "high",
      "selfRepoUsage": 97299561694,
      "upperLimitSpace": 158230491136,
      "usedSpace": 133804243686,
      "windowsDriverRepoUsage": 1819433701
   },
   "updatedDate": "06-22-2016-19:47",
   "updates": [{
      "applied": "Applied",
      "buildNumber": "SWITCH-01",
      "datainfo": "Info",
      "fixid": "lnvgy_sw_lxca-fw-cmm-switch-repository-pack_1-1.2.0_anyos_noarch",
      "flavor": "supplement pack",
      "id": 1,
      "payload": "lnvgy_sw_lxca-fw-cmm-switch-repository-pack_1-1.2.0_anyos_noarch.tgz",
      "readableName": "Lenovo XClarity Administrator Repository Pack for Flex CMM and Switches",
      "releasedate": "2016-06-03",
      "size": 4091905320,
      "status": "Acquired",
      "title": "lnvgy_sw_lxca-fw-cmm-switch-repository-pack_1-1.2.0_anyos_noarch",
      "version": "Version 1.2.0-[SWITCH-01-1.2.0]-"
   }],
   "version": "1.2.0"
}
```


PUT /managementServer/updates

Use this method to install a management-server update.

This method starts a job to perform the operation. The response body includes a job ID that represents the job that is monitored by the management server. You can use GET /tasks/*{job_list}* to determine the status of the job. If a job was not successfully started, refer to the response code and response body for details.

To cancel the request, use GET /tasks/*{job_list}*, where *{job_id}* is the ID that is returned by this request.

Attention: A successful response indicates that the request was successfully transmitted and accepted by the management server. It does not indicate that the operation that is associated with the job was successful.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/managementServer/updates`

Query parameters

Parameters	Required / Optional	Description
action=apply	Required	Installs the specified management-server updates.

The following example applies a specific update to the management server.

```
PUT https://192.0.2.0/managementServer/updates?action=apply
```

Request body

Attributes	Required / Optional	Type	Description
fixids	Required	Array of strings	Update ID. You can specify only one update ID. To obtain the update UUID, use the GET /chassis method.

The following example installs a management-server update.

```
{
   "fixids": ["lnvgy_sw_lxca_222-1.2.0_anyos_noarch"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
jobid	String	Job ID
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
errorMsg	Object	Information about one or more messages
messages	Array of objects	Information about a message
id	String	Message identifier of a returned message.
recovery	Object	
text	String	
text	String	Message text associated with the message identifier.
result	String	Results of the request. This can be one of the following values. • **informational**. • **warning**.

The following example is returned if the request is successful.

```
{
   "jobid": "5",
   "result": "success",
   "errorMsg": {
```

```
      "messages": [{
         "id": "FQXHMUP2508I",
         "text": "The operation has started successfully."
      }],
      "result": "informational"
   }
}
```


POST /managementServer/updates

Use this method to manage management-server updates in the updates repository.

When the **action=import** query parameter is specified, this method creates a job that can be used to import a management-server update package into the updates repository. The method returns the job ID, which you can then use with the POST /files/managementServer/updates?action=import&jobid=*{job_id}* method.

To import a management-server update package into the updates repository, follow these steps:

1. Start a job to import the update using POST /managementServer/updates?action=import.
2. Import the update using POST /files/managementServer/updates?action=import&jobid=*{job_id}* method, where the job ID is the ID that was returned in step 1.
3. Monitor the status of the import job using GET /tasks/*{job_list}*, where the job ID is the ID that was returned in step 1. You can also cancel the import job using this method.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/managementServer/updates`

Query parameters

Parameters	Required / Optional	Description
action=*{action}*	Required	Action to take. This can be one of the following values. • **acquire**. Downloads the specified management-server update packages from the Lenovo XClarity Support website. • **import**. Creates a job to import one or more management-server updates. • **refresh**. Retrieves information (metadata) about the latest available management-server updates from the Lenovo XClarity Support website.

The following example downloads management-server update packages to the management-server updates repository

`POST https://192.0.2.0/managementServer/updates?action=acquire`

The following example import management-server updates from the local system.

`POST https://192.0.2.0/managementServer/updates?action=import`

Request body

Attributes	Required / Optional	Type	Description
mts	Required if action=refresh	Array of strings	For management-server updates, this is always “lxca.”
fixid	Required if action=acquire	Array of strings	UUIDs of one or more update packages, separated by a comma. To obtain the update UUIDs, use the GET /chassis method.
size	Optional	Long	Total size, in bytes, of the file to be imported

The following example downloads a management-server update package from the web when **action=refresh**.

```
{
   "mts": ["lxca"],
}
```

The following example downloads multiple updates to the management server when **action=acquire**.

```
{
   "fixids": ["lnvgy_sw_lxca_222-1.2.0_anyos_noarch,
               lnvgy_sw_lxca_cmmswitchrepo1-1.2.0_anyos_noarch"]
}
```

The following example imports a 1234567-byte update package when **action=import**.

```
{
   "size": 1234567
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
jobid	String	Job ID
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
errorMsg	Object	Information about one or more messages

Attributes	Type	Description
messages	Array of objects	Information about a message
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
result	String	Results of the request. This can be one of the following values. • **informational** • **warning**

The following example is returned if the request is successful.

```
{
   "jobid": "5",
   "result": "success",
   "errorMsg": {
      "messages": [{
         "id": "FQXHMUP2508I",
         "text": "The operation has started successfully."
      }],
      "result": "informational"
   }
}
```

/managementServer/updates/*{fix_id_list}*

Use this REST API to retrieve information or the readme or change history file for a specific update in the management-server updates repository.

HTTP methods

GET, DELETE

GET /managementServer/updates/*{fix_id_list}*

Use this method to return information or the readme or change history file for a specific update in the management-server updates repository.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/managementServer/updates/`
{fix_id_list}

Where *{fix_id_list}* is the ID of one or more update packages, separated b y a comma. You can specify one or more IDs, separated by a comma. To obtain the update UUID, use the GET /chassis method.

Query parameters

You can specify one of the following query parameters, but both at the same time.

Parameters	Required / Optional	Description
key=*{value}*	Optional	Returns the specified type of information for a specific management-server update. This can be one of the following values. • **all**. (default) Returns all information. • **actions**. Returns the actions that are supported by the specified update. • **keys**. Returns the specified key values. • **filetypes**. Returns the file types that are supported by the specified update. • **update**. Returns information about the update package.
filetype=*{type}*	Optional	Returns the readme or change history file. This can be one of the following values. • **changeHistory**. Returns the change-history file for the specified management-server update. • **readme**. Returns the readme file for the specified management-server update

The following example returns all information about multiple specific updates.

```
GET https://192.0.2.0/managementServer/updates/
lnvgy_sw_lxca_222-1.1.0_anyos_noarch,lnvgy_sw_lxca_222-1.2.0_anyos_noarch
```

The following example returns the status a specific update.

```
GET https://192.0.2.0/managementServer/updates/
lnvgy_sw_lxca_222-1.2.0_anyos_noarch?action=status
```

The following example returns the readme file for a specific update.

```
GET https://192.0.2.0/managementServer/updates/
lnvgy_sw_lxca_222-1.2.0_anyos_noarch?filetype=readme
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Table 73. Returns key values

Attributes	Type	Description
actions	Object	Information about the actions that are supported by the specified update.
action	String	Action to take. This can be one of the following value. • **acquire**. • **apply**. • **delete**.
filetypes	String	File types that are supported by the specified update
keys	Object	Information about the specified key values
key	String	Key values for this request. This can be one of the following values. • **all**. (default) Returns all information. • **actions**. Returns the actions that are available for the specified update. • **keys**. Returns the specified key values. • **filetypes**. Returns the file types that are available for the specified update. • **update**. Returns information about the update package.
update	Array of objects	Information about the update package
applyable	String	Identifies whether the management-server update can be installed. This can be one of the following values. • **true**. • **false**.
buildNumber	String	Update package build number
buildType	String	Build type
change	String	Identifies whether a change-history file exists in the update package. This can be one of the following values. • **true**. A change-history file exists. • **false**. A change-history file does not exist.
comp	String	Component name that is defined in the XML file • **Utility**.
downloadedsize	Integer	Size of the downloaded update package
errorMsg	String	Error message when downloading
fixid	String	Update package ID
latest	String	Indicates whether the update package is the latest package for the component in the repository for the components. This can be one of the following values. • **true**. • **false**.
name	String	Update package name
origin	String	
payload	String	Identifies whether a payload file exists in the update package This can be one of the following values. • **true**. A payload file exists. • **false**. A payload file does not exist.

Table 73. Returns key values (continued)

Attributes		Type	Description
	payloadFilename	String	Name of the payload file
	percentage	Integer	Download percentage if the package is downloading
	readableName	String	Package readable name (for example, such as Lenovo XClarity Administrator Pack for Flex CMM and Switches)
	readme	String	Identifies whether a readme file exists in the update package. This can be one of the following values. • **true**. A readme file exists. • **false**. A readme file does not exist.
	releasedate	String	Date when the update package was released
	severity	Integer	Update severity. This can be one of the following values. • **initialRelease**. This is the first release of the firmware. • **critical**. The firmware release contains urgent fixes for data corruption, security, or stability issue. • **suggested**. The firmware release contains significant fixes for problems that you are likely to encounter. • **noncritical**. The firmware release contains minor fixes, performance enhancements, and textual changes.
	state	String	Package status
	supportDownload	String	Indicates whether the update package can be downloaded from the web. This can be one of the following values. • **true**. • **false**.
	totalsize	Long	Total size of the update package
	version	String	Update package version

The following example returns information about a specific management-server update.

```
{
   "actions": [
      {"action": "acquire"},
      {"action": "apply"},
      {"action": "delete"}
   ],
   "filetypes": ["change", "readme"],
   "keys": [
      {"key": "actions"},
      {"key": "update"},
      {"key": "filetypes"},
      {"key": "keys"}
   ],
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }]
   },
   "update": [{
      "applyable": "false",
      "buildNumber": "SWITCH-01",
```

```
      "buildType": "production",
      "change": "true",
      "comp": "Utility",
      "downloadedsize": 0,
      "errorMsg": "",
      "fixid": "lnvgy_sw_lxca_cmmswitchrepo1-1.1.0_anyos_noarch",
      "latest": "false",
      "name": "",
      "origin": "lnvgy_sw_lxca_cmmswitchrepo1-1.1.0_anyos_noarch.xml",
      "payload": "false",
      "payloadFilename": "",
      "percentage": 0,
      "readableName": "Lenovo XClarity Administrator Repository Pack for Flex CMM and Switches",
      "readme": "true",
      "releasedate": "2016-04-21",
      "severity": 2,
      "state": "",
      "supportDownload": "true",
      "totalsize": 3846590000,
      "version": "1.1.0"
   }]
}
```


Table 74. Returns file types that are supported by the specified update

Attributes	Type	Description
field	String	File type. This can be one of the following values. • **changeHistory**. Returns the change-history file for the specified management-server update. • **readme**. Returns the readme file for the specified management-server update.
fixid	String	UUID of the update package
status	Object	Information about one or more messages
messages	Array of objects	Message
id	String	Identifier of a returned message
text	String	Text associated with the message identifier
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned.
value	String	Contents of the file

The following example returns the readme for the specified update.


```
{
   "field": "readme",
   "fixid": "lnvgy_sw_lxca_222-1.2.0_anyos_noarch",
   "status": {
      "result": "informational",
      "messages": [{
         "id": "FQXHMUP2500I",
         "text": "Repository operation completed successfully."
      }],
      "value": "Lenovo XClarity Administrator Virtual Appliance 1.2.0
```

```
                Installation README File

                Version 1.2.0 Build 222

                (C) Copyright Lenovo Corporation 2015, 2016.
                LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered
                pursuant a General Services Administration "GSA" contract, use,
                reproduction, or disclosure is subject to restrictions set forth in
                Contract No. GS-35F-05925.

                CONTENTS
                --------
                1.0 Overview
                2.0 Installation and Setup Instructions
                3.0 Web Sites and Support Phone Number
                4.0 Trademarks and Notices
                5.0 Disclaimer

                1.0 Overview

                1.1 This README file contains the latest information about installing the
                    XClarity Administrator virtual appliance update package.

                1.2 Limitations:

                - This update only applies to the 1.0 and 1.1 release families of
                  XClarity Administrator.

                1.3 Enhancements:

                - Refer to the change history file lnvgy_sw_lxca_222-1.2.0_anyos_noarch.chg
                  for a history of enhancements and fixes.

                1.4 Recommendations and Prerequisites for the Updates:
                ..."
   }
}
```


DELETE /managementServer/updates/*{fix_id_list}*

Use this method to delete update packages and metadata from the management-server updates repository.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/managementServer/updates/{fix_id_list}`

Where *{fix_id_list}* is the ID of one or more update packages, separated b y a comma. You can specify one or more IDs, separated by a comma. To obtain the update UUID, use the GET /chassis method.

Query parameters

Parameters	Required / Optional	Description
key=removeMetadata	Optional	Identifies whether to delete the management-server update package and metadata If not specified, the update packages are deleted and the metadata is not deleted.

The following example deletes a specific management-server update package but not the metadata.

```
DELETE https://192.0.2.0/managementServer/updates/lnvgy_sw_lxca_cmmswitchrepo1-1.1.0_anyos_noarch
```

The following example deletes a specific management-server update package and the associated metadata.

```
DELETE https://192.0.2.0/managementServer/updates/lnvgy_sw_lxca_cmmswitchrepo1-1.1.0_anyos_noarch
?key=removeMetadata
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
errorMsg	Object	Information about one or more messages
messages	Array of objects	Message
id	String	ID of a returned message
text	String	Text associated with the message ID
result	String	Results of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message is returned.

The following example is returned if the request is successful.

```
{
   "result": "success",
   "errorMsg": {
```

```
      "messages": [{
         "id": "FQXHMUP2508I",
         "text": "The operation has started successfully."
      }],
      "result": "informational"
   }
}
```

/notificationsLicense

Use this REST API to retrieve information about warnings regarding non-compliance of installed licenses.

HTTP methods

GET

GET /notificationsLicense

Use this method to return information about warnings regarding non-compliance of installed licenses.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/notificationsLicense`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
413	Request Entity Too Large	Clients might impose limitations on the length of the request URI, and the request URI is too long to be handled. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
response	Array of objects	Information about non-compliance for each license
accepted_eula	String	Indicates whether the end-user license agreement was accepted. This can be one of the following values. • **0**. License agreement was not accepted. • **1**. License agreement was accepted.
active_entitlements	String	Total number of active licenses
compliant	String	Indicates whether XClarity Administrator is compliant with installed licenses. This can be one of the following values. • **0**. XClarity Administrator is not compliant with installed licenses. The number of devices exceeds the permissible limit. • **1**. XClarity Administrator is compliant with installed licenses. The number of devices does not exceed the license limit. • **2**. XClarity Administrator is compliant with installed licenses. The number of devices exceeds the license limit but does not exceed the permissible limit.
enable_functions	String	Indicates whether licensed functions are enabled. This can be one of the following values. • **0**. Licensed functions are disabled. • **1**. Licensed functions are enabled.
expiring_soon	String	Indicates whether any licenses will expire in 90 days or less. This can be one of the following values. • **0**. Licenses will expire soon. • **1**. Licenses will not expire soon.
managed_devices	String	Total number of managed devices
remaining_days	Integer	Number of days before licensed function is disabled
notifications	Array of objects	Information about license notifications
contact	String	Contact details
description	String	Message description
type	String	Type of the message. This can be one of the following values. • **error** • **warning**
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information

Parameters		Type	Description
	text	String	User actions that can be taken to recover from the event
	URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.


```
{
   "response": [{
      "accepted_eula": "0",
      "active_entitlements": "0",
      "compliant": "0",
      "enable_functions": "1",
      "expiring_soon": "0",
      "managed_devices": "1",
      "remaining_days": "89"
   },
   {
      "notifications": [{
         "contact": "To purchase additional licenses, contact your Lenovo representative or
                        authorized business partner. Learn more <a href=\"javascript:void(0);\"
                       class=\"helpWindow\" data-help-url=\"update_license.html\">here</a>",
         "description": "There are 0 active license keys that entitle licenses for 0 devices;
                             however, 1 managed devices require licenses. You have 89 days remaining
                             to install the appropriate number of licenses to be in compliance.",
         "type": "warning"
      }]
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "explanation": "",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      }
   }]
}
```


/notificationsLicense/warning_period

Use this REST API to retrieve or modify the license warning period, which determines the number of days before license expire when Lenovo XClarity Administrator triggers a warning

HTTP methods

GET, PUT

GET /notificationsLicense/warning_period

Use this method to return the license warning period, which determines the number of days before license expire when Lenovo XClarity Administrator triggers a warning.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/notificationsLicense/warning_period`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
response	Array of objects	
warning_period	String	Number of days before license expire when XClarity Administrator triggers a warning
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "response": [{
      "warning_period": 90
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
```

```
   }]
}
```

/quantityLicense

Use this REST API to return information about all installed licenses or upload and install a license.

HTTP methods

GET, POST

GET /quantityLicense

Use this method to return information about all installed licenses.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/quantityLicense`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters		Type	Description
messages		Array of objects	Information about each license
	end_date	String	Date when the license ends
	enterprise	Boolean	Indicates whether this is an enterprise license. This can be one of the following values. • **true**. This is an enterprise license. • **false**. This is a standard license.

Parameters	Type	Description
id	Integer	License ID
product	String	Product license name
product_description	String	Product license description
quantity	Integer	Number of devices that can be managed under this license
start_date	String	Date when the license starts
valid	Integer	License status. This can be one of the following values. • **0**. The license is not valid. • **1**. The license is valid. • **2**. The license is about to expire.
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "response": [{
      "end_date": "02/25/2019",
      "enterprise": false,
      "id": 1,
      "product": "00MT201",
      "product_description": "Lenovo xClarity Pro per Managed Server for 1 year",
      "quantity": 80,
      "start_date": "02/25/2018"
      "valid": 0,
   },
   ...,
   {
      "end_date": "12/30/2019",
      "enterprise": false,
      "id": 3,
      "product": "00MT201",
      "product_description": "Lenovo xClarity Pro per Managed Server for 1 year",
      "quantity": 30,
      "start_date": "12/30/2018"
      "valid": 0,
   }],
   "result": "success",
```

```
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```


POST /quantityLicense

Use this method to uploads and install a new license to Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/quantityLicense`

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
{license_file>	Required	File	License file

Request example

```
1]tLLenovo SYSTEM X FEATURE ON DEMAND ENTERPRISE ACTIVATION KEY FOR 0123401237   $  System
Independent Feature       < 9   4Lenovo XClarity Administrator Enterprise Activation
$ Activation Expiration     p”w €œ SHA-256 RSA 3072
...
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```

/quantityLicense/*{id}*

Use this REST API to save one or more specific license files in Lenovo XClarity Administrator to the local system or , or delete (uninstall) a specific license.

HTTP methods

GET, DELETE

GET /quantityLicense/*{id_list}*

Use this method to save one or more specific license files in Lenovo XClarity Administrator to the local system.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/quantityLicense/{id_list}
```

where *{id_list}* is one or more license IDs, separated by a comma. To obtain the license IDs, use GET /quantityLicense.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /quantityLicense/*{id_list}*

Use this method to delete a specific license from Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/quantityLicense/{id_list}`

where *{id_list}* is one or more license IDs, separated by a comma. To obtain the license IDs, use GET /quantityLicense.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```

Chapter 11. Events and alerts

The following resources are available for performing monitoring and event functions, such as getting events, getting event status, and setting up event monitors.

Note: When retrieving events from Lenovo XClarity Administrator, use the sequence numbers to verify that no events are missing. If the sequence number of an event is not sequential with that last event that you retrieved for the target device, perform another GET /events to request the events that are associated with all the sequence numbers that you missed.

Filtering events

You can use the parameter **filterWith** to return a subset of all active events based on Java REGEX expressions or based on comparison operators.

You can choose to filter using one of the following methods:

- Java REGEX expressions
- Comparison operators. The following comparison operators are provided:
  - EQ (equal)
  - NOT (not equal)
  - GT (greater than)
  - GTE (greater than or equal to)
  - LT (less than)
  - LTE (less than or equal to).

Note: You cannot combine Java REGEX expressions with comparison operators.

Comparison operators

Some fields support only specific comparison operators.

Parameter	EQ	GT	GTE	LT	LTE	NOT
action	√	√	√	√	√	√
ARGS	√					√
cn	√	√	√	√	√	√
componentID	√	√	√	√	√	√
eventClass	√	√	√	√	√	√
eventDate	√	√	√	√	√	√
eventID	√					√
FAILFRUS	√					√
FAILSNS	√					√
groupUUID	√					√
localLogID	√	√	√	√	√	√
localLogSequence	√	√	√	√	√	√
location	√					√

Parameter	EQ	GT	GTE	LT	LTE	NOT
msgID	√					√
mtm	√					√
search	√	√	√	√	√	√
sequenceid	√	√	√	√	√	√
serialnum	√					√
service	√	√	√	√	√	√
severity	√	√	√	√	√	√
sourceID	√	√	√	√	√	√
sourceLogID						
sourceLogSequence	√	√	√	√	√	√
timeStamp	√	√	√	√	√	√
USERID	√					√

Filtering examples

Filtering is passed as part of the URI parameters. The filter itself is in JSON format. All filters follow the following parameter format.

Obtaining all events that have a cn (sequence ID) greater than 1:

```
https://<Server IP Address>/events?filterWith={"filterType":"FIELDNOTREGEXAND",
"fields":[{"operation":"GT","field":"cn","value":"1"}]}
```

Events can be filtered based on the following fields:

Parameter	Comparison operators example	Regex expression example

action	{
	"operation":"EQ",
	"field":"action",
	"value":"ABCDE"
	}
		{
		"field":"action",
		"value":"ABCDE"
		}

cn	{
	"operation":"EQ",
	"field":"cn",
	"value":"1"
	}
		{
		"field":"cn",
		"value":"1"
		}

componentID	{
	"operation":"EQ",
	"field":"componentID",
	"value":"FFFFF"
	}
		{
		"field":"componentID",
		"value":"FFFFF"
		}

Parameter	Comparison operators example	Regex expression example

eventClass	{
	"operation":"EQ",
	"field":"eventClass",
	"value":"200"
	}
	or
	{
	"operation":"EQ",
	"field":"eventClass",
	"value":"AUDIT"
	}
		{
		"field":"eventClass",
		"value":"200"
		}
		or
		{
		"field":"eventClass",
		"value":"AUDIT"
		}

eventDate	{
	"operation":"EQ",
	"field":"eventDate",
	"value":"2014-02-11T09:54:58Z"
	}
		{
		"field":"eventDate",
		"value":"2014-02-11T09:54:58Z"
		}

eventID	{
	"operation":"EQ",
	"field":"eventID",
	"value":"FQXHMCP5810I"
	}
		{
		"field":"eventID",
		"value":"FQXHMCP5810I"
		}

groupUUID	{
	"operation":"EQ",
	"field":"groupUUID",
	"value": [
	"FFB657408BEB4161950704AB",
	"59AFBFCF8DBB376A25D68A0A"]
	}
		{
		"field":"groupUUID",
		"value": [
		"FFB657408BEB4161950704AB",
		"59AFBFCF8DBB376A25D68A0A"]
		}

localLogID	{
	"operation":"EQ",
	"field":"localLogID",
	"value":"ABCDE"
	}
		{
		"field":"localLogID",
		"value":"ABCDE"
		}

localLogSequence	{
	"operation":"EQ",
	"field":"localLogSequence",
	"value":"1"
	}
		{
		"field":"localLogSequence",
		"value":"1"
		}

location	{
	"operation":"EQ",
	"field":"location",
	"value":"ABCDE"
	}
		{
		"field":"location",
		"value":"ABCDE"
		}

msgID	{
	"operation":"EQ",
	"field":"msgID",
	"value":"ABCDE"
	}
		{
		"field":"msgID",
		"value":"ABCDE"
		}

mtm	{
	"operation":"EQ",
	"field":"mtm",
	"value":"ABCDE"
	}
		{
		"field":"mtm",
		"value":"ABCDE"
		}

Parameter	Comparison operators example	Regex expression example

search	{
	"operation":"EQ",
	"field":"search",
	"value":"ABCDE"
	}
		{
		"field":"search",
		"value":"ABCDE"
		}

sequenceid	{
	"operation":"EQ",
	"field":"sequenceid",
	"value":"1"
	}
		{
		"field":"sequenceid",
		"value":"1"
		}

serialnum	{
	"operation":"EQ",
	"field":"serialnum",
	"value":"ABCDE"
	}
		{
		"field":"serialnum",
		"value":"ABCDE"
		}

service	{
	"operation":"EQ",
	"field":"service",
	"value":"100"
	}
	or
	{
	"operation":"EQ",
	"field":"service",
	"value":"NONE"
	}
		{
		"field":"service",
		"value":"100"
		}
		or
		{
		"field":"service",
		"value":"NONE"
		}

severity	{
	"operation":"EQ",
	"field":"severity",
	"value":"200"
	}
	or
	{
	"operation":"EQ",
	"field":"severity",
	"value":"INFORMATIONAL"
	}
		{
		"field":"severity",
		"value":"200"
		}
		or
		{
		"field":"severity",
		"value":"INFORMATIONAL"
		}

sourceID	{
	"operation":"EQ",
	"field":"sourceID",
	"value":"ABCDE"
	}
		{
		"field":"sourceID",
		"value":"ABCDE"
		}

sourceLogID	{
	"operation":"EQ",
	"field":"sourceLogID",
	"value":"ABCDE"
	}
		{
		"field":"sourceLogID",
		"value":"ABCDE"
		}

Parameter	Comparison operators example	Regex expression example

sourceLogSe-quence	{
	"operation":"EQ",
	"field":"sourceLogSequence",
	"value":"1234"
	}
		{
		"field":"sourceLogSequence",
		"value":"1234"
		}

timeStamp	{
	"operation":"EQ",
	"field":"timeStamp",
	"value":"2014-02-11T09:54:58Z"
	}
		{
		"field":"timeStamp",
		"value":"2014-02-11T09:54:58Z"
		}

Applying a filter to match a single event with a sequence ID equal to 16:

```
{
   "filterType":"FIELDNOTREGEXAND",
   "fields": [{
      "operation":"EQ",
      "field":"cn",
      "value":"16"
   }]
}

{
   "filterType":"FIELDREGEXAND",
   "fields": [{
      "field":"cn",
      "value":"16"
   }]
}
```

These two filters are equivalent; they both will match with a single event, the event that has the cn/sequenceid equal to 16.

The filtering is composed of two parts:

1. The first part is the filterType that can have only one value from the following enumeration:
   - **FIELDREGEXAND**. Regex filter of type AND
   - **FIELDREGEXOR**.Regex filter of type OR
   - **FIELDREGEXNOT**. Regex filter of type NOT
   - **FIELDNOTREGEXAND**. Non-Regex filter of type AND
   - **FIELDNOTREGEXOR**. Non-Regex filter of type OR
   - **FIELDNOTREGEXNOT**. Non-Regex filter of type NOT

   The REGEX filters accept only REGEX expressions in the "value" field. The Non-REGEX filters do not accept REGEX expressions in the "value" field. The Non-REGEX filter works with the six comparison operators (EQ, NOT, GT, GTE, LT, LTE). It also has a special field called "operation" in which to specify the comparison operation.

   The "filterType" is a mandatory field.
2. The second part is an enumeration of "fields" that define the target of the filter match. This field is required.The "fields" is a JSONArray Enumeration composed of JSON Objects. In the above example it can be seen that there is only one JSON ({"operation":"EQ" , "field":"cn" , "value":"16"}) in the entire JSONArray ([{"operation":"EQ" , "field":"cn" , "value":"16"}]).

Applying a complex filter:

```
{
   "filterType":"FIELDNOTREGEXAND",
   "fields": [
      {"operation":"GT", "field":"cn", "value":"16"},
```

```
        {"operation":"GTE", "field":"severity", "value":"400"},
        {"operation":"GTE", "field":"timeStamp", "value":"2014-02-11T09:20:35Z"}
    ]
}
```

This filter will match all events that have the cn/sequenceid greater than 16, a severity greater than or equal to 400, and a timeStamp greater than or equal to 9:20:35 Zulu - February 11, 2014.

/events

Use this REST API to retrieve information about events, and delete all events in the events log.

HTTP methods

GET, DELETE

GET /events

Use this method to return hardware and management-server events in the events log. If no query parameters are specified, all hardware and management-server events are returned.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events`

Query parameters

Parameters	Required / Optional	Description

filterWith=*{filter}*	Optional	Returns only the events that apply to the specified filters, where *{filter}* is a JSON object in the following format.
		`{`
		`  "filterType": "{filter_type}",`
		`  "fields": [{`
		`  "field": "{filter}",`
		`  "operation": "{operation}",`
		`  "value": "{value}"`
		`  }]`
		`}`
		For more information, see Filtering events.

sort=*{event_field}*	Optional	Returns events that are sorted by the specified event field. To sort in descending order, add a dash (-) to the event field.
type=excluded	Optional	Returns only exclude events

Parameters	Required / Optional	Description
translations=*{JSON_filter}*	Optional	Returns translated events based on the criteria that is specified using encoded JSON format (see GET /events?translations=*{JSON_filter}*)
escapeHTML=*{Boolean}*	Optional	Indicates whether to replace escape characters in the message with special characters (for example, "). This can be one of the following values. • **true**. Replaces escape characters with special characters in the returned message. • **false**. Does not replaces escape characters in the returned message. **Note:** Escape characters must be included in arguments when there is HTML in message descriptions.

The following example returns a list of excluded events sorted by the local log sequence and replaces escape characters in the message with special characters:

```
GET https://192.0.2.0/events?sort=localLogSequence&type=excluded&escapeHTML=true
```

The following example returns only events that have a cn (sequence ID) greater than 1.

```
GET https://<Server IP Address>/events?filterWith={"filterType":"FIELDNOTREGEXAND",
"fields":[{"field":"cn","operation":"GT"," value":"1"}]}
```

The following example returns translated events using specific criteria:

```
GET https://192.0.2.0/events?sort=localLogSequence&translations=%7B%22filters%22%3A%7B%22
excludedevents%22%3Afalse%2C%22eventclass%22%3A%5B%22SYSTEM%22%5D%2C%22
severity%22%3A%5B%22CRITICAL%22%2C%22WARNING%22%2C%22INFORMATIONAL%22%5D%2C%22
evsource%22%3A%22%2%2C%22uuids%22%3A%5B%5D%2C%22evdate%22%3A%7B%22
start%22%3A%222017-05-29T13%3A06%3A41.508Z%22%2C%22end%22%3A%22%22%7D%2C%22
customfilter%22%3A%7B%22searchfor%22%3A%22%22%2C%22applyon%22%3A%5B%5D%7D%7D%2C%22
pagination%22%3A%7B%22offset%22%3A0%2C%22limit%22%3A10%7D%2C%22sort%22%3A%7B%22
applyon%22%3A%22timeStamp%22%2C%22mode%22%3A%22DESC%22%7D%7D
```

Request body

None

Request header

Attributes	Required / Optional	Description

Range	Optional	Request the events with the given range of sequence numbers. If the range goes beyond the actual available sequence numbers, the start of the range through the last sequence number is returned. For example:
		`GET /events`
		`Range: item=0-24`
		`--------`
		`Response Header:`
		`Content-Range: 0-24/3000`
		Note: When retrieving events from Lenovo XClarity Administrator, use the sequence numbers to verify that no events are missing. If the sequence number of an event is not sequential with that last event that you retrieved for the target device, perform another GET /events to request the events that are associated with all the sequence numbers that you missed.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
action	Integer	Action category. This can be one of the following values. • **100**. NONE • **200**. TOPOLOGY • **300**. IP • **400**. INVENTORY If not available, an empty string is returned.
args	Array of string	List of dynamic arguments in the event message string. If not available, an empty string is returned. If not available, an empty string is returned.
bayText	String	
chassisText	String	
cn	String	Event Sequence number. It is the order in which the events were processed.
commonEventID	String	Common event ID.
componentID	Array of string	Unique ID of the component on which the event occurred. If not available, an empty string is returned.

Attributes	Type	Description
componentIdentifierText	String	The component description. This can be one of the following values. • **Canister/Appliance** • **Client Data Storage Device** • **Cooling** • **Device Driver** • **Display** • **Hypervisor** • **I/O connectivity** • **Interconnect (Fabric)** • **Interconnect (Interfaces)** • **Interconnect (Networking)** • **Interconnect (PCI Manager)** • **Interconnect (PIE)** • **Interconnect (Utilities / Infrastructure)** • **Memory** • **OS** • **OS/Hypervisor Interface** • **Power** • **Processing** • **Storage RAID** • **System board** • **Systems Management** • **Time Reference** • **Unknown** • **Vendor Events** • **VPD**
decriptionArgs	Array of strings	List of dynamic arguments in the event message description. If not available, an empty string is returned.
eventClass	Integer	The source of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch If not available, an empty string is returned.
eventDate	String	Time and date that the event was created on source system. This is the time and date from the managed system and might be quite different from **timeStamp**, which is when the event was processed by the Lenovo XClarity Administrator. The string is in ISO-8601 format: `yyyy-MM-dd'T'HH:mm:ss'Z'`
eventID	String	Event ID is a unique identifier for each event supported by a product.
eventSourceText	String	
failFRUNames	Array of strings	For hardware fault events, includes names of one or more FRUs that are associated with the fault. If not available, an empty string is returned.

Attributes	Type	Description
failFRUPartNumbers	Array of strings	For hardware fault events, includes part numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUs	Array of strings	For hardware fault events, includes FRU numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUUUIDs	Array of strings	For hardware fault events, includes UUIDs for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failSNs	Array of strings	For hardware fault events, includes serial numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
flags	Array of strings	Proprietary event flag definitions. This can be one of the following values. • **Hidden**. The event not to be displayed in normal log views. It is displayed only for diagnostic views. • **Historical**. The event occurred while the management server was down and can be ignored by EventActions. • **Ignored**. The event is ignored. • **Recovered**. The event was involved in the reliable event recovery process. • **Unsequenced**. Switch system traps are not sequenced. Reliable event recovery is skipped. • **VM**. VM Migration (Blade "Trust the Source Logging Model") If not available, an empty string is returned.
fruSerialNumberText	String	
groupName	Array of strings	List of resource-groups, by name, to which the source of the event belongs. If the source does not belong to a resource group, the value is “Not Available.”
groupUUID	Array of strings	List of resource-groups, by UUID, to which the source of the event belongs.
localLogID	String	Log type. This can be one of the following values. • **AUDIT**. Audit events • **EVENT**. All other events.
localLogSequence	Integer	Log Sequence Number, which uniquely identifies this event on the audit or event log If not available, an empty string is returned.
location	String	Location information for event association in the format of “Slot#01.”
msg	String	Event message string.
msgID	String	Event message ID.
mtm	String	System machine type and model of the managed system on which the event occurred.
originatorUUID	String	The unique ID of the managed system on which the event occurred.
Attributes	Object	Reserved. If not available, an empty string is returned.
senderUUID	String	
serialnum	String	Serial number of system generating the event (event source). Not set for internal events.

Attributes	Type	Description
service	Integer	Identifer that specifies how service is performed. It can be one of the following. • **100**. Not Serviceable. • **200**. Serviceable by Lenovo (called home) • **300**. Serviceable by the customer If not available, an empty string is returned.
serviceabilityText	String	
severity	Integer	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred. If not available, an empty string is returned.
severityText	String	Severity text. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred. If not available, an empty string is returned.
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
sourceLogID	String	Identifier of log of event source system. System may have multiple logs for events and this identifier is used with the System Log Sequence Number for reliable event support.
sourceLogSequence	Integer	Source Log Sequence Number, uniquely identifies this event in source Log ID
systemFruNumberText	String	
systemName	String	System identifier. It correlates to the display name used for the device on the CMM.
systemSerialNumberText	String	
systemText	String	
systemTypeModelText	String	
systemTypeText	String	
timeStamp	String	Time and date of when the log entry was created for the Lenovo XClarity Administrator log. The string is in ISO-8601 format (for example, `yyyy-MM-dd'T'HH:mm:ss'Z'`).
typeText	String	
userActionArgs	Array of strings	List of dynamic arguments in the event message action If not available, an empty string is returned.

Attributes	Type	Description
userid	String	For internal audit events, this is the associated user ID. This is not available for external events.
userIDIndex	Integer	

The following example is returned if the request is successful.


```
[{
    "action": 100,
    "args": ["nist800-131a", "Demo - 00404X5462", "nistcomp"],
    "chassisText": "Not Available",
    "bayText": "Not Available",
    "commonEventID": "FQXHMSE0006G",
    "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
    "cn": "6",
    "componentIdentifierText": "Systems Management",
    "decriptionArgs": "",
    "eventClass": 800,
    "eventDate": "2017-07-24T19:32:35Z",
    "eventID": "FQXHMSE0006G",
    "eventSourceText": "Management",
    "failFRUNames": [],
    "failFRUPartNumbers": [],
    "failFRUs": [],
    "failFRUUUIDs": [],
    "failSNs": [],
    "flags": "",
    "fruSerialNumberText": "Not Available",
    "groupName": ["e-Commerce Servers","Lenovo Solutions"],
    "groupUUID": ["599D9BF18DBB37078155E985","59AFBFCF8DBB376A25D68A0A"],
    "localLogID": "",
    "localLogSequence": "",
    "location": "",
    "msg": "Cryptographic mode nist800-131a on Demo - 00404X5462 does not match cryptographic mode
                nistcomp on the management server.",
    "msgID": "",
    "mtm": "",
    "originatorUUID": "",
    "parameters": {},
    "senderUUID": "",
    "serialnum": "",
    "service": 100,
    "serviceabilityText": "Not Required",
    "severity": 300,
    "severityText": "Warning",
    "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
    "sourceLogID": "",
    "sourceLogSequence": 0,
    "systemFruNumberText": "Not Available",
    "systemName": "Management Server",
    "systemSerialNumberText": "Not Available",
    "systemText": "Management Server",
    "systemTypeModelText": "Not Available",
    "systemTypeText": "Management",
    "timeStamp": "2017-07-24T19:32:35Z",
    "typeText": "System",
    "userActionArgs": "",
    "userid": "",
    "userIDIndex": 0
}]
```

DELETE /events

Use this method to delete all events in the event log.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events?translations={*JSON_filter*}

Use this REST API to retrieve translated events based on the criteria that is specified using encoded JSON format.

HTTP methods

GET

GET /events?translations={*JSON_filter*}

Use this method to return translated events based on the criteria that is specified using encoded JSON format.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events?translations={JSON_filter}`

Query parameters

Parameters	Re-quired / Optional	Description
translations={*JSON_filter*>	Required	Returns translated events based on the criteria that is specified using encoded JSON format.

The following example returns translated events using specific criteria.

```
GET https://192.0.2.0/events?translations=%7B%22filters%22%3A%7B%22
excludedevents%22%3Afalse%2C%22eventclass%22%3A%5B%22SYSTEM%22%5D%2C%22
severity%22%3A%5B%22CRITICAL%22%2C%22WARNING%22%2C%22INFORMATIONAL%22%5D%2C%22
evsource%22%3A%22%2%2C%22uuids%22%3A%5B%5D%2C%22evdate%22%3A%7B%22
start%22%3A%222017-05-29T13%3A06%3A41.508Z%22%2C%22end%22%3A%22%22%7D%2C%22
customfilter%22%3A%7B%22searchfor%22%3A%22%22%2C%22applyon%22%3A%5B%5D%7D%7D%2C%22
pagination%22%3A%7B%22offset%22%3A0%2C%22limit%22%3A10%7D%2C%22sort%22%3A%7B%22
applyon%22%3A%22timeStamp%22%2C%22mode%22%3A%22DESC%22%7D%7D
```

Where *{JSON_filter}* contains the following attributes:

Attributes	Required / Optional	Type	Description
filters	Optional	Object	Filter information
customfilter	Optional	Object	Custom filter
applyon	Optional	Array of strings	Columns on which the text is checked against
searchfor	Optional	String	Search text
eventclass	Optional	Array of strings	List of event classes. This can be one or more of the following values. • **SYSTEM** • **AUDIT**
evdate	Optional	Object	Date interval
end	Optional	String	End date
start	Optional	String	Start date
evsource	Optional	String	Event source. This can be one of the following values. • **MANAGEMENT** • **HARDWARE** • **IBM_SERVICEABLE** • **CUSTOMER_SERVICEABLE**
excludedevents	Optional	Boolean	Indicates whether the server fetches only excluded events only. This can be one of the following values. • **true**. The server retrieves only excluded events • **false**. The server retrieves all events.
groupName	Optional	Strings	Resource-group name to which the source of the event belongs
groupUUID	Optional	Strings	Resource-group UUID to which the source of the event belongs
severity	Required	Array of strings	List of event severities. This can be one or more of the following values. • **INFORMATIONAL** • **WARNING** • **CRITICAL**
uuids	Optional	Array of strings	Event source and component UUIDs
pagination	Optional	Object	Pagination information
limit	Optional	Integer	Number of events to be returned per page

Attributes	Re-quired / Optional	Type	Description
offset	Optional	Integer	Start of the next page
sort	Optional	Object	Sort information
applyon	Optional	String	Name of the column on which the filter is to be applied
mode	Optional	String	Sort mode. This can be one of the following values. • **ASC**. Ascending • **DESC**. Decending
sourceLink	Optional	String	Link to the source of the event. This attribute is returned only when the **translations** query parameter is specified.

For example,

```
{
   "filters": {
      "customfilter" : {
         "applyon"    : [],
         "searchfor" : ""
      },
      "groupName" : "e-Commerce Servers",
      "evdate" : {
         "end"  :"",
         "start" :"2017-05-29T13:06:41.508Z"
      },
      "eventclass" : ["SYSTEM"],
      "evsource" : "",
      "excludedevents" : false,
      "severity" : ["CRITICAL","WARNING","INFORMATIONAL"],
      "uuids" : []
   },
   "pagination" : {
      "limit" : 10,
      "offset" : 0
   },
   "sort" : {
      "applyon"   : "timeStamp",
      "mode" : "DESC"
   }
}
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
action	Integer	Action category. This can be one of the following values. • **100**. NONE • **200**. TOPOLOGY • **300**. IP • **400**. INVENTORY If not available, an empty string is returned.
args	Array of string	List of dynamic arguments in the event message string. If not available, an empty string is returned. If not available, an empty string is returned.
bayText	String	
chassisText	String	
cn	String	Event Sequence number. It is the order in which the events were processed.
commonEventID	String	Common event ID.
componentID	Array of string	Unique ID of the component on which the event occurred. If not available, an empty string is returned.
componentIdentifierText	String	The component description. This can be one of the following values. • **Canister/Appliance** • **Client Data Storage Device** • **Cooling** • **Device Driver** • **Display** • **Hypervisor** • **I/O connectivity** • **Interconnect (Fabric)** • **Interconnect (Interfaces)** • **Interconnect (Networking)** • **Interconnect (PCI Manager)** • **Interconnect (PIE)** • **Interconnect (Utilities / Infrastructure)** • **Memory** • **OS** • **OS/Hypervisor Interface** • **Power** • **Processing** • **Storage RAID** • **System board** • **Systems Management** • **Time Reference** • **Unknown** • **Vendor Events** • **VPD**

Attributes	Type	Description
decriptionArgs	Array of strings	List of dynamic arguments in the event message description. If not available, an empty string is returned.
eventClass	Integer	The source of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch If not available, an empty string is returned.
eventDate	String	Time and date that the event was created on source system. This is the time and date from the managed system and might be quite different from **timeStamp**, which is when the event was processed by the Lenovo XClarity Administrator. The string is in ISO-8601 format: `yyyy-MM-dd'T'HH:mm:ss'Z'`
eventID	String	Event ID is a unique identifier for each event supported by a product.
eventSourceText	String	
failFRUNames	Array of strings	For hardware fault events, includes names of one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUPartNumbers	Array of strings	For hardware fault events, includes part numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUs	Array of strings	For hardware fault events, includes FRU numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUUUIDs	Array of strings	For hardware fault events, includes UUIDs for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failSNs	Array of strings	For hardware fault events, includes serial numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.

Attributes	Type	Description
flags	Array of strings	Proprietary event flag definitions. This can be one of the following values. • **Hidden**. The event not to be displayed in normal log views. It is displayed only for diagnostic views. • **Historical**. The event occurred while the management server was down and can be ignored by EventActions. • **Ignored**. The event is ignored. • **Recovered**. The event was involved in the reliable event recovery process. • **Unsequenced**. Switch system traps are not sequenced. Reliable event recovery is skipped. • **VM**. VM Migration (Blade "Trust the Source Logging Model") If not available, an empty string is returned.
fruSerialNumberText	String	
groupName	Array of strings	List of resource-groups, by name, to which the source of the event belongs. If the source does not belong to a resource group, the value is “Not Available.”
groupUUID	Array of strings	List of resource-groups, by UUID, to which the source of the event belongs.
localLogID	String	Log type. This can be one of the following values. • **AUDIT**. Audit events • **EVENT**. All other events.
localLogSequence	Integer	Log Sequence Number, which uniquely identifies this event on the audit or event log If not available, an empty string is returned.
location	String	Location information for event association in the format of “Slot#01.”
msg	String	Event message string.
msgID	String	Event message ID.
mtm	String	System machine type and model of the managed system on which the event occurred.
originatorUUID	String	The unique ID of the managed system on which the event occurred.
Attributes	Object	Reserved. If not available, an empty string is returned.
senderUUID	String	
serialnum	String	Serial number of system generating the event (event source). Not set for internal events.
service	Integer	Identifer that specifies how service is performed. It can be one of the following. • **100**. Not Serviceable. • **200**. Serviceable by Lenovo (called home) • **300**. Serviceable by the customer If not available, an empty string is returned.
serviceabilityText	String	

Attributes	Type	Description
severity	Integer	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred. If not available, an empty string is returned.
severityText	String	Severity text. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred. If not available, an empty string is returned.
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
sourceLogID	String	Identifier of log of event source system. System may have multiple logs for events and this identifier is used with the System Log Sequence Number for reliable event support.
sourceLogSequence	Integer	Source Log Sequence Number, uniquely identifies this event in source Log ID
systemFruNumberText	String	
systemName	String	System identifier. It correlates to the display name used for the device on the CMM.
systemSerialNumberText	String	
systemText	String	
systemTypeModelText	String	
systemTypeText	String	
timeStamp	String	Time and date of when the log entry was created for the Lenovo XClarity Administrator log. The string is in ISO-8601 format (for example, `yyyy-MM-dd'T'HH:mm:ss'Z'`).
typeText	String	
userActionArgs	Array of strings	List of dynamic arguments in the event message action If not available, an empty string is returned.
userid	String	For internal audit events, this is the associated user ID. This is not available for external events.
userIDIndex	Integer	

The following example is returned if the request is successful.

```
[{
```

```
   "action": 100,
   "args": ["nist800-131a", "Demo - 00404X5462", "nistcomp"],
   "chassisText": "Not Available",
   "bayText": "Not Available",
   "commonEventID": "FQXHMSE0006G",
   "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
   "cn": "6",
   "componentIdentifierText": "Systems Management",
   "decriptionArgs": "",
   "eventClass": 800,
   "eventDate": "2017-07-24T19:32:35Z",
   "eventID": "FQXHMSE0006G",
   "eventSourceText": "Management",
   "failFRUNames": [],
   "failFRUPartNumbers": [],
   "failFRUs": [],
   "failFRUUUIDs": [],
   "failSNs": [],
   "flags": "",
   "fruSerialNumberText": "Not Available",
   "groupName": ["e-Commerce Servers","Lenovo Solutions"],
   "groupUUID": ["599D9BF18DBB37078155E985","59AFBFCF8DBB376A25D68A0A"],
   "localLogID": "",
   "localLogSequence": "",
   "location": "",
   "msg": "Cryptographic mode nist800-131a on Demo - 00404X5462 does not match cryptographic mode
               nistcomp on the management server.",
   "msgID": "",
   "mtm": "",
   "originatorUUID": "",
   "parameters": {},
   "senderUUID": "",
   "serialnum": "",
   "service": 100,
   "serviceabilityText": "Not Required",
   "severity": 300,
   "severityText": "Warning",
   "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
   "sourceLogID": "",
   "sourceLogSequence": 0,
   "systemFruNumberText": "Not Available",
   "systemName": "Management Server",
   "systemSerialNumberText": "Not Available",
   "systemText": "Management Server",
   "systemTypeModelText": "Not Available",
   "systemTypeText": "Management",
   "timeStamp": "2017-07-24T19:32:35Z",
   "typeText": "System",
   "userActionArgs": "",
   "userid": "",
   "userIDIndex": 0
}]
```


/events/actions

Use this REST API to retrieve information about all event action or to post an event action entry to the registry for filtering on incoming events. *Event actions* are actions or functions that are called based on an incoming event.

HTTP methods

GET, POST

GET /events/actions

Use this method to return information about all event actions.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/actions`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
eventFilter	Object	Information about the event filter
fields	Array of objects	Fields to filter on and the associated REGEX string to filter. The event field must match one of the supported fields in the event class (see Filtering events).
field	String	Fields to filter on This field must match one of the supported fields in the event class. For more information about filtering events, see Filtering events.
value	String	Associated REGEX string to filter
filtertype	String	The type of filter. This can be one of the following values. • **FIELDREGEXAND**. Event filter matches only if all fields find a match with the given field REGEX. • **FIELDREGEXOR**. Event filter matches if *any* field finds a match with the given field REGEX. • **FIELDREGEXNOT**. Event filter matches only if all fields do *not* find a match with the given field REGEX.
name	String	Name used to identify the event action **Note:** This name must be unique.
persistent	String	Indicates whether this event action entry should be saved across restarts of the XClarity Administrator

Attributes	Type	Description
port	Integer	Port to use for this event action The default port is 8080.
uri	String	The action or function to call when an incoming event is found to match the filter. The action must be a REST API supporting a POST call to the URI with the JSON object form of the event in the body.

The following example is returned if the request is successful.

```
[{
    "eventFilter": {
       "fields": [{
          "field": "eventID",
          "value": "FQXHMDM0001I|FQXHMDI0002I|FQXHMDI0001I|FQXHMDI0003A|FQXHMDI0003G|FQXHMDI0004A|
                    FQXHMDI0101I|FQXHMDI0102I|FQXHMDI0103G|FQXHMDI0104G |FQXHMDI0024I|0EA04001|
                    0EA04002|0EA04003|0EA04004|0E004001|0E004002|0E004003|0E004004|0E004005|0E004006|
                    0E004007|0E004008|0E004009|0E004009||0E00400B|0E00400C|0E00400D|0E00400E|00284001|
                    00284002|806F012B210100FF"
       }],
       "filterType": "FIELDREGEXOR"
    },
    "persistent": "false",
    "port": "8080",
    "name": "updates_event_handler",
    "uri": "/stgupdates/inventory/events"
},
{
    "eventFilter": {
       "fields": [{
          "field": "eventID",
          "value": "FQXHMDM0001I|FQXHMDI0002I|FQXHMDI0001I|FQXHMDI0101I|FQXHMDI0102I|FQXHMSS1001I"
       }],
       "filterType": "FIELDREGEXOR"
    },
    "name": "flexcat-event-handler",
    "persistent": "false",
    "port": "8080",
    "uri": "/osdeployment/rest/internal/event"
},
{...,
{
    "eventFilter": {
       "fields": [{
          "field": "eventID",
          "value": "FQXHMDM0002I"
       }],
       "filterType": "FIELDREGEXAND"
    },
    "name": "EAT_43",
    "port": "8080",
    "persistent": "false",
    "uri": "/events/actions/ap/AP_11/EAT_43"
}]
```

POST /events/actions

Use this method to post an event action entry to the registry for filtering on incoming events.

Authentication

Authentication with username and password is required.

Request URL

```
POST https://{management_server_IP}/events/actions
```

Query parameters

None

Request body

A JSON object that contains the event action or function URL and event filter.

Attributes	Re-quired / Optional	Type	Description
eventFilter	Required	Object	Information about the event filter. At least one of the following JSON objects must be specified.
fields	Optional	Array of objects	Fields to filter on and the associated REGEX string to filter. The event field must match one of the supported fields in the event class (see Filtering events).
field	Required if **fields** is specified	String	Fields to filter on This field must match one of the supported fields in the event class. For more information about filtering events, see Filtering events.
value	Required if **fields** is specified	String	Associated REGEX string to filter
filtertype	Optional	String	Type of filter. This can be one of the following values. • **FIELDREGEXAND**. Event filter matches only if all fields find a match with the given field REGEX. • **FIELDREGEXOR**. Event filter matches if *any* field finds a match with the given field REGEX. • **FIELDREGEXNOT**. Event filter matches only if all fields do *not* find a match with the given field REGEX.
name	Required	String	Name used to identify the event action **Note:** This name must be unique.
persistent	Optional	String	Indicates whether this event action entry should be saved across restarts of the XClarity Administrator
port	Optional	Integer	Port to use for this event action The default port is 8080.
uri	Required	String	Action or function to call when an incoming event is found to match the filter. The action must be a REST API supporting a POST call to the URI with the JSON object form of the event in the body.

The following example posts an event action.

```
{
   "eventFilter": {
      "fields":[{
```

```
            "field":"eventID",
            "value":"FQXHMDM0001I|FQXHMDI0002I|FQXHMDI0001I|FQXHMSS1001I"
        }],
        "filterType":"FIELDREGEXOR"
    },
    "persistent":"false",
    "name":"flexcat-event-handler",
    "port": "8080",
    "uri" : "/osdeployment/rest/internal/event"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/actions/*{action_name}*

Use this REST API to retrieve information about or delete a specific event action. *Event actions* are actions or functions that are performed based on an incoming event.

HTTP methods

GET, DELETE

DELETE /events/actions/*{action_name}*

Use the method to delete a specific event action.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/actions/{action_name}`

where *{action_name}* is the name of the action to be retrieved. To obtain the action name, use the GET /events/actions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

GET /events/actions/*{action_name}*

Use this method to return information about a specific event action.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/actions/{action_name}`

where *{action_name}* is the name of the action to be retrieved. To obtain the action name, use the GET /events/actions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
eventFilter	Object	Information about the event filter
fields	Array of objects	Fields to filter on and the associated REGEX string to filter. The event field must match one of the supported fields in the event class (see Filtering events).
field	String	Fields to filter on This field must match one of the supported fields in the event class. For more information about filtering events, see Filtering events.

Attributes	Type	Description
value	String	Associated REGEX string to filter
filtertype	String	The type of filter. This can be one of the following values. • **FIELDREGEXAND**. Event filter matches only if all fields find a match with the given field REGEX. • **FIELDREGEXOR**. Event filter matches if *any* field finds a match with the given field REGEX. • **FIELDREGEXNOT**. Event filter matches only if all fields do *not* find a match with the given field REGEX.
name	String	Name used to identify the event action **Note:** This name must be unique.
persistent	String	Indicates whether this event action entry should be saved across restarts of the XClarity Administrator
port	Integer	Port to use for this event action The default port is 8080.
uri	String	The action or function to call when an incoming event is found to match the filter. The action must be a REST API supporting a POST call to the URI with the JSON object form of the event in the body.

The following example is returned if the request is successful.


```
{
   "eventFilter": {
      "fields": [{
         "field": "eventID",
         "value": "FQXHMDM0001I|FQXHMDI0002I|FQXHMDI0001I|FQXHMDI0003A|FQXHMDI0003G|FQXHMDI0004A|
                   FQXHMDI0101I|FQXHMDI0102I|FQXHMDI0103G|FQXHMDI0104G |FQXHMDI0024I|0EA04001|
                  0EA04002|0EA04003|0EA04004|0E004001|0E004002|0E004003|0E004004|0E004005|0E004006|
                  0E004007|0E004008|0E004009|0E004009||0E00400B|0E00400C|0E00400D|0E00400E|00284001|
                  00284002|806F012B21010OFF"
      }],
      "filterType": "FIELDREGEXOR"
   },
   "persistent": "false",
   "name": "updates_event_handler",
   "port": "808",
   "uri": "/stgupdates/inventory/events"
}
```


/events/acknowledgeAlerts

Use this REST API to retrieve a list of active alerts that were acknowledged, to acknowledge an active alert, or to remove the acknowledge status for an active alert.

When an active alert is *acknowledged*, the alert is still included in view but is no longer included in the severity status for a device.

Note: This API requires Lenovo XClarity Administrator v3.0.0 or later.

HTTP methods

GET, PUT, DELETE

GET /events/acknowledgeAlerts

Use this method to return a list of active alerts that were acknowledged.

When an active alert is *acknowledged*, the alert is still included in view but is no longer included in the severity status for a device.

Note: This API requires Lenovo XClarity Administrator v3.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/acknowledgeAlerts`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
componentID	String	ID of the component that raised the alert
date	String	Time and date that the event was raised on source device. This is the time and date from the managed device and might be different from timestamp when the alert was processed by the Lenovo XClarity Administrator. This timestamp is specified using ISO-8601 format (for example, 2019-05-02T19:28:14.000Z). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
eventID	String	Event ID of the event that is associated with the alert
sourceID	String	ID of the source that raised the alert

The following example is returned if the request is successful.

```
[{
   "componentID": "3015DE7E2B6011E881940A94EF5F5B65",
   "date": "2019-07-08T16:19:10Z",
   "eventID": "FQXHMDM0163J",
   "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
},
...,
{
   "componentID": "3015DE7E2B6011E881940A94EF5AC567",
   "date": "2019-07-08T16:19:10Z",
```

```
   "eventID": "FQXHMDM0163J",
   "sourceID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
}]
```

PUT /events/acknowledgeAlerts

Use this method to acknowledge one or more active alerts.

When an active alert is *acknowledged*, the alert is still included in view but is no longer included in the severity status for a device.

Note: This API requires Lenovo XClarity Administrator v3.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/events/acknowledgeAlerts`

Query parameters

None

Request body

Parameter	Re-quired / Optional	Type	Description
componentID		String	ID of the component that raised the alert
date		String	Time and date that the event was raised on source device. This is the time and date from the managed device and might be different from timestamp when the alert was processed by the Lenovo XClarity Administrator. This timestamp is specified using ISO-8601 format (for example, 2019-05-02T19:28:14.000Z). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
eventID		String	Event ID of the event that is associated with the alert
sourceID		String	ID of the parent of the component that raised the alert If there is no parent, this is the same as the component ID.

The following example acknowledges an active alert.

```
{
   "componentID": "3015DE7E2B6011E881940A94EF5F5B65",
   "date": "2019-07-08T16:19:10Z",
   "eventID": "FQXHMDM0163J",
   "sourceID": "3015DE7E2B6011E881940A94EF5F5B65"
}
```

The following example acknowledges two active alerts.

```
[{
   "componentID": "3015DE7E2B6011E881940A94EF5F5B65",
   "date": "2020-06-16T16:10:26.000Z",
   "eventID": "0X806F030C2001FFFF",
   "sourceID": "3015DE7E2B6011E881940A94EF5F5B65"
```

```
},
{
   "componentID":"3015DE7E2B6011E881940A94EF5A832",
   "date" : "2020-06-16T16:10:26.000Z",
   "eventID":"0X806F030C2001FFFF",
   "sourceID":"3015DE7E2B6011E881940A94EF5A832"
}]
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
206	Partial Content	The part, but not all, of the request completed successfully. A descriptive message is returned in the response body indicating how many active alerts were acknowledge, how many were already acknowledged, how many were invalid, and how many failed to be acknowledged.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /events/acknowledgeAlerts

Use this method to remove the acknowledgement for one or more active alerts.

Note: This API requires Lenovo XClarity Administrator v3.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/acknowledgeAlerts`

Query parameters

None

Request body

Parameter	Re-quired / Optional	Type	Description
componentID		String	ID of the component that raised the alert
date		String	Time and date that the event was raised on source device. This is the time and date from the managed device and might be different from timestamp when the alert was processed by the Lenovo XClarity Administrator. This timestamp is specified using ISO-8601 format (for example, 2019-05-02T19:28:14.000Z). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
eventID		String	Event ID of the event that is associated with the alert
sourceID		String	ID of the parent of the component that raised the alert If there is no parent, this is the same as the component ID.

The following example remove the acknowledgement for an active alert.

```
{
   "componentID": "3015DE7E2B6011E881940A94EF5F5B65",
   "date": "2019-07-08T16:19:10Z",
   "eventID": "FQXHMDM0163J",
   "sourceID": "3015DE7E2B6011E881940A94EF5F5B65"
}
```

The following example remove the acknowledgement for two active alerts.

```
[{
   "componentID": "3015DE7E2B6011E881940A94EF5F5B65",
   "date": "2020-06-16T16:10:26.000Z",
   "eventID": "0X806F030C2001FFFF",
   "sourceID": "3015DE7E2B6011E881940A94EF5F5B65"
},
{
   "componentID":"3015DE7E2B6011E881940A94EF5A832",
   "date" : "2020-06-16T16:10:26.000Z",
   "eventID":"0X806F030C2001FFFF",
   "sourceID":"3015DE7E2B6011E881940A94EF5A832"
}]
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
206	Partial Content	The part, but not all, of the request completed successfully. A descriptive message is returned in the response body indicating how many acknowledgements were deleted, how many did not exist, how many were invalid, and how many failed to be deleted.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/activeAlerts

Use this REST API to retrieve information about active alerts or the number of active alerts per resource group. *Alerts* are hardware or management conditions that need investigation and user action.

HTTP methods

GET

GET /events/activeAlerts

Use this method to return information about active alerts or the number of active alerts per resource group. If no query parameters are specified, information about all active alerts is returned.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/activeAlerts`

Query parameters

Parameters	Required / Optional	Description
escapeHTML=*{Boolean}*	Optional	Indicates whether to replace escape characters in the message with special characters (for example, "). This can be one of the following values. • **true**. Replaces escape characters with special characters in the returned message. • **false**. Does not replaces escape characters in the returned message. **Note:** Escape characters must be included in arguments when there is HTML in messages.
filterWith=*{filter}*	Optional	Returns only the active alerts that apply to the specified filters (see Filtering events).
groupUIDs=*{uuid}*	Optional	If **outputFormat=summary** is specified, returns the number of active alerts for one or more resource groups, specified by UUID. Separate multiple UUIDs by a comma.
outputFormat=*{type}*	Optional	Returns information for the specified type. This can be one of the following values. • **default**. Information about all active alerts • **summary**. Number of active alerts (critical and warning) per resource group

Parameters	Re-quired / Optional	Description
type=*{type}*	Optional	Returns only active alerts of the specific type. This can be one of the following values. • **excluded**. Returns only exclude active alerts. • **acknowledge**. Returns only acknowledged active alerts.
uidList=*{uuid_list}*	Optional	If **outputFormat=default** is specified, returns alert information only for one or more specific groups and devices. To obtain the group or device UUIDs, use GET /resourceGroups, GET /chassis, GET /cmms, GET /nodes, GET /storage, and GET /switches.

The following example returns a list of all active alerts for two specific devices.

```
GET https://192.0.2.0/events/activeAlerts?
uidList=["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA","BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"]
```

The following example returns a list of all *excluded* active alerts and replaces escape characters in the message with special characters.

```
GET https://192.0.2.0/events/activeAlerts?type=excluded&escapeHTML=true
```

The following example returns the number of *acknowledge* active alerts for two specific resource groups.

```
GET https://192.0.2.0/events/activeAlerts?type=acknowledge&outputFormat=summary&
groupUIDs=["11111","22222"]
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Table 75. Number of active alerts per resource group

Attributes	Type	Description
{group_UID>	Object	Active alerts for the specified resource group
critical	Integer	Number of critical alerts
warning	Integer	Number of warning alerts

The following example is returned if the request is successful and **outputFormat=summary** is specified.

```
[{
   "11111": {
      "critical": 0,
      "warning": 1
   },
   "22222": {
      "critical": 0,
      "warning ": 0
   },
   "333333333333333333333333": {
      "critical": 0,
      "warning ": 0
   },
   "444444444444444444444444": {
      "critical": 0,
      "warning ": 0
   }
}]
```

Table 76. Default information about all active alerts

Attributes	Type	Description
alertID	String	Alert identifier
args	Array of string	List of dynamic arguments in the event message string. If not available, an empty string is returned. If not available, an empty string is returned.
bayText	String	
chassisText	String	
commonEventID	String	Common event ID
componentID	String	ID of the component associated with the active alert
componentIdentifierText	String	Component description. This can be one of the following values. • **Canister/Appliance** • **Client Data Storage Device** • **Cooling** • **Device Driver** • **Display** • **Hypervisor** • **I/O connectivity** • **Interconnect (Fabric)** • **Interconnect (Interfaces)** • **Interconnect (Networking)** • **Interconnect (PCI Manager)** • **Interconnect (PIE)** • **Interconnect (Utilities / Infrastructure)** • **Memory** • **OS** • **OS/Hypervisor Interface** • **Power** • **Processing** • **Storage RAID** • **System board** • **Systems Management** • **Time Reference** • **Unknown** • **Vendor Events** • **VPD**

Table 76. Default information about all active alerts (continued)

Attributes	Type	Description
eventClass	String	Source of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch
eventDate	String	Time and date that the event was created on source system. This is the time and date from the managed system and might be quite different from **timeStamp**, which is when the event was processed by the Lenovo XClarity Administrator. The string is in ISO-8601 format: `yyyy-MM-dd'T'HH:mm:ss'Z'`
eventID	String	Event ID is a unique identifier for each event supported by a product
eventSourceText	String	
failFRUNames	Array of strings	For hardware fault events, includes names of one or more FRUs that are associated with the fault If not available, an empty string is returned.
failFRUPartNumbers	Array of strings	For hardware fault events, includes part numbers for one or more FRUs that are associated with the fault If not available, an empty string is returned.
failFRUs	Array of strings	For hardware fault events, includes FRU numbers for one or more FRUs that are associated with the fault If not available, an empty string is returned.
failFRUUUIDs	Array of strings	For hardware fault events, includes UUIDs for one or more FRUs that are associated with the fault If not available, an empty string is returned.
failSNs	Array of strings	For hardware fault events, includes serial numbers for one or more FRUs that are associated with the fault If not available, an empty string is returned.
flags	String	
fruSerialNumberText	String	
groupName	Array of strings	List of resource-groups, by name, to which the source of the alert belongs. If the source does not belong to a resource group, the value is “Not Available.”
groupUUID	Array of strings	List of resource-groups, by UUID, to which the source of the alert belongs.
isManagement	Boolean	
location	String	Location information for event association in the format of `Slot#01`

Table 76. Default information about all active alerts (continued)

Attributes	Type	Description
msg	String	Event message string. This is provided in the language requested if translation is supported. If translation is not supported, the message as received in the event will be provided, in whatever language the product provided at time of event (typically this is English).
msgID	String	
raisedDate	String	Date/time active alert was raised by REST user in the ISO-8601 format. `yyyy-MM-dd'T'HH:mm:ss'Z`
relatedAlerts	String	Other alerts related to this alert, if applicable.
service	String	Indicates how service is performed. This can be one of the following value. • **100** . Not serviceable. • **200**. Serviceable by Lenovo (called home). • **300**. Serviceable by the customer.
serviceabilityText	String	
severity	Integer	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred.
severityText	String	Severity text. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred. If not available, an empty string is returned.
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
systemFruNumberText	String	
systemName	String	System identifier. It correlates to the display name used for the device on the CMM
systemSerialNumberText	String	
systemText	String	
systemTypeModelText	String	

Table 76. Default information about all active alerts (continued)

Attributes	Type	Description
systemTypeText	String	
typeText	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch

The following example is returned if the request is successful and **outputFormat=default** is specified.


```
[{
    "alertID": "IAL:1:FFB657408BEB4161950704AB0ED3A84A",
    "args": ["FFB657408BEB4161950704AB0ED3A84A",""],
    "bayText": "Not Available",
    "chassisText": "Not Available",
    "commonEventID": "",
    "componentID": "FFB657408BEB4161950704AB0ED3A84A",
    "componentIdentifierText": "Unknown",
    "eventClass": 800,
    "eventDate": "2019-07-08T16:19:10Z",
    "eventID": "FQXHMDM0163J",
    "eventSourceText": "Hardware",
    "failFRUNames": [],
    "failFRUPartNumbers": [],
    "failFRUs": [],
    "failFRUUUIDs": [],
    "failSNs": [],
    "flags": "",
    "fruSerialNumberText": "Not Available",
    "groupName": ["Not Available"],
    "groupUUID": [],
    "isManagement": true,
    "location": "",
    "msg": "The connection between the management server and the management controller
            FFB657408BEB4161950704AB0ED3A84A is offline.",
    "msgID": "FQXHMDM0163J",
    "raisedDate": "2019-07-08T16:19:10Z",
    "relatedAlerts": "",
    "service": 100,
    "serviceabilityText": "Not Required",
    "severity": 300,
    "severityText": "Warning",
    "sourceID": "FFB657408BEB4161950704AB0ED3A84A",
    "systemFruNumberText": "Not Available",
    "systemName": "",
    "systemSerialNumberText": "Not Available",
    "systemText": "Not Available",
    "systemTypeModelText": "Not Available",
```

```
    "systemTypeText": "Not Available",
    "typeText": "System"
}
...
]
```


/events/activeAlerts/*{uuid}*

Use this REST API to retrieve information about active alerts that are associated with a specific managed device. *Alerts* are hardware or management conditions that need investigation and user action.

HTTP methods

GET

GET /events/activeAlerts/*{uuid}*

Use this method to return information about active alerts that are associated with a specific managed device. If no query parameters are specified, all active alerts that are associated with the specified managed device are returned.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/activeAlerts/{uuid}`

where *{uuid}* is the unique ID of the managed device to be retrieved. To obtain the device UUID, use the inventory GET methods (for example, GET /chassis, GET /nodes, GET /storage, and GET /switches).

Query parameters

Parameters	Required / Optional	Description
escapeHTML=*{Boolean}*	Optional	Indicates whether to replace escape characters in the message with special characters (for example, "). This can be one of the following values. • **true**. Replaces escape characters with special characters in the returned message. • **false**. Does not replaces escape characters in the returned message. **Note:** Escape characters must be included in arguments when there is HTML in messages.
filterWith=*{filter}*	Optional	Returns only the active alerts that apply to the specified filters (see Filtering events).
type=*{type}*	Optional	Returns only exclude active alerts. Returns only active alerts of the specific type. This can be one of the following values. • **excluded**. Returns only exclude active alerts. • **acknowledge**. Returns only acknowledged active alerts.

The following example returns a list of all active alerts for the specified device.

```
GET https://192.0.2.0/events/activeAlerts/EA35F98A144E11E2BA81864E72900ECC
```

The following example returns a list of all excluded active alerts for the specified device and replaces escape characters in the message with special characters.

```
GET https://192.0.2.0/events/activeAlerts/EA35F98A144E11E2BA81864E72900ECC?type=excluded&escapeHTML=true
```

The following example returns a list of all acknowledged active alerts for the specified device.

```
GET https://192.0.2.0/events/activeAlerts/EA35F98A144E11E2BA81864E72900ECC?type=acknowledge
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Table 77. Default information about all active alerts

Attributes	Type	Description
alertID	String	Alert identifier
args	Array of string	List of dynamic arguments in the event message string. If not available, an empty string is returned. If not available, an empty string is returned.
bayText	String	
chassisText	String	
commonEventID	String	Common event ID
componentID	String	ID of the component associated with the active alert

Table 77. Default information about all active alerts (continued)

Attributes	Type	Description
componentIdentifierText	String	Component description. This can be one of the following values. • **Canister/Appliance** • **Client Data Storage Device** • **Cooling** • **Device Driver** • **Display** • **Hypervisor** • **I/O connectivity** • **Interconnect (Fabric)** • **Interconnect (Interfaces)** • **Interconnect (Networking)** • **Interconnect (PCI Manager)** • **Interconnect (PIE)** • **Interconnect (Utilities / Infrastructure)** • **Memory** • **OS** • **OS/Hypervisor Interface** • **Power** • **Processing** • **Storage RAID** • **System board** • **Systems Management** • **Time Reference** • **Unknown** • **Vendor Events** • **VPD**
eventClass	String	Source of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch
eventDate	String	Time and date that the event was created on source system. This is the time and date from the managed system and might be quite different from **timeStamp**, which is when the event was processed by the Lenovo XClarity Administrator. The string is in ISO-8601 format: `yyyy-MM-dd'T'HH:mm:ss'Z'`
eventID	String	Event ID is a unique identifier for each event supported by a product
eventSourceText	String	
failFRUNames	Array of strings	For hardware fault events, includes names of one or more FRUs that are associated with the fault If not available, an empty string is returned.

Table 77. Default information about all active alerts (continued)

Attributes	Type	Description
failFRUPartNumbers	Array of strings	For hardware fault events, includes part numbers for one or more FRUs that are associated with the fault If not available, an empty string is returned.
failFRUs	Array of strings	For hardware fault events, includes FRU numbers for one or more FRUs that are associated with the fault If not available, an empty string is returned.
failFRUUUIDs	Array of strings	For hardware fault events, includes UUIDs for one or more FRUs that are associated with the fault If not available, an empty string is returned.
failSNs	Array of strings	For hardware fault events, includes serial numbers for one or more FRUs that are associated with the fault If not available, an empty string is returned.
flags	String	
fruSerialNumberText	String	
groupName	Array of strings	List of resource-groups, by name, to which the source of the alert belongs. If the source does not belong to a resource group, the value is “Not Available.”
groupUUID	Array of strings	List of resource-groups, by UUID, to which the source of the alert belongs.
isManagement	Boolean	
location	String	Location information for event association in the format of `Slot#01`
msg	String	Event message string. This is provided in the language requested if translation is supported. If translation is not supported, the message as received in the event will be provided, in whatever language the product provided at time of event (typically this is English).
msgID	String	
raisedDate	String	Date/time active alert was raised by REST user in the ISO-8601 format. `yyyy-MM-dd'T'HH:mm:ss'Z`
relatedAlerts	String	Other alerts related to this alert, if applicable.
service	String	Indicates how service is performed. This can be one of the following value. • **100** . Not serviceable. • **200**. Serviceable by Lenovo (called home). • **300**. Serviceable by the customer.
serviceabilityText	String	
severity	Integer	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred.

Table 77. Default information about all active alerts (continued)

Attributes	Type	Description
severityText	String	Severity text. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred. If not available, an empty string is returned.
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
systemFruNumberText	String	
systemName	String	System identifier. It correlates to the display name used for the device on the CMM
systemSerialNumberText	String	
systemText	String	
systemTypeModelText	String	
systemTypeText	String	
typeText	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch

The following example is returned if the request is successful.


```
{
    "alertID": "IAL:1:FFB657408BEB4161950704AB0ED3A84A",
    "args": ["FFB657408BEB4161950704AB0ED3A84A",""],
    "bayText": "Not Available",
    "chassisText": "Not Available",
    "commonEventID": "",
    "componentID": "FFB657408BEB4161950704AB0ED3A84A",
    "componentIdentifierText": "Unknown",
    "eventClass": 800,
    "eventDate": "2019-07-08T16:19:10Z",
    "eventID": "FQXHMDM0163J",
    "eventSourceText": "Hardware",
    "failFRUNames": [],
    "failFRUPartNumbers": [],
```

```
    "failFRUs": [],
    "failFRUUUIDs": [],
    "failSNs": [],
    "flags": "",
    "fruSerialNumberText": "Not Available",
    "groupName": ["Not Available"],
    "groupUUID": [],
    "isManagement": true,
    "location": "",
    "msg": "The connection between the management server and the management controller
            FFB657408BEB4161950704AB0ED3A84A is offline.",
    "msgID": "FQXHMDM0163J",
    "raisedDate": "2019-07-08T16:19:10Z",
    "relatedAlerts": "",
    "service": 100,
    "serviceabilityText": "Not Required",
    "severity": 300,
    "severityText": "Warning",
    "sourceID": "FFB657408BEB4161950704AB0ED3A84A",
    "systemFruNumberText": "Not Available",
    "systemName": "",
    "systemSerialNumberText": "Not Available",
    "systemText": "Not Available",
    "systemTypeModelText": "Not Available",
    "systemTypeText": "Not Available",
    "typeText": "System"
}
```

/events/activeAlerts/helptext/*{alert_id}*

Use this REST API to retrieve the description and recovery action for a specific alert.

HTTP methods

GET

GET /events/activeAlerts/helptext/*{alert_id}*

Use this method to return the description and recovery action for a specific alert.

For message-description and user-action text in the job summary, you can specify the text directly in the request body if no translations are needed, or you can reference the text from a translated bundle file (for example, `com.lenovo.lxca.server.jobs.bundle.jobsSummary`).

When the job description and recovery actions require formatted text, you must specify the text as an array of objects in JSON format. You cannot use HTML.

Tip: In the translated bundle files, braces {} must be escaped by a single quote for help text (for example, `'{'`).

Attribute	Re-quired / Optional	Type	Description
format	Required	Array of strings	List of formats for the text. This can be one of the following values. • **bold**. Corresponds to the <b> HTML tag. • **italic**. Corresponds to the <i> HTML tag. • **underline**. Corresponds to the <u> HTML tag. • **link**. Corresponds to the <a> HTML tag. • **newline**. Corresponds to the HTML tag. • **paragraph**. Corresponds to the <p> HTML tag. • **quotation**. Corresponds to the <q> HTML tag. • **orderedList**. Corresponds to the HTML tag. • **bulletList**. Corresponds to the HTML tag. • **listElement**. Corresponds to the HTML tag. If no format is needed, use an empty array.
link	Optional	String	URL to be linked to
text	Required	String or array of strings	Text to be formatted

The following example has formatted text in the user action. It includes paragraphs, ordered list, unordered list, link, and formatted text. Note that braces {} *are not* escaped by a single quote.

```
[{
   "text": "To display the text correctly, the following steps are made.",
   "format": []
},
{
   "text": [],
   "format": ["newline"]
},
{
   "text": [{
      "text": "Segment the text into pieces between HTML tags.",
      "format": ["listElement"]
   },
   {
      "text": [{
         "text": "If the segmented text contains ",
         "format": []
      },
      {
         "text": "multiple tags",
         "format": ["bold"]
      },
      {
         "text": ", segment them as well.",
         "format": []
      }],
      "format": ["listElement"]
   },
   {
      "text": [ {
         "text": "After having all segments, add the tags as follows:",
         "format": []
      },
      {
         "text": [{
```

```
            "text": "Add the text between the tags in the text field of JSON. If multiple tags are found,
                      text field is an array of JSON Objects.",
            "format": ["listElement"]
         },
         {
            "text": "Add the format for each text between tags.",
            "format": ["listElement"]
         }],
         "format": ["bulletList"]
      }],
      "format": ["listElement"]
   },
   {
      "text": "Make sure this is a json format.",
      "format": ["listElement", "bold", "underline"]
   }],
   "format": ["orderedList"]
},
{
   "text": [],
   "format": ["newline"]
},
{
   "text": [{
      "text": "This is how a paragraph looks like with a ",
      "format": []
   },
   {
      "text": "link",
      "format": ["link"],
      "link": "https://www3.lenovo.com/"
   }],
   "format": ["paragraph"]
},
{
   "text": "This is how the result should look.",
   "format": ["paragraph", "italic"]
}]
```

This example correlates to the following HTML format

```
To display the text correctly, the following steps are made.
<br></br>
<ol>
<li>Segment the text into pieces between HTML tags.</li>
<li>If the segmented text contains <b>multiple tags</b>, segment them as well.</li>
<li>After having all segments, add the tags as follows:
<ul>
<li>Add the text between the tags in the text field of JSON. If multiple tags are found,
text field is an array of JSON Objects.</li>
<li>Add the format for each text between tags.</li>
</ul></li>
<li><b><u>Make sure this is a json format.</u></b></li>
</ol>
<br></br>
<p>This is how a paragraph looks like with a <a href="https://www3.lenovo.com/">link</a></p>
<p><i>This is how the result should look.</i></p>
```

This example correlates to the following formatted output:

To display the text correctly, the following steps are made.

1. Segment the text into pieces between HTML tags.
2. If the segmented text contains **multiple tags**, segment them as well.
3. After having all segments, add the tags as follows:
   - Add the text between the tags in the text field of JSON. If multiple tags are found, text field is an array of JSON Objects.
   - Add the format for each text between tags.
4. **Make sure this is a json format.**

This is how a paragraph looks like with a link

This is how the result should look.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/activeAlerts/helptext/{alert_id}`

where *{alert_id}* is the sequence number of the alert to be retrieved. To obtain the alert sequence number, use the **cn** attribute that is returned by the GET /events method).

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
description	Array of objects	Information about the message descriptions
format	Array of strings	
text	String	Alert description

Attributes	Type	Description
useraction	Array of objects	Information about the recovery actions
format	Array of strings	
text	String	Recovery actions to resolve the alert

The following example is returned if the request is successful.

```
{
   "description": [{
      "format": [],
      "text": "The specified user cannot log in."
   }],
   "useraction": [{
      "format": [],
      "text": "Information only; no action is required."
   }]
}
```

/events/activeAlerts/status

Use this REST API to retrieve the alert status, as defined by highest severity of active alerts, for all managed devices. *Alerts* are hardware or management conditions that need investigation and user action.

HTTP methods

GET

GET /events/activeAlerts/status

Use this method to return the alert status, as defined by highest severity of active alerts, for all managed devices. If no query parameters are specified, all active alerts are returned.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/activeAlerts/status`

Query parameters

Parameters	Required / Optional	Description
filterWith=*{filter}*	Optional	Returns only the active alerts that apply to the specified filters (see Filtering events)
type=excluded	Optional	Returns only exclude active alerts

The following example returns the alert status for all excluded active alerts:

```
GET https://192.0.2.0/events/activeAlerts/status?type=excluded
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
componentID	String	Component ID
eventClass	String	Surce of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
status	Integer	Status of the event. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred.

The following example is returned if the request is successful.

```
[{
   "componentID": "DUMMYFFB657408BEB41610101030203020000",
   "eventClass": 50,
   "sourceID": "FFB657408BEB4161950704AB0ED3A84A",
   "status": 600
},
...,
{
```

```
   "componentID": "E81E37592C6911E18AC4C4B91C9FD1E6",
   "eventClass": 50,
   "sourceID": "FFB657408BEB4161950704AB0ED3A84A",
   "status": 300
}]
```

/events/activeAlerts/status/*{uuid}*

Use this REST API to retrieve the alert status, as defined by highest severity of active alerts, for a specific managed device. *Alerts* are hardware or management conditions that need investigation and user action.

HTTP methods

GET

GET /events/activeAlerts/status/*{uuid}*

Use this method to return the alert status, as defined by highest severity of active alerts, for a specific managed device. If no query parameters are specified, all active alerts are returned.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/activeAlerts/status/{uuid}`

where *{uuid}* is the unique ID of the managed device to be retrieved. To obtain the device UUID, use the inventory GET methods (for example, GET /nodes/*{uuid_list}* or GET /chassis).

Query parameters

Parameters	Required / Optional	Description
filterWith=*{filter}*	Optional	Returns only the active alerts that apply to the specified filters (see Filtering events).
type=excluded	Optional	Returns only exclude active alerts.

The following example returns the alert status for all excluded active alerts for the specified device:

```
GET https://192.0.2.0/events/activeAlerts/status/
EA35F98A144E11E2BA81864E72900ECC?type=excluded
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
componentID	String	Component ID
eventClass	String	Source of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
status	Integer	Status of the event. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred.

The following example is returned if the request is successful.

```
[{
   "componentID" : "56781234891012345678",
   "eventClass" : 800,
   "sourceID" : "1234567891213456876 4",
   "status": 100
}]
```

/events/activeAlerts/summary

Use this REST API to retrieve a summary of all active alerts.

HTTP methods

GET

GET /events/activeAlerts/summary

Use this method to return the severity and messages for active alert. If no query parameters are specified, all active alerts are returned.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/activeAlerts/summary
```

Query parameters

Parameters	Re-quired / Optional	Description
filterWith=*{filter}*	Optional	Returns only the active alerts that apply to the specified filters (see Filtering events)
type=excluded	Optional	Returns only exclude active alerts

The following example returns the severity and messages for all excluded active alerts.

```
GET https://192.0.2.0/events/activeAlerts/summary?type=excluded
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
severity	String	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred.
msg	String	Event message string. This is provided in the language requested if translation is supported. If translation is not supported, the message as received in the event will be provided, in whatever language the product provided at time of event (typically this is English).

The following example is returned if the request is successful.

```
[{
   "severity": 300,
   "msg":"Power supply Power Supply 02 is off. Input fault."
}]
```

/events/activeAlerts/summary/*{uuid}*

Use this REST API to retrieve a summary of all active alerts that are associated with a specific managed device.

GET /events/activeAlerts/summary/*{uuid}*

Use this method to return the severity and messages for active alerts that are associated with a specific managed device. If no query parameters are specified, all active alerts are returned.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/activeAlerts/summary/{uuid}`

where *{uuid}* is the unique ID of the managed device to be retrieved. To obtain the device UUID, use the inventory GET methods (for example, GET /nodes/*{uuid_list}* or GET /chassis).

Query parameters

Parameters	Required / Optional	Description
type=excluded	Optional	Returns only exclude active alerts.
filterWith=*{filter}*	Optional	Returns only the active alerts that apply to the specified filters (see Filtering events).

The following example returns the severity and messages for all excluded active alerts for the specified device:

```
GET https://192.0.2.0/events/activeAlerts/summary/EA35F98A144E11E2BA81864E72900ECC?type=excluded
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
severity	String	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred.
msg	String	Event message string. This is provided in the language requested if translation is supported. If translation is not supported, the message as received in the event will be provided, in whatever language the product provided at time of event (typically this is English).

The following example is returned if the request is successful.

```
[{
   "severity": 300,
   "msg":"Power supply Power Supply 02 is off. Input fault."
}]
```

/events/audit

Use this REST API to retrieve events in the Lenovo XClarity Administrator audit log.

HTTP methods

GET

GET /events/audit

Use this method to return audit events in the audit log. If no query parameters are specified, all audit events are returned.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/audit
```

Query parameters

Parameters	Required / Optional	Description

filterWith=*{filter}*	Optional	Returns only the events that apply to the specified filters, where *{filter}* is a JSON object in the following format.
		{
		"filterType": "*{filter_type}*",
		"fields": [{
		"field": "*{filter}*",
		"operation": "*{operation}*",
		"value": "*{value}*"
		}]
		}
		For more information, see Filtering events.

sort=*{event_field}*	Optional	Returns events that are sorted by the specified event field. To sort in descending order, add a dash (-) to the event field.
type=excluded	Optional	Returns only exclude events
translations=*{JSON_filter}*	Optional	Returns translated events based on the criteria that is specified using encoded JSON format (see GET /events?translations=*{JSON_filter}*)
escapeHTML=*{Boolean}*	Optional	Indicates whether to replace escape characters in the message with special characters (for example, "). This can be one of the following values. • **true**. Replaces escape characters with special characters in the returned message. • **false**. Does not replaces escape characters in the returned message. **Note:** Escape characters must be included in arguments when there is HTML in message descriptions.

The following example returns a list of excluded events sorted by the local log sequence and replaces escape characters in the message with special characters:

```
GET https://192.0.2.0/events/audit?sort=localLogSequence&type=excluded&escapeHTML=true
```

Request header

Attributes	Required / Optional	Description

Range	Optional	Request the events with the given range of sequence numbers. If the range goes beyond the actual available sequence numbers, the start of the range through the last sequence number is returned. For example:
		`GET /events`
		`Range: item=0-24`
		`--------`
		`Response Header:`
		`Content-Range: 0-24/3000`
		Note: When retrieving events from Lenovo XClarity Administrator, use the sequence numbers to verify that no events are missing. If the sequence number of an event is not sequential with that last event that you retrieved for the target device, perform another GET /events to request the events that are associated with all the sequence numbers that you missed.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
action	Integer	Action category. This can be one of the following values. • **100**. NONE • **200**. TOPOLOGY • **300**. IP • **400**. INVENTORY If not available, an empty string is returned.
args	Array of string	List of dynamic arguments in the event message string. If not available, an empty string is returned. If not available, an empty string is returned.
bayText	String	
chassisText	String	
cn	String	Event Sequence number. It is the order in which the events were processed.
commonEventID	String	Common event ID.
componentID	Array of string	Unique ID of the component on which the event occurred. If not available, an empty string is returned.

Attributes	Type	Description
componentIdentifierText	String	The component description. This can be one of the following values. • **Canister/Appliance** • **Client Data Storage Device** • **Cooling** • **Device Driver** • **Display** • **Hypervisor** • **I/O connectivity** • **Interconnect (Fabric)** • **Interconnect (Interfaces)** • **Interconnect (Networking)** • **Interconnect (PCI Manager)** • **Interconnect (PIE)** • **Interconnect (Utilities / Infrastructure)** • **Memory** • **OS** • **OS/Hypervisor Interface** • **Power** • **Processing** • **Storage RAID** • **System board** • **Systems Management** • **Time Reference** • **Unknown** • **Vendor Events** • **VPD**
decriptionArgs	Array of strings	List of dynamic arguments in the event message description. If not available, an empty string is returned.
eventClass	Integer	The source of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch If not available, an empty string is returned.
eventDate	String	Time and date that the event was created on source system. This is the time and date from the managed system and might be quite different from **timeStamp**, which is when the event was processed by the Lenovo XClarity Administrator. The string is in ISO-8601 format: `yyyy-MM-dd'T'HH:mm:ss'Z'`
eventID	String	Event ID is a unique identifier for each event supported by a product.
eventSourceText	String	
failFRUNames	Array of strings	For hardware fault events, includes names of one or more FRUs that are associated with the fault. If not available, an empty string is returned.

Attributes	Type	Description
failFRUPartNumbers	Array of strings	For hardware fault events, includes part numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUs	Array of strings	For hardware fault events, includes FRU numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUUUIDs	Array of strings	For hardware fault events, includes UUIDs for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failSNs	Array of strings	For hardware fault events, includes serial numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
flags	Array of strings	Proprietary event flag definitions. This can be one of the following values. • **Hidden**. The event not to be displayed in normal log views. It is displayed only for diagnostic views. • **Historical**. The event occurred while the management server was down and can be ignored by EventActions. • **Ignored**. The event is ignored. • **Recovered**. The event was involved in the reliable event recovery process. • **Unsequenced**. Switch system traps are not sequenced. Reliable event recovery is skipped. • **VM**. VM Migration (Blade "Trust the Source Logging Model") If not available, an empty string is returned.
fruSerialNumberText	String	
groupName	Array of strings	List of resource-groups, by name, to which the source of the event belongs. If the source does not belong to a resource group, the value is “Not Available.”
groupUUID	Array of strings	List of resource-groups, by UUID, to which the source of the event belongs.
localLogID	String	Log type. This can be one of the following values. • **AUDIT**. Audit events • **EVENT**. All other events.
localLogSequence	Integer	Log Sequence Number, which uniquely identifies this event on the audit or event log If not available, an empty string is returned.
location	String	Location information for event association in the format of “Slot#01.”
msg	String	Event message string.
msgID	String	Event message ID.
mtm	String	System machine type and model of the managed system on which the event occurred.
originatorUUID	String	The unique ID of the managed system on which the event occurred.
Attributes	Object	Reserved. If not available, an empty string is returned.
senderUUID	String	
serialnum	String	Serial number of system generating the event (event source). Not set for internal events.

Attributes	Type	Description
service	Integer	Identifer that specifies how service is performed. It can be one of the following. • **100**. Not Serviceable. • **200**. Serviceable by Lenovo (called home) • **300**. Serviceable by the customer If not available, an empty string is returned.
serviceabilityText	String	
severity	Integer	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred. If not available, an empty string is returned.
severityText	String	Severity text. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred. If not available, an empty string is returned.
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
sourceLogID	String	Identifier of log of event source system. System may have multiple logs for events and this identifier is used with the System Log Sequence Number for reliable event support.
sourceLogSequence	Integer	Source Log Sequence Number, uniquely identifies this event in source Log ID
systemFruNumberText	String	
systemName	String	System identifier. It correlates to the display name used for the device on the CMM.
systemSerialNumberText	String	
systemText	String	
systemTypeModelText	String	
systemTypeText	String	
timeStamp	String	Time and date of when the log entry was created for the Lenovo XClarity Administrator log. The string is in ISO-8601 format (for example, `yyyy-MM-dd'T'HH:mm:ss'Z'`).
typeText	String	
userActionArgs	Array of strings	List of dynamic arguments in the event message action If not available, an empty string is returned.

Attributes	Type	Description
userid	String	For internal audit events, this is the associated user ID. This is not available for external events.
userIDIndex	Integer	

The following example is returned if the request is successful.


```
[{
    "action": 100,
    "args": ["USERID", "10.38.106.229"],
    "bayText": "Not Available",
    "chassisText": "Not Available",
    "cn": "25",
    "commonEventID": "FQXHMSE0200I",
    "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
    "componentIdentifierText": "Systems Management",
    "decriptionArgs": "",
    "eventClass": 200,
    "eventDate": "2017-07-31T14:30:03Z",
    "eventID": "FQXHMSE0200I",
    "eventSourceText": "Management",
    "flags": "",
    "failFRUs": "",
    "failSNs": "",
    "fruSerialNumberText": "Not Available",
    "localLogID": "",
    "localLogSequence": "",
    "location": "",
    "msg": "The login was successful for user ID USERID at IP address 10.38.106.229.",
    "msgID": "",
    "mtm": "",
    "originatorUUID": "",
    "parameters": {    },
    "senderUUID": "",
    "serialnum": "",
    "service": 100,
    "serviceabilityText": "Not Required",
    "severity": 200,
    "severityText": "Informational",
    "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
    "sourceLogID": "",
    "sourceLogSequence": 0,
    "systemFruNumberText": "Not Available",
    "systemName": "Management Server",
    "systemSerialNumberText": "Not Available",
    "systemText": "Management Server",
    "systemTypeModelText": "Not Available",
    "systemTypeText": "Management",
    "timeStamp": "2017-07-31T14:30:03Z",
    "typeText": "System",
    "userActionArgs": "",
    "userid": "USERID",
    "userIDIndex": 1
}]
```


/events/config

Use this REST API to retrieve information about configuration settings for the Lenovo XClarity Administrator event log, modify the event configuration settings, and clear the event and audit logs.

HTTP methods

GET, PUT

GET /events/config

Use this method to return the configuration settings for the event log.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/config`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
auditLog100Fill	String	Indicates whether the audit log is 100 percent full. This can be one of the following values. • **true**. The event log is 100 percent full. • **false**. The event log is not 100 percent full.
auditLog80Fill	String	Indicates whether the audit log is 80 percent full. This can be one of the following values. • **true**. The event log is 80 percent full. • **false**. The event log is not 80 percent full.
auditLogCurrentSize	String	Current number of entries in the audit log
auditLogMaxSize	String	Maximum number of entries allowed in the audit log. Any entries beyond this number causes the oldest entry to be removed from the log.
eventAggSubscTimeOut	String	Amount of time to wait for an event aggregation subscription
eventLogCurrentSize	String	Current number of entries in the event log

Attributes	Type	Description
eventLogMaxSize	String	Maximum number of entries allowed in the event log. Any entries beyond this number causes the oldest entry to be removed from the log.
eventLog100Fill	String	Indicates whether the event log is 100 percent full. This can be one of the following values. • **true**. The event log is 100 percent full. • **false**. The event log is not 100 percent full.
eventLog80Fill	String	Indicates whether the event log is 80 percent full. This can be one of the following values. • **true**. The event log is 80 percent full. • **false**. The event log is not 80 percent full.

The following example is returned if the request is successful.

```
{
   "auditLog100Fill": "false",
   "auditLog80Fill": "false",
   "auditLogCurrentSize": "264",
   "auditLogMaxSize": "2000",
   "eventLog100Fill": "true",
   "eventLog80Fill": "true",
   "eventAggSubscTimeOut": "2",
   "eventLogCurrentSize": "2000",
   "eventLogMaxSize": "2000"
}
```

PUT /events/config

Use this method to modify the event configuration settings and to clear the event and audit logs.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/events/config`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
clearAuditLog	Required	String	Indicates whether to clear the audit log. This can be one of the following values. • **true**. Clears the audit log. • **false**. (default) Do not clear the audit log.
clearEventLog	Required	String	Indicates whether to clear the event log. This can be one of the following values. • **true**. Clears the event log. • **false**. (default) Do not clear the event log.
eventAggSubscTimeOut	Required	String	Amount of time to wait for an event aggregation subscription

The following example clears the event and audit logs.

```
{
   "clearAuditLog": true,
   "clearEventLog": true,
   "eventAggSubscTimeOut":15,
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/csv/auditLog

Use this REST API to retrieve the Lenovo XClarity Administrator audit log in a .CSV format.

HTTP methods

GET

GET /events/csv/auditLog

Use this method to return the audit log in .CSV format.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/csv/auditLog`

Query parameters

Parameters	Required / Optional	Description
filterWith=*{filter}*	Optional	Returns only the events that apply to the specified filters (see Filtering events).

Request header

Attributes	Required / Optional	Description

Range	Optional	Request the events with the given range of sequence numbers. If the range goes beyond the actual available sequence numbers, the start of the range through the last sequence number is returned. For example:
		`GET /events`
		`Range: item=0-24`
		`--------`
		`Response Header:`
		`Content-Range: 0-24/3000`
		Note: When retrieving events from Lenovo XClarity Administrator, use the sequence numbers to verify that no events are missing. If the sequence number of an event is not sequential with that last event that you retrieved for the target device, perform another GET /events to request the events that are associated with all the sequence numbers that you missed.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response body contains .CSV data. The key definitions are listed in the following table.

Attributes	Type	Description
action	Integer	Action category. This can be one of the following values. • **100**. NONE • **200**. TOPOLOGY • **300**. IP • **400**. INVENTORY If not available, an empty string is returned.
args	Array of string	List of dynamic arguments in the event message string. If not available, an empty string is returned. If not available, an empty string is returned.
bayText	String	
chassisText	String	
cn	String	Event Sequence number. It is the order in which the events were processed.
commonEventID	String	Common event ID.

Attributes	Type	Description
componentID	Array of string	Unique ID of the component on which the event occurred. If not available, an empty string is returned.
componentIdentifierText	String	The component description. This can be one of the following values. • **Canister/Appliance** • **Client Data Storage Device** • **Cooling** • **Device Driver** • **Display** • **Hypervisor** • **I/O connectivity** • **Interconnect (Fabric)** • **Interconnect (Interfaces)** • **Interconnect (Networking)** • **Interconnect (PCI Manager)** • **Interconnect (PIE)** • **Interconnect (Utilities / Infrastructure)** • **Memory** • **OS** • **OS/Hypervisor Interface** • **Power** • **Processing** • **Storage RAID** • **System board** • **Systems Management** • **Time Reference** • **Unknown** • **Vendor Events** • **VPD**
decriptionArgs	Array of strings	List of dynamic arguments in the event message description. If not available, an empty string is returned.
eventClass	Integer	The source of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch If not available, an empty string is returned.
eventDate	String	Time and date that the event was created on source system. This is the time and date from the managed system and might be quite different from **timeStamp**, which is when the event was processed by the Lenovo XClarity Administrator. The string is in ISO-8601 format: `yyyy-MM-dd'T'HH:mm:ss'Z'`
eventID	String	Event ID is a unique identifier for each event supported by a product.
eventSourceText	String	

Attributes	Type	Description
failFRUNames	Array of strings	For hardware fault events, includes names of one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUPartNumbers	Array of strings	For hardware fault events, includes part numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUs	Array of strings	For hardware fault events, includes FRU numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUUUIDs	Array of strings	For hardware fault events, includes UUIDs for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failSNs	Array of strings	For hardware fault events, includes serial numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
flags	Array of strings	Proprietary event flag definitions. This can be one of the following values. • **Hidden**. The event not to be displayed in normal log views. It is displayed only for diagnostic views. • **Historical**. The event occurred while the management server was down and can be ignored by EventActions. • **Ignored**. The event is ignored. • **Recovered**. The event was involved in the reliable event recovery process. • **Unsequenced**. Switch system traps are not sequenced. Reliable event recovery is skipped. • **VM**. VM Migration (Blade "Trust the Source Logging Model") If not available, an empty string is returned.
fruSerialNumberText	String	
groupName	Array of strings	List of resource-groups, by name, to which the source of the event belongs. If the source does not belong to a resource group, the value is “Not Available.”
groupUUID	Array of strings	List of resource-groups, by UUID, to which the source of the event belongs.
localLogID	String	Log type. This can be one of the following values. • **AUDIT**. Audit events • **EVENT**. All other events.
localLogSequence	Integer	Log Sequence Number, which uniquely identifies this event on the audit or event log If not available, an empty string is returned.
location	String	Location information for event association in the format of “Slot#01.”
msg	String	Event message string.
msgID	String	Event message ID.
mtm	String	System machine type and model of the managed system on which the event occurred.
originatorUUID	String	The unique ID of the managed system on which the event occurred.
Attributes	Object	Reserved. If not available, an empty string is returned.

Attributes	Type	Description
senderUUID	String	
serialnum	String	Serial number of system generating the event (event source). Not set for internal events.
service	Integer	Identifer that specifies how service is performed. It can be one of the following. • **100**. Not Serviceable. • **200**. Serviceable by Lenovo (called home) • **300**. Serviceable by the customer If not available, an empty string is returned.
serviceabilityText	String	
severity	Integer	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred. If not available, an empty string is returned.
severityText	String	Severity text. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred. If not available, an empty string is returned.
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
sourceLogID	String	Identifier of log of event source system. System may have multiple logs for events and this identifier is used with the System Log Sequence Number for reliable event support.
sourceLogSequence	Integer	Source Log Sequence Number, uniquely identifies this event in source Log ID
systemFruNumberText	String	
systemName	String	System identifier. It correlates to the display name used for the device on the CMM.
systemSerialNumberText	String	
systemText	String	
systemTypeModelText	String	
systemTypeText	String	
timeStamp	String	Time and date of when the log entry was created for the Lenovo XClarity Administrator log. The string is in ISO-8601 format (for example, `yyyy-MM-dd'T'HH:mm:ss'Z'`).

Attributes	Type	Description
typeText	String	
userActionArgs	Array of strings	List of dynamic arguments in the event message action If not available, an empty string is returned.
userid	String	For internal audit events, this is the associated user ID. This is not available for external events.
userIDIndex	Integer	

The following example is returned if the request is successful.

```
"Sequence ID", "Type", "Severity", "Time Stamp", "Source ID", "Originator UUID", "Component ID",
"Source Log ID", "Local Log ID", "Local Log Sequence", "Event Code", "Event Date", "Message ID",
"Event Message", "Serial Number", "Mtm", "Service", "Action", "Location", "User ID",
"Source Log Sequence", "Flags", "Fail SNs", "Fail FRUs",

"151", "SYSTEM", "INFORMATIONAL", "1424290017496", "63E29269BB634AB9A610D6F8FCE2B28F", "",
"4378eb1f6cf111e4bf1fb0ffa5d3ca74", "LENOVO:CMM01:Y030BG4BA020:01", "EVENT", "83", "0001608C",
"1423627952000", "CMM0207", "SSH host key auto-generation started.", "", "", "NONE", "",
"01010201", "", "14707", "Recovered", "", ""
```

/events/csv/eventLog

Use this REST API to return the Lenovo XClarity Administrator event log in a .CSV format.

HTTP methods

GET

GET /events/csv/eventLog

Use this method to return the event log in .CSV format.

Authentication

Authentication is required.

Request URL

`GET https://{management_server_IP}/events/csv/eventLog`

Query parameters

Parameters	Required / Optional	Description
filterWith=*{filter}*	Optional	Returns only the events that apply to the specified filters (see Filtering events)

Request header

Attributes	Required / Optional	Description

Range	Optional	Request the events with the given range of sequence numbers. If the range goes beyond the actual available sequence numbers, the start of the range through the last sequence number is returned. For example:
		`GET /events`
		`Range: item=0-24`
		`--------`
		`Response Header:`
		`Content-Range: 0-24/3000`
		Note: When retrieving events from Lenovo XClarity Administrator, use the sequence numbers to verify that no events are missing. If the sequence number of an event is not sequential with that last event that you retrieved for the target device, perform another GET /events to request the events that are associated with all the sequence numbers that you missed.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response body contains .CSV data. The key definitions are listed in the following table.

Attributes	Type	Description
action	Integer	Action category. This can be one of the following values. • **100**. NONE • **200**. TOPOLOGY • **300**. IP • **400**. INVENTORY If not available, an empty string is returned.
args	Array of string	List of dynamic arguments in the event message string. If not available, an empty string is returned. If not available, an empty string is returned.
bayText	String	
chassisText	String	
cn	String	Event Sequence number. It is the order in which the events were processed.

Attributes	Type	Description
commonEventID	String	Common event ID.
componentID	Array of string	Unique ID of the component on which the event occurred. If not available, an empty string is returned.
componentIdentifierText	String	The component description. This can be one of the following values. • **Canister/Appliance** • **Client Data Storage Device** • **Cooling** • **Device Driver** • **Display** • **Hypervisor** • **I/O connectivity** • **Interconnect (Fabric)** • **Interconnect (Interfaces)** • **Interconnect (Networking)** • **Interconnect (PCI Manager)** • **Interconnect (PIE)** • **Interconnect (Utilities / Infrastructure)** • **Memory** • **OS** • **OS/Hypervisor Interface** • **Power** • **Processing** • **Storage RAID** • **System board** • **Systems Management** • **Time Reference** • **Unknown** • **Vendor Events** • **VPD**
decriptionArgs	Array of strings	List of dynamic arguments in the event message description. If not available, an empty string is returned.
eventClass	Integer	The source of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch If not available, an empty string is returned.
eventDate	String	Time and date that the event was created on source system. This is the time and date from the managed system and might be quite different from **timeStamp**, which is when the event was processed by the Lenovo XClarity Administrator. The string is in ISO-8601 format: `yyyy-MM-dd'T'HH:mm:ss'Z'`
eventID	String	Event ID is a unique identifier for each event supported by a product.
eventSourceText	String	

Attributes	Type	Description
failFRUNames	Array of strings	For hardware fault events, includes names of one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUPartNumbers	Array of strings	For hardware fault events, includes part numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUs	Array of strings	For hardware fault events, includes FRU numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUUUIDs	Array of strings	For hardware fault events, includes UUIDs for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failSNs	Array of strings	For hardware fault events, includes serial numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
flags	Array of strings	Proprietary event flag definitions. This can be one of the following values. • **Hidden**. The event not to be displayed in normal log views. It is displayed only for diagnostic views. • **Historical**. The event occurred while the management server was down and can be ignored by EventActions. • **Ignored**. The event is ignored. • **Recovered**. The event was involved in the reliable event recovery process. • **Unsequenced**. Switch system traps are not sequenced. Reliable event recovery is skipped. • **VM**. VM Migration (Blade "Trust the Source Logging Model") If not available, an empty string is returned.
fruSerialNumberText	String	
groupName	Array of strings	List of resource-groups, by name, to which the source of the event belongs. If the source does not belong to a resource group, the value is “Not Available.”
groupUUID	Array of strings	List of resource-groups, by UUID, to which the source of the event belongs.
localLogID	String	Log type. This can be one of the following values. • **AUDIT**. Audit events • **EVENT**. All other events.
localLogSequence	Integer	Log Sequence Number, which uniquely identifies this event on the audit or event log If not available, an empty string is returned.
location	String	Location information for event association in the format of “Slot#01.”
msg	String	Event message string.
msgID	String	Event message ID.
mtm	String	System machine type and model of the managed system on which the event occurred.
originatorUUID	String	The unique ID of the managed system on which the event occurred.
Attributes	Object	Reserved. If not available, an empty string is returned.

Attributes	Type	Description
senderUUID	String	
serialnum	String	Serial number of system generating the event (event source). Not set for internal events.
service	Integer	Identifer that specifies how service is performed. It can be one of the following. • **100**. Not Serviceable. • **200**. Serviceable by Lenovo (called home) • **300**. Serviceable by the customer If not available, an empty string is returned.
serviceabilityText	String	
severity	Integer	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred. If not available, an empty string is returned.
severityText	String	Severity text. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred. If not available, an empty string is returned.
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
sourceLogID	String	Identifier of log of event source system. System may have multiple logs for events and this identifier is used with the System Log Sequence Number for reliable event support.
sourceLogSequence	Integer	Source Log Sequence Number, uniquely identifies this event in source Log ID
systemFruNumberText	String	
systemName	String	System identifier. It correlates to the display name used for the device on the CMM.
systemSerialNumberText	String	
systemText	String	
systemTypeModelText	String	
systemTypeText	String	
timeStamp	String	Time and date of when the log entry was created for the Lenovo XClarity Administrator log. The string is in ISO-8601 format (for example, `yyyy-MM-dd'T'HH:mm:ss'Z'`).

Attributes	Type	Description
typeText	String	
userActionArgs	Array of strings	List of dynamic arguments in the event message action If not available, an empty string is returned.
userid	String	For internal audit events, this is the associated user ID. This is not available for external events.
userIDIndex	Integer	

The following example is returned if the request is successful.

```
"Sequence ID", "Type", "Severity", "Time Stamp", "Source ID", "Originator UUID", "Component ID",
"Source Log ID", "Local Log ID", "Local Log Sequence", "Event Code", "Event Date", "Message ID",
"Event Message", "Serial Number", "Mtm", "Service", "Action", "Location", "User ID",
"Source Log Sequence", "Flags", "Fail SNs", "Fail FRUs",

"151", "SYSTEM", "INFORMATIONAL", "1424290017496", "63E29269BB634AB9A610D6F8FCE2B28F", "",
"4378eb1f6cf111e4bf1fb0ffa5d3ca74", "LENOVO:CMM01:Y030BG4BA020:01", "EVENT", "83", "0001608C",
"1423627952000", "CMM0207", "SSH host key auto-generation started.", "", "", "NONE", "", "01010201",
"", "14707", "Recovered", "", ""
```

/events/csv/eventsLogs

Use this REST API to retrieve the Lenovo XClarity Administrator event log and audit log in a .CSV format.

HTTP methods

GET

GET /events/csv/eventsLogs

Use this method to return the event log and audit log in .CSV format.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/csv/eventsLogs
```

Query parameters

Parameters	Required / Optional	Description
filterWith=*{filter}*	Optional	Returns only the events that apply to the specified filters (see Filtering events)

Request header

Attributes	Required / Optional	Description

Range	Optional	Request the events with the given range of sequence numbers. If the range goes beyond the actual available sequence numbers, the start of the range through the last sequence number is returned. For example:
		`GET /events`
		`Range: item=0-24`
		`--------`
		`Response Header:`
		`Content-Range: 0-24/3000`
		Note: When retrieving events from Lenovo XClarity Administrator, use the sequence numbers to verify that no events are missing. If the sequence number of an event is not sequential with that last event that you retrieved for the target device, perform another GET /events to request the events that are associated with all the sequence numbers that you missed.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response body contains .CSV data. The key definitions are listed in the following table.

Attributes	Type	Description
action	Integer	Action category. This can be one of the following values. • **100**. NONE • **200**. TOPOLOGY • **300**. IP • **400**. INVENTORY If not available, an empty string is returned.
args	Array of string	List of dynamic arguments in the event message string. If not available, an empty string is returned. If not available, an empty string is returned.
bayText	String	
chassisText	String	
cn	String	Event Sequence number. It is the order in which the events were processed.
commonEventID	String	Common event ID.

Attributes	Type	Description
componentID	Array of string	Unique ID of the component on which the event occurred. If not available, an empty string is returned.
componentIdentifierText	String	The component description. This can be one of the following values. • **Canister/Appliance** • **Client Data Storage Device** • **Cooling** • **Device Driver** • **Display** • **Hypervisor** • **I/O connectivity** • **Interconnect (Fabric)** • **Interconnect (Interfaces)** • **Interconnect (Networking)** • **Interconnect (PCI Manager)** • **Interconnect (PIE)** • **Interconnect (Utilities / Infrastructure)** • **Memory** • **OS** • **OS/Hypervisor Interface** • **Power** • **Processing** • **Storage RAID** • **System board** • **Systems Management** • **Time Reference** • **Unknown** • **Vendor Events** • **VPD**
decriptionArgs	Array of strings	List of dynamic arguments in the event message description. If not available, an empty string is returned.
eventClass	Integer	The source of the event. This can be one of the following values. • **50**. Unknown • **200**. Audit • **300**. Cooling • **400**. Power • **500**. Disks (storage) • **600**. Memory • **700**. Processor • **800**. Rack or tower server • **900**. Test • **1000**. Adapter card • **1100**. Expansion board • **1200**. Flex System switch • **1300**. Flex System server • **1400**. switch If not available, an empty string is returned.
eventDate	String	Time and date that the event was created on source system. This is the time and date from the managed system and might be quite different from **timeStamp**, which is when the event was processed by the Lenovo XClarity Administrator. The string is in ISO-8601 format: `yyyy-MM-dd'T'HH:mm:ss'Z'`
eventID	String	Event ID is a unique identifier for each event supported by a product.
eventSourceText	String	

Attributes	Type	Description
failFRUNames	Array of strings	For hardware fault events, includes names of one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUPartNumbers	Array of strings	For hardware fault events, includes part numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUs	Array of strings	For hardware fault events, includes FRU numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failFRUUUIDs	Array of strings	For hardware fault events, includes UUIDs for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
failSNs	Array of strings	For hardware fault events, includes serial numbers for one or more FRUs that are associated with the fault. If not available, an empty string is returned.
flags	Array of strings	Proprietary event flag definitions. This can be one of the following values. • **Hidden**. The event not to be displayed in normal log views. It is displayed only for diagnostic views. • **Historical**. The event occurred while the management server was down and can be ignored by EventActions. • **Ignored**. The event is ignored. • **Recovered**. The event was involved in the reliable event recovery process. • **Unsequenced**. Switch system traps are not sequenced. Reliable event recovery is skipped. • **VM**. VM Migration (Blade "Trust the Source Logging Model") If not available, an empty string is returned.
fruSerialNumberText	String	
groupName	Array of strings	List of resource-groups, by name, to which the source of the event belongs. If the source does not belong to a resource group, the value is “Not Available.”
groupUUID	Array of strings	List of resource-groups, by UUID, to which the source of the event belongs.
localLogID	String	Log type. This can be one of the following values. • **AUDIT**. Audit events • **EVENT**. All other events.
localLogSequence	Integer	Log Sequence Number, which uniquely identifies this event on the audit or event log If not available, an empty string is returned.
location	String	Location information for event association in the format of “Slot#01.”
msg	String	Event message string.
msgID	String	Event message ID.
mtm	String	System machine type and model of the managed system on which the event occurred.
originatorUUID	String	The unique ID of the managed system on which the event occurred.
Attributes	Object	Reserved. If not available, an empty string is returned.

Attributes	Type	Description
senderUUID	String	
serialnum	String	Serial number of system generating the event (event source). Not set for internal events.
service	Integer	Identifer that specifies how service is performed. It can be one of the following. • **100**. Not Serviceable. • **200**. Serviceable by Lenovo (called home) • **300**. Serviceable by the customer If not available, an empty string is returned.
serviceabilityText	String	
severity	Integer	Severity. This can be one of the following values. • **100**. Unknown. The severity is unknown. • **200**. Informational. Informational • **300**. Warning. User can decide if action is needed. • **400**. Minor. Action is needed, but the situation is not serious at this time. • **500**. Major. Action is needed now. • **600**. Critical. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **700**. Fatal. A non-recoverable error has occurred. If not available, an empty string is returned.
severityText	String	Severity text. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred. If not available, an empty string is returned.
sourceID	String	System UUID for the system or device that is/was the event source (raiser/owner)
sourceLogID	String	Identifier of log of event source system. System may have multiple logs for events and this identifier is used with the System Log Sequence Number for reliable event support.
sourceLogSequence	Integer	Source Log Sequence Number, uniquely identifies this event in source Log ID
systemFruNumberText	String	
systemName	String	System identifier. It correlates to the display name used for the device on the CMM.
systemSerialNumberText	String	
systemText	String	
systemTypeModelText	String	
systemTypeText	String	
timeStamp	String	Time and date of when the log entry was created for the Lenovo XClarity Administrator log. The string is in ISO-8601 format (for example, `yyyy-MM-dd'T'HH:mm:ss'Z'`).

Attributes	Type	Description
typeText	String	
userActionArgs	Array of strings	List of dynamic arguments in the event message action If not available, an empty string is returned.
userid	String	For internal audit events, this is the associated user ID. This is not available for external events.
userIDIndex	Integer	

The following example is returned if the request is successful.

```
"Sequence ID", "Type", "Severity", "Time Stamp", "Source ID", "Originator UUID", "Component ID",
"Source Log ID", "Local Log ID", "Local Log Sequence", "Event Code", "Event Date", "Message ID",
"Event Message", "Serial Number", "Mtm", "Service", "Action", "Location", "User ID",
"Source Log Sequence", "Flags", "Fail SNs", "Fail FRUs",

"151", "SYSTEM", "INFORMATIONAL", "1424290017496", "63E29269BB634AB9A610D6F8FCE2B28F", "",
"4378eb1f6cf111e4bf1fb0ffa5d3ca74","LENOVO:CMM01:Y030BG4BA020:01", "EVENT", "83", "0001608C",
"1423627952000", "CMM0207", "SSH host key auto-generation started.", "", "", "NONE", "", "01010201",
"", "14707", "Recovered", "", ""
```

/events/exclusionfilters

Use this REST API to retrieve information about, create, and modify event exclusion filters. *Exclusion filters* are used to exclude events or alerts on the Lenovo XClarity Administrator user interface and not have any actions taken on them when received, if those events are of no interest for managing remote systems.

HTTP methods

GET, PUT, POST

GET /events/exclusionfilters

Use this method to return information about all event exclusion filters, regardless of whether they are currently enabled or disabled.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/exclusionfilters`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
description	String	Optional description for the exclusion filter
eventFilter	Array	Event filter information
fields	Object	Fields to filter on and the associated REGEX string to filter. The event fields must match one of the supported fields in the event class (see Filtering events).
filterType	String	Type of filter. This can be one of the following values. • **FIELDREGEXAND**. Event filter matches only if all fields find a match with the given field REGEX. • **FIELDREGEXOR**. Event filter matches if *any* field finds a match with the given field REGEX. • **FIELDREGEXNOT**. Event filter matches only if all fields do *not* find a match with the given field REGEX.
id	String	Unique ID assigned to the exclusion filter when it is configured
name	String	User-defined name for the exclusion filter. This must be unique for all monitors.
state	String	Current state of the exclusion filter. This can be one of the following values. • **disabled** • **enabled**
type	String	Event type. This can be one of the following values. • **activeAlert** • **event**

The following example is returned if the request is successful.

```
[{
   "description": "A DHCP issued IP address was changed on eth0",
   "eventFilter": {
      "fields": [{
         "field": "eventID",
         "value": "FQXHMCR0001W"
      }],
      "filterType": "FIELDREGEXOR"
   },
   "id": "XFT:1",
   "name": " z543oy0",
   "state": "enabled",
   "type": "event"
},
{
   "description": "Connectivity to chassis 4p3cmm has been restored. UUID is
                   FFB657408BEB4161950704AB0ED3A84A.",
   "eventFilter": {
      "fields": [{
```

```
            "field": "eventID",
            "value": "FQXHMDM0004I"
        },
        {
            "field": "sourceID",
            "value": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
        }]
        "filterType": "FIELDREGEXAND",
    },   "id": "XFT:2",
    "name": " 53sr900",
    "state": "enabled",
    "type": "event"
}]
```

POST /events/exclusionfilters

Use this method to exclude events or alerts that are of no interest for managing devices and no actions need to be taken when the events or alerts are received.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/events/exclusionfilters`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
description	Required	String	User-defined description

eventFilter	Required	Array of objects	Event filters. Each object that contain the following attributes.
			`{`
			`"filterType": "{filter_type}",`
			`"fields": [{`
			`"field": "{filter}",`
			`"operation": "{operation}",`
			`"value": "{value}"`
			`}]`
			`}`
			For more information, see Filtering events.

name	Required	String	User defined name for the exclusion filter **Note:** This name must be unique.
type	Required	String	Type of exclusion filter. This can be one of the following values. • **event** • **activeAlert**

The following example ignores all FQXHMCP5810I events on all devices in two specific groups.

```
{
   "description": "Ignore all FIELDREGEXAND events from devices in specific groups",>,
```

```
   "eventFilter": {
      "filterType": "FIELDREGEXAND",
      "fields": [{
         "field": "eventID",
         "value": "FQXHMCP5810I",
      },
      {
         "field"  "groupUUID",
         "value": ["FFB657408BEB4161950704AB0ED3A84A","FFB657408BEB4161950704AB0ED3A84B"]
      }]
   },
   "name": "group events",
   "type": "event"
}
```

The following example ignores all alerts from server 65AEDE9C03B311E18A2AC4C1BD6B35B2.

```
{
   "description": "Ignore all events from server 65AEDE9C03B311E18A2AC4C1BD6B35B2",
   "eventFilter": {
      "filterType": "FIELDREGEXAND",
      "fields": [{
         "field": "sourceID",
         "value": "65AEDE9C03B311E18A2AC4C1BD6B35B2"
      }]
   },
   "name": "65AEDE9C03B311E18A2AC4C1BD6B35B2 alerts",
   "type": "activeAlert"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	String	Unique ID of the exclusion-filter

The following example is returned if the request is successful.

```
{
   "id": "AUG:XFT:0"
}
```

PUT /events/exclusionfilters

Use this method to modify event exclusion filters after they are configured without requiring that they be deleted and re-added. When editing an exclusion filter, the ID of the updated exclusion filter is included in the response.

All attributes in the exclusion filter can be changed. For example, a monitor could be temporarily disabled and then enabled again at a later time.

Authentication

Authentication with username and password is required.

Request URL

```
PUT https://{management_server_IP}/events/exclusionfilters
```

Query parameters

None

Request body

Attributes	Required / Optional	Type	Definition
description	Optional	String	Optional description for the exclusion filter
eventFilter	Required	Array	Event filter information
fields	Optional	Object	Fields to filter on and the associated REGEX string to filter. The event field must match one of the supported fields in the event class (see Filtering events).
filterType	Optional	String	Type of filter. This can be one of the following values: • **FIELDREGEXAND**. Event filter matches only if all fields find a match with the given field REGEX. • **FIELDREGEXOR**. Event filter matches if *any* field finds a match with the given field REGEX. • **FIELDREGEXNOT**. Event filter matches only if all fields do *not* find a match with the given field REGEX.
id	Required	String	Unique ID assigned to the exclusion filter when it is configured
name	Required	String	User-defined name for the exclusion filter. This must be unique for all monitors.
state	Optional	String	Current state of the exclusion filter. This can be one of the following values. • **disabled** • **enabled**
type	Required	String	Event type. This can be one of the following values. • **activeAlert** • **event**

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

If successful, response includes a JSON object that contains the ID for the exclusion filter along with other optional attributes.

/events/exclusionfilters/*{filter_id}*

Use this REST API to remove a specific exclusion filter. *Exclusion filters* are used to exclude events or alerts on the Lenovo XClarity Administrator user interface and not have any actions taken on them when received, if those events are of no interest for managing remote systems.

HTTP methods

DELETE

DELETE /events/exclusionfilters/*{filter_id}*

Use this method to remove a specific exclusion filter.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/exclusionfilters/{filter_id}`

where *{filter_id}* is the ID of the exclusion filter to be deleted. To obtain the filter ID, use the GET /events/exclusionfilters method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/helptext/*{event_id}*

Use this REST API to return the description and recovery action for a specific event.

HTTP methods

GET

GET /events/helptext/*{event_id}*

Use this method to return the description and recovery action for a specific event.

For message-description and user-action text in the job summary, you can specify the text directly in the request body if no translations are needed, or you can reference the text from a translated bundle file (for example, `com.lenovo.lxca.server.jobs.bundle.jobsSummary`).

When the job description and recovery actions require formatted text, you must specify the text as an array of objects in JSON format. You cannot use HTML.

Tip: In the translated bundle files, braces {} must be escaped by a single quote for help text (for example, `'{'`).

Attribute	Required / Optional	Type	Description
format	Required	Array of strings	List of formats for the text. This can be one of the following values. • **bold**. Corresponds to the <b> HTML tag. • **italic**. Corresponds to the <i> HTML tag. • **underline**. Corresponds to the <u> HTML tag. • **link**. Corresponds to the <a> HTML tag. • **newline**. Corresponds to the HTML tag. • **paragraph**. Corresponds to the <p> HTML tag. • **quotation**. Corresponds to the <q> HTML tag. • **orderedList**. Corresponds to the HTML tag. • **bulletList**. Corresponds to the HTML tag. • **listElement**. Corresponds to the HTML tag. If no format is needed, use an empty array.
link	Optional	String	URL to be linked to
text	Required	String or array of strings	Text to be formatted

The following example has formatted text in the user action. It includes paragraphs, ordered list, unordered list, link, and formatted text. Note that braces {} must be escaped by a single quote for help text (for example, `'{'`).

```
['{'
   "text": "To display the text correctly, the following steps are made.",
   "format": []
'}',
'{'
   "text": [],
   "format": ["newline"]
'}',
'{'
   "text": ['{'
      "text": "Segment the text into pieces between HTML tags.",
```

```
      "format": ["listElement"]
   '}',
   '{'
      "text": ['{'
         "text": "If the segmented text contains ",
         "format": []
      '}',
      '{'
         "text": "multiple tags",
         "format": ["bold"]
      '}',
      '{'
         "text": ", segment them as well.",
         "format": []
      '}' ],
      "format": ["listElement"]
   '}',
   '{'
      "text": ['{'
         "text": "After having all segments, add the tags as follows:",
         "format": []
      '}',
      '{'
         "text": ['{'
            "text": "Add the text between the tags in the text field of JSON. If multiple tags are found,
                     text field is an array of JSON Objects.",
            "format": ["listElement"]
         '}',
         '{'
            "text": "Add the format for each text between tags.",
            "format": ["listElement"]
         '}' ],
         "format": ["bulletList"]
      '}'],
      "format": ["listElement"]
   '}',
   '{'
      "text": "Make sure this is a json format.",
      "format": ["listElement", "bold", "underline"]
   '}' ],
   "format": ["orderedList"]
'}',
'{'
   "text": [],
   "format": ["newline"]
'}',
'{'
   "text": ['{'
      "text": "This is how a paragraph looks like with a ",
      "format": []
   '}',
   '{'
      "text": "link",
      "format": ["link"],
      "link": "https://www3.lenovo.com/"
   '}' ],
   "format": ["paragraph"]
'}',
'{'
   "text": "This is how the result should look.",
   "format": ["paragraph", "italic"]
```

```
'}']
```

This example correlates to the following HTML format

```
To display the text correctly, the following steps are made.
<br></br>
<ol>
<li>Segment the text into pieces between HTML tags.</li>
<li>If the segmented text contains <b>multiple tags</b>, segment them as well.</li>
<li>After having all segments, add the tags as follows:
<ul>
<li>Add the text between the tags in the text field of JSON. If multiple tags are found,
text field is an array of JSON Objects.</li>
<li>Add the format for each text between tags.</li>
</ul></li>
<li><b><u>Make sure this is a json format.</u></b></li>
</ol>
<br></br>
<p>This is how a paragraph looks like with a <a href="https://www3.lenovo.com/">link</a></p>
<p><i>This is how the result should look.</i></p>
```

This example correlates to the following formatted output:

To display the text correctly, the following steps are made.

1. Segment the text into pieces between HTML tags.
2. If the segmented text contains **multiple tags**, segment them as well.
3. After having all segments, add the tags as follows:
    - Add the text between the tags in the text field of JSON. If multiple tags are found, text field is an array of JSON Objects.
    - Add the format for each text between tags.
4. **Make sure this is a json format.**

This is how a paragraph looks like with a link

This is how the result should look.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/helptext/{event_id}`

where <*event_id}* is the sequence number of the event to be retrieved. To obtain the event sequence number, use the **cn** attribute that is returned by the GET /events method).

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
description	Array of objects	Information about the message descriptions
format	Array of strings	
text	String	Event description
useraction	Array of objects	Information about the recovery actions
format	Array of strings	
text	String	Recovery actions to resolve the event

The following example is returned if the request is successful.

```
{
   "description": [{
      "format": [],
      "text": "The specified user cannot log in."
   }],
   "useraction": [{
      "format": [],
      "text": "Information only; no action is required."
   }]
}
```

/events/monitors

Use this REST API to retrieve information about, create, and modify event forwarders.

Event forwarders are used to provide a remote location and protocol to which events are forwarded. Every generated event is monitored to see if it matches the configured filter. If it matches, the event is forwarded to the specified location using the indicated protocol.

Several forwarding protocols are supported for event forwarders.

The following protocols are supported:

- **Azure Log Analytics**. Lenovo XClarity Administrator forwards the monitored events to over the network to Microsoft Azure Log Analytics.
- **Email**. Lenovo XClarity Administrator forwards the monitored events to one or more email addresses using SMTP. The email contains information about the event, the host name of the source device, and links to the Lenovo XClarity Administrator web interface and Lenovo XClarity Mobile app.
- **FTP**. Forwards monitored events over the network to an FTP server.
- **REST**. Lenovo XClarity Administrator forwards the monitored events over the network to a REST Web Service.
- **SNMP**. Lenovo XClarity Administrator forwards the monitored events over the network to a remote SNMP manager. SNMPv1 and SNMPv3 traps are supported.

  For information about the management information base (MIB) file that describes the SNMP traps Lenovo XClarity Administrator generates, see lenovoMgrAlert.mib file in the Lenovo XClarity Administrator online documentation.
- **Syslog**. Lenovo XClarity Administrator forwards the monitored events over the network to a central log server where native tools can be used to monitor the syslog.

HTTP methods

GET, PUT, POST

GET /events/monitors

Use this method to return information about all enabled and disabled event forwarders.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/monitors
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The attributes that are returned vary depending on the type of recipient to which events are forwarded.

- Table 78 “Azure Log Analytics” on page 961

- Table 79 “Email service using SMTP” on page 965
- Table 80 “FTP server” on page 970
- Table 81 “REST Web Service” on page 974
- Table 82 “Remote SNMPv1 or SNMPv3 manager” on page 978
- Table 83 “Syslog” on page 983

Table 78. Azure Log Analytics

Attributes	Type	Description
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.

Table 78. Azure Log Analytics (continued)

Attributes	Type	Description
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder
matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarder.
outputFormat	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	String	TCP/UDP port used for the connection. For Azure Log Analytics, this value is always **443**.

Table 78. Azure Log Analytics (continued)

primaryKey	String	Primary key of the log-analytics device that is obtained from the Azure portal.
protocol	String	Type of event forwarder. For Azure Log Analytics, this value is always **oms_log_analytics**.
requestTimeout	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out. By default, the time-out value is 30 seconds.
scheduler	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Array of objects	List of event-fowarding schedules
calendar	String	Schedule name
daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
endingDate	String	Date when the schedule ends
endTime	String	Time when the schedule ends
id	Integer	Schedule ID
initialEndTime	String	
initialStartTime	String	
repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
seriesId	Integer	Schedule index
startingDate	String	Date when the schedule starts
startTime	String	Time when the schedule starts
summary	Boolean	
showSummary	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.
workspaceID	String	Workspace ID of the log-analytics device that is obtained from the Azure portal.

The following example is returned if the request is successful for event forwarders to Azure Log Analytics.


```
[{
    "createdBy": "ADMIN",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "resourceGroupsUUIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "id": "1520009819404",
    "ignoreExcluded": false,
    "ipAddress": "3268497b-7842-4a00-a9b8-8128e125e916.ods.opinsights.azure.com",
    "lastEditBy": "ADMIN",
    "matchEverything": true,
    "name": "ALA_forwarder",
    "outputFormat": "{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",
                        \"Serialnum\":\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",
                        \"Flags\":\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",
                    \"LocalLogID\":\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",
                    \"SystemName\":\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",
                    \"FailFRUs\":\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",
                    \"SourceID\":\"[[EventSourceUUID]]\",
                    \"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
                    \"FailSNs\":\"[[EventFailSerialNumbers]]\",
                    \"FailFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",
                    \"ComponentID\":\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",
                    \"MsgID\":\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",
                    \"TimeStamp\":\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],
                    \"Service\":\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",
                    \"EventDate\":\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",
                    \"DeviceSerialNumber\":\"[[DeviceSerialNumber]]\",
                    \"DeviceIPAddress\":\"[[DeviceIPAddress]]\",\"LXCA\":\"[[LXCA_IP]]\"}",
    "port": "58443",
    "primaryKey": "BA7qbCEy7tsTVJ0S3LMATXKXeoHrdPvOx4CfzcnsgM3qKYjZgph64oIKWH9FuSO1xakjmasW0VGeNAUiGSomuQ==",
    "protocol": "oms_log_analytics",
    "requestTimeout": 30,
    "scheduler": {
        "showSummary": false,
        "enabled": false,
        "events": []
    },
    "workspaceID": "3268497b-7842-4a00-a9b8-8128e125e916"
}]
```

Table 79. Email service using SMTP

Attributes	Type	Description
authenticationEmail	String	Authentication type. This can be one of the following values. • **Regular**. Authenticates to the specified SMTP server using the specified user ID and password. • **NTLM**. Uses the NT LAN Manager (NTLM) protocol to authentication to the specified SMTP server using the specified user ID, password, and domain name. • **OAUTH2**. Uses the Simple Authentication and Security Layer (SASL) protocol to authenticate to the specified SMTP server using the specified user name and security token. Typically, the user name is your email address. **Attention:** The security token expires after a short time. It is your responsibility to refresh the security token. • **None**. No authentication is used.
connectionEmail	Array of strings	Connection type to secure connection to the SMTP server. This can be one of the following values. • **SSL**. Use the SSL protocol while communicating. • **TLS**. Uses TLS to form a secure communication over an unsecure channel.
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder.
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource

Table 79. Email service using SMTP (continued)

Attributes	Type	Description
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder
matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarder.

Table 79. Email service using SMTP (continued)

outputFormat		String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port		String	TCP/UDP port used for the connection. For email, this value is always **25**.
protocol		String	Type of event forwarder. For email, this value is always **email_alert**.
recipients		Array of strings	List of email addresses for the event forwarder, in the format *userid@domain* (for example, `XClarity1@company.com`)
requestTimeout		Integer	The amount of time, in seconds, that an event forwarder has to forward events before the request times out. By default, the time-out value is 30 seconds.
scheduler		Object	Information about times and days when you want the specified events to be forwarded to this event forwarder recipient
	enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events	Array of objects	List of event-fowarding schedules
		calendar	String	Schedule name
		daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	String	Date when the schedule ends
		endTime	String	Time when the schedule ends
		id	Integer	Schedule ID
		initialEndTime	String	
		initialStartTime	String	
		repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Integer	Schedule index
		startingDate	String	Date when the schedule starts
		startTime	String	Time when the schedule starts

Table 79. Email service using SMTP (continued)

summary	Boolean	
showSummary	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.
senderDomain	String	Sender domain (for example, company.com) If you do not specify the **senderDomain** or **senderUserName**, this is `LXCA.`*{source_identifier}*`@`*{smtp_host}* by default. If you specify the **senderDomain** but not **senderUserName**, the format of the sender address is *{LXCA_host_name}@{sender_domain}* (for example, XClarity1@company.com).
senderUserName	String	Sender name
subjectFormat	String	Email subject For a description of fields that can be specified in the subject format, use GET /events/monitors?format=defaultFormat.
useSupportContact	Boolean	Indicates to use the email address that is defined for the support contact that is assigned to the device. This can be one of the following values. • **true**. Email forwarder uses the email address for the support contact. • **false**. (default) Email forwarder uses the email addresses that are specified in the **recipients** attribute.

The following example is returned if the request is successful for event forwarders to email services.


```
[{
    "authenticationEmail": "none",
    "connectionEmail": ["SSL"],
    "createdBy": "ADMIN",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY","STATUS_CHANGE","STATUS_UPDATE","GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": ["none","support","user"],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "resourceGroupsUUIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "UNKNOWN"
            },
            {
                "severity": "WARNING",
                "type": "UNKNOWN"
            },
            {
                "severity": "MINOR",
                "type": "UNKNOWN"
            },
            ...,
```

```
        {
            "severity": "FATAL",
            "type": "AUDIT"
        }]
    }
  },
  "forwardHidden": false,
  "id": "1520009765759",
  "ignoreExcluded": false,
  "ipAddress": "192.0.2.20",
  "lastEditBy": "ADMIN",
  "matchEverything": true,
  "name": "email forwarder",
  "outputFormat": "Alert: [[EventDate]] [[EventMessage]]\n
                  \n
                  Hardware Information:\n
                  Managed Endpoint     : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
                  Device name          : [[DeviceName]]\n
                  Product name         : [[DeviceProductName]]\n
                  Host name            : [[DeviceHostName]]\n
                  Machine Type         : [[DeviceMachineType]]\n
                  Machine Model        : [[DeviceMachineModel]]\n
                  Serial Number        : [[DeviceSerialNumber]]\n
                  DeviceHealthStatus   : [[DeviceHealthStatus]]\n
                  IPv4 addresses       : [[DeviceIPV4Addresses]]\n
                  IPv6 addresses       : [[DeviceIPV6Addresses]]\n
                  Chassis              : [[DeviceChassisName]]\n
                  DeviceBays           : [[DeviceBays]]\n
                  \n
                  LXCA is: [[ManagementServerIP]]\n
                  \n
                  Event Information:\n
                  Event ID          : [[EventID]]\n
                  Common Event ID   : [[CommonEventID]]\n
                  EventSeverity     : [[EventSeverity]]\n
                  Event Class       : [[EventClass]]\n
                  Sequence ID       : [[EventSequenceID]]\n
                  Event Source ID   : [[EventSourceUUID]]\n
                  Component ID      : [[EventComponentUUID]]\n
                  Serial Num        : [[EventSerialNumber]]\n
                  MTM               : [[EventMachineTypeModel]]\n
                  EventService      : [[EventService]]\n
                  Console link      : [[ConsoleLink]]\n
                  iOS link          : [[iOSLink]]\n
                  Android link      : [[AndroidLink]]\n
                  System Name       : [[DeviceFullPathName]]
                  \n",
  "port": "25",
  "protocol": "email_alert",
  "recipients": "user1@company.com",
  "requestTimeout": 30,
  "scheduler": {
      "enabled": false,
      "events": [],
      "showSummary": false
  },
  "senderDomain": "company.com",
  "senderUserName": "LXCA1",
  "subjectFormat": "[[DeviceName]]-[[EventMessage]]",
  "useSupportContact": false
}]
```

Table 80. FTP servers

Attributes	Type	Description
authUser	Boolean	Authentication user ID if authentication is used
characterEncoding	String	Character set. This can be one of the following values. • **UTF-8**. (default) • **Big5**
charactersToRemove	String	Sequence of characters to be removed from the file content
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.

Table 80. FTP servers (continued)

Attributes	Type	Description
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ftpAuthentication	String	Authentication type. This can be one of the following values. • **Regular**. Authenticates to the specified SMTP server using the specified user ID and password. This is the same as basic authentication. • **None**. (default) No authentication is used. This is the same as anonymous authentication.
ftpFileName	String	File-name format to use for the file that contains the forwarded event. The default format is `event_[[EventSequenceID]].txt`. **Note:** Each file contains information for a single event.
ftpPath	String	Path on the remote FTP server where the file is to be uploaded
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder

Table 80. FTP servers (continued)

matchEverything		Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name		String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat		String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port		String	TCP/UDP port used for the connection. For FTP, this value is always **21**.
protocol		String	Type of event forwarder. For FTP, this value is always **ftp**.
requestTimeout		Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler		Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events	Array of objects	List of event-forwarding schedules
		calendar	String	Schedule name
		daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	String	Date when the schedule ends
		endTime	String	Time when the schedule ends
		id	Integer	Schedule ID
		initialEndTime	String	
		initialStartTime	String	
		repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Integer	Schedule index
		startingDate	String	Date when the schedule starts

Table 80. FTP servers (continued)

			startTime	String	Time when the schedule starts
			summary	Boolean	
	showSummary			String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example is returned if the request is successful for event forwarders to FTP servers.


```
[{
    "authUser": "admin",
    "characterEncoding": "UTF-8",
    "charactersToRemove": null,
    "createdBy": "ADMIN",
    "description": "",
    "enable": "false",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }],
        }
    },
    "forwardHidden": false,
    "ftpAuthentication": "REGULAR",
    "ftpFileName": "event_[[EventSequenceID]].txt",
    "ftpPath": "lxca_events",
    "id": "1534862502642",
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.30",
    "lastEditBy": "ADMIN",
    "matchEverything": true,
    "name": "FTP_forwarder",
    "outputFormat": "Alert: [[EventDate]] [[EventMessage]]\n\nHardware Information:\n
                        Managed Endpoint      : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
                          Device name          : [[DeviceName]]\n
                          Product name         : [[DeviceProductName]]\n
                          Host name            : [[DeviceHostName]]\n
                          Machine Type         : [[DeviceMachineType]]\n
                          Machine Model        : [[DeviceMachineModel]]\n
                          Serial Number        : [[DeviceSerialNumber]]\n
                          DeviceHealthStatus   : [[DeviceHealthStatus]]\n
                          IPv4 addresses       : [[DeviceIPV4Addresses]]\n
                          IPv6 addresses       : [[DeviceIPV6Addresses]]\n
```

```
                        Chassis                 : [[DeviceChassisName]]\n
                        DeviceBays              : [[DeviceBays]]\n
                       \n
                       LXCA is: [[ManagementServerIP]]\n
                       \n
                          Event Information:\n
                            Event ID            : [[EventID]]\n
                            Common Event ID : [[CommonEventID]]\n
                            EventSeverity    : [[EventSeverity]]\n
                            Event Class       : [[EventClass]]\n
                            Sequence ID       : [[EventSequenceID]]\n
                            Event Source ID : [[EventSourceUUID]]\n
                            Component ID     : [[EventComponentUUID]]\n
                            Serial Num        : [[EventSerialNumber]]\n
                            MTM                 : [[EventMachineTypeModel]]\n
                            EventService     : [[EventService]]\n
                            Console link     : [[ConsoleLink]]\n
                            iOS link          : [[iOSLink]]\n
                            Android link     : [[AndroidLink]]\n
                            System Name      : [[DeviceFullPathName]]\n",
    "port": "21",
    "protocol": "ftp",
    "requestTimeout": 30,
    "scheduler": {
        "showSummary": false,
        "enabled": false,
        "events": []
    }
}]
```

Table 81. REST Web Services

Attributes	Type	Description
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**

Table 81. REST Web Services (continued)

Attributes	Type	Description
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarderID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.

Table 81. REST Web Services (continued)

lastEditBy	String	Name of the user that last edited the event forwarder
matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	String	TCP/UDP port used for the connection. For REST Web Services, this value is always **80**.
protocol	String	Type of event forwarder. For REST Web Services, this value is always **rest**.
requestTimeout	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
restAuthentication	String	Authentication type. This can be one of the following values. • **basic**. Authenticates to the specified server using the specified user ID and password. • **none**. No authentication is used.
restMethod	String	REST method to use for forwarding events. This can be one of the following values. • **POST** • **PUT**
restPath	String	Resource path on which the forwarder is to post the events (for example, /rest/test)
restProtocol	String	Protocol to use for forwarding events. This can be one of the following values. • **HTTP** • **HTTPS**
restRequestHeaders	Array of strings	REST header to use for forwarding events
scheduler	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Array of objects	List of event-forwarding schedules
calendar	String	Schedule name

Table 81. REST Web Services (continued)

			daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
			endingDate	String	Date when the schedule ends
			endTime	String	Time when the schedule ends
			id	Integer	Schedule ID
			initialEndTime	String	
			initialStartTime	String	
			repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
			seriesId	Integer	Schedule index
			startingDate	String	Date when the schedule starts
			startTime	String	Time when the schedule starts
			summary	Boolean	
	showSummary			String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example is returned if the request is successful for event forwarders to REST Web Services.

```
[{
    "createdBy": "ADMIN",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "excludedEventIDs": "",
            "eventServices": [],
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
```

```
    },
    "forwardHidden": false,
    "id": "1520009679583",
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.40",
    "lastEditBy": "ADMIN",
    "matchEverything": true,
    "name": "REST_forwarder",
    "outputFormat": "{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",
                        \"serialnum\":\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",
                    \"flags\":\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",
                    \"localLogID\":\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",
                    \"action\":[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",
                    \"severity\":[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
                    \"sourceLogSequence\":[[EventSourceLogSequenceNumber]],
                    \"failFRUSNs\":\"[[EventFailSerialNumbers]]\",
                    \"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",\"eventClass\":[[EventClassNumber]],
                    \"componentID\":\"[[EventComponentUUID]]\",\"mtm\":\"[[EventMachineTypeModel]]\",
                    \"msgID\":\"[[EventMessageID]]\",\"sequenceNumber\":\"[[EventSequenceID]]\",
                    \"timeStamp\":\"[[EventTimeStamp]]\",\"args\":[[EventMessageArguments]],
                    \"service\":[[EventServiceNumber]],\"commonEventID\":\"[[CommonEventID]]\",
                    \"eventDate\":\"[[EventDate]]\"}",
    "port": "80",
    "protocol": "rest",
    "requestTimeout": 30,
    "restAuthentication": "NONE",
    "restMethod": "POST",
    "restPath": "lxca_events",
    "restProtocol": "HTTP",
    "restRequestHeaders": [],
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    }
}]
```


Table 82. Remote SNMPv1 or SNMPv3 manager

Attributes	Type	Description
authPasswordSet	String	Password string. This attribute is required if you specify **authUser**.
authProtocol	String	Authentication protocol. This can be one of the following. • **MD5** • **SHA** This attribute is required if you specify **authUser**.
authUser	String	Authentication user ID if authentication is used
community	String	(SNMPv1 only) The community password that is sent with every SNMP request to the device.
contactName	String	The user-defined contact name for XClarity Administrator traps
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.

Table 82. Remote SNMPv1 or SNMPv3 manager (continued)

Attributes	Type	Description
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.

Table 82. Remote SNMPv1 or SNMPv3 manager (continued)

Attributes	Type	Description
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder
location	String	Location information, such as site, address, and geography
matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
port	String	TCP/UDP port used for the connection. For SNMP, this value is always **162**.
privacyPasswordSet	String	Privacy password. This attribute is required if encryption is used.

Table 82. Remote SNMPv1 or SNMPv3 manager (continued)

privacyProtocol		String	Privacy protocol. This can be one of the following values. • **AES** • **DES** This attribute is required if you specify **privacyPassword**.
protocol		String	Type of event forwarder. For SNMP, this can be one of the following values. • **snmpv1**. Events are forwarded to a remote SNMP manager using SNMPv1. • **snmpv3**. Events are forwarded to a remote SNMP manager using SNMPv3. The trap formats for each event are defined in the lenovoMgrAlert.mib file in the Lenovo XClarity Administrator online documentation.
requestTimeout		Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler		Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events	Array of objects	List of event-fowarding schedules
		calendar	String	Schedule name
		daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	String	Date when the schedule ends
		endTime	String	Time when the schedule ends
		id	Integer	Schedule ID
		initialEndTime	String	
		initialStartTime	String	
		repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Integer	Schedule index
		startingDate	String	Date when the schedule starts
		startTime	String	Time when the schedule starts

Table 82. Remote SNMPv1 or SNMPv3 manager (continued)

	summary	Boolean	
showSummary		String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example is returned if the request is successful for event forwarders to remote SNMP managers.


```
[{
    "authPasswordSet": "false",
    "authProtocol": "NONE",
    "authUser": "",
    "contactName": "",
    "createdBy": "ADMIN",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "id": "1520009466990",
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.50",
    "lastEditBy": "ADMIN",
    "location": "",
    "matchEverything": true,
    "name": "SNMP_forwarder",
    "port": "162",
    "privacyPasswordSet": "false",
    "privacyProtocol": "NONE",
    "protocol": "snmpv3",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": true,
        "events": [{
            "calendar": "Calendar1",
            "daysOfWeek": ["1", "2", "3", "4", "5"],
            "endingDate": "2017-12-31T22:00:00.000Z",
            "endTime": "2017-10-06T21:00:00.000Z",
            "id": 0,
```

```
            "initialEndTime":  "2017-10-06T21:00:00.000Z",
            "initialStartTime":  "2017-10-06T12:00:00.000Z",
            "repeatable":  true,
            "seriesId":  1
            "startingDate":  "2017-10-06T12:00:00.000Z",
            "startTime":  "2017-10-06T12:00:00.000Z",
            "summary":  "Forwarder  (repeatable)",
        }],
        "showSummary":  false
    }
}]
```

Table 83. Syslog

Attributes	Type	Description
communicationProtocol	String	Identifies the type of protocol that the syslog monitor uses to send messages. This can be one of the following values. • **TCP** • **UDP**. (default)
createdBy	String	Name of the user that created the event forwarder
dateFormat	String	Format for the timestamp in the syslog. This can be one of the following values. • **Default_Format**. The default format using local time, for example `Fri Mar 31 05:57:18 EDT 2017`. • **GMT**. International standard (ISO8601) for dates and times, for example `2017-03-31T05:58:20-04:00`.
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded

Table 83. Syslog (continued)

Attributes	Type	Description
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder

Table 83. Syslog (continued)

matchEverything		Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name		String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat		String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port		String	TCP/UDP port used for the connection. For syslog, this value is always **514**.
protocol		String	Type of event forwarder. For syslog, this value is always **syslog**.
requestTimeout		Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler		Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events	Array of objects	List of event-fowarding schedules
		calendar	String	Schedule name
		daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	String	Date when the schedule ends
		endTime	String	Time when the schedule ends
		id	Integer	Schedule ID
		initialEndTime	String	
		initialStartTime	String	
		repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Integer	Schedule index
		startingDate	String	Date when the schedule starts

Table 83. Syslog (continued)

			startTime	String	Time when the schedule starts
			summary	Boolean	
	showSummary			String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example is returned if the request is successful for event forwarders to syslogs.

```
[{
    "communicationProtocol": "UDP",
    "createdBy": "ADMIN",
    "dateFormat": "Default_Format",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "id": "1520009382682",
    "ignoreExcluded": true,
    "ipAddress": "192.0.2.60",
    "lastEditBy": "ADMIN",
    "matchEverything": true,
    "name": "syslog_forwarder",
    "outputFormat": "<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]]
                    severity=[[EventSeverity]] class=[[EventClass]] appladdr=[[LXCA_IP]]
                user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
                me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]]
                systemName=[[DeviceFullPathName]] seq=[[EventSequenceID]] EventID=[[EventID]]
                CommonEventID=[[CommonEventID]] [[EventMessage]]",
    "port": "514",
    "protocol": "syslog",
    "requestTimeout": 30,
    "scheduler": {
        "showSummary": false,
        "enabled": false,
        "events": []
    },
}]
```

POST /events/monitors

Use this method to create an event forwarder.

You can create and enable up to 20 event forwarders to send events to specific recipients.

To forward email to a web-based email service (such as Gmail, Hotmail, or Yahoo), your SMTP server must support forwarding web mail.

Before setting up an event forwarder to a Gmail web service, review information in Setting up event forwarding to syslog, remote SNMP manager, or email in the Lenovo XClarity Administrator online documentation.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/events/monitors`

Query parameters

None

Request body

The attributes vary depending on the type of recipient.

- Table 84 “Azure Log Analytics recipients” on page 987
- Table 85 “Email recipients” on page 991
- Table 86 “FPT recipients” on page 996
- Table 87 “REST recipients” on page 1000
- Table 88 “SNMPv1 and SNMPv3 recipients” on page 1005
- Table 89 “Syslog recipients” on page 1009

Table 84. Azure Log Analytics

Attributes	Required / Optional	Type	Description
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.

Table 84. Azure Log Analytics (continued)

		eventID	Optional	String	List of event IDs, separated by a comma, to be included
		eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
		excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
		negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
		resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
		sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
		typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
			severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
			type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden				Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.

Table 84. Azure Log Analytics (continued)

ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	Optional	String	TCP/UDP port used for the connection. For Azure Log Analytics, this value is always **443**.
primaryKey	Required	String	Primary key of the log-analytics device that is obtained from the Azure portal.
protocol	Required	String	Type of event forwarder. For Azure Log Analytics, this value is always **oms_log_analytics**.
requestTimeout	Optional	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler	Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Required	Array of objects	List of event-forwarding schedules
calendar	Optional	String	Schedule name
daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday

Table 84. Azure Log Analytics (continued)

			endingDate	Optional	String	Date when the schedule ends
			endTime	Optional	String	Time when the schedule ends
			id	Optional	Integer	Schedule ID
			initialEndTime	Optional	String	
			initialStartTime	Optional	String	
			repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
			seriesId	Optional	Integer	Schedule index
			startingDate	Optional	String	Date when the schedule starts
			startTime	Optional	String	Time when the schedule starts
			summary	Optional	Boolean	
		showSummary		Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.
workspaceID				Required	String	Workspace ID of the log-analytics device that is obtained from the Azure portal.

The following example creates an event forwarder for Azure Log Analytics.

```
{
    "description": null,
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF", "3B3C5CBDBE81446D9F27035A28E75745"],
            "sourceIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF", "3B3C5CBDBE81446D9F27035A28E75745"],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "UNKNOWN"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "SWITCH"
            }]
        }
    },
    "forwardHidden": false,
    "ignoreExcluded": false,
    "ipAddress": "3268497b-7842-4a00-a9b8-8128e125e916.ods.opinsights.azure.com",
    "name": "Azure Log Analytics Forwarder",
    "outputFormat": "{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",
                     \"SerialNum\":\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",
                     \"Flags\":\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",
                     \"LocalLogID\":\"[[EventLocalLogID]]\",\"SystemName\":\"[[DeviceFullPathName]]\",
                     \"Action\":\"[[EventAction]]\",\"FailFRUs\":\"[[EventFailFRUs]]\",
```

```
                        \"Severity\":\"[[EventSeverity]]\",\"SourceID\":\"[[EventSourceUUID]]\",
                        \"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
                        \"FailSNs\":\"[[EventFailSerialNumbers]]\", \"FailFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
                        \"EventClass\":\"[[EventClass]]\",\"ComponentID\":\"[[EventComponentUUID]]\",
                        \"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":\"[[EventMessageID]]\",
                        \"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":\"[[EventTimeStamp]]\",
                        \"Args\":[[EventMessageArguments]],\"Service\":\"[[EventService]]\",
                        \"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":\"[[EventDate]]\",
                        \"LXCA\":\"[[LXCA_IP]]\"}",
    "port": "443",
    "primaryKey": "BA7qbCEy7tsTVJ0S3LMATXKXeoHrdPvOx4CfzcnsgM3qKYjZgph64oIKWH9FuSO1xakjmasW0VGeNAUiGSomuQ=
    "protocol": "Azure Log Analytics_log_analytics",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    },
    "workspaceID": "3268497b-7842-4a00-a9b8-8128e125e916"
}
```


Table 85. Email service using SMTP

Attributes	Required / Optional	Type	Description
authenticationEmail	Optional	String	Authentication type. This can be one of the following values. • **Regular**. Authenticates to the specified SMTP server using the specified user ID and password. • **NTLM**. Uses the NT LAN Manager (NTLM) protocol to authentication to the specified SMTP server using the specified user ID, password, and domain name. • **OAUTH2**. Uses the Simple Authentication and Security Layer (SASL) protocol to authenticate to the specified SMTP server using the specified user name and security token. Typically, the user name is your email address. **Attention:** The security token expires after a short time. It is your responsibility to refresh the security token. • **None**. No authentication is used.
connectionEmail	Optional	Array of strings	Connection type to secure connection to the SMTP server. This can be one of the following values. • **SSL**. Use the SSL protocol while communicating. • **TLS**. (default) Uses TLS to form a secure communication over an unsecure channel.
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values: • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter

Table 85. Email service using SMTP (continued)

Attributes	Required / Optional	Type	Description
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
eventID	Optional	String	List of event IDs, separated by a comma, to be included
eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.

Table 85. Email service using SMTP (continued)

Attributes	Re-quired / Optional	Type	Description
severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.

Table 85. Email service using SMTP (continued)

port		Optional	String	TCP/UDP port used for the connection. For email, this value is always **25**.
protocol		Required	String	Type of event forwarder. For email, this value is always **email_alert**.
recipients		Required	Array of strings	List of email addresses for the event forwarder, in the format *userid@domain* (for example, `XClarity1@company.com`)
requestTimeout		Optional	Integer	Amount of time, in seconds, that a event forwarderhas to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler		Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled	Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events	Required	Array of objects	List of event-fowarding schedules
		calendar	Optional	String	Schedule name
		daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	Optional	String	Date when the schedule ends
		endTime	Optional	String	Time when the schedule ends
		id	Optional	Integer	Schedule ID
		initialEndTime	Optional	String	
		initialStartTime	Optional	String	
		repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Optional	Integer	Schedule index
		startingDate	Optional	String	Date when the schedule starts
		startTime	Optional	String	Time when the schedule starts

Table 85. Email service using SMTP (continued)

summary	Optional	Boolean	
showSummary	Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.
senderDomain	Optional	String	Sender domain (for example, company.com). If you do not specify the **senderDomain** or **senderUserName**, this is `LXCA.`*{source_identifier}*`@`*{smtp_host}* by default. If you specify the **senderDomain** but not **senderUserName**, the format of the sender address is *{LXCA_host_name}@{sender_domain}* (for example, `XClarity1@company.com`).
senderUserName	Optional	String	Sender name
subjectFormat	Optional	String	Email subject For a description of fields that can be specified in the subject format, use GET /events/monitors?format=defaultFormat.
useSupportContact	Optional	Boolean	Indicates to use the email address that is defined for the support contact that is assigned to the device. This can be one of the following values. • **true**. Email forwarder uses the email address for the support contact. • **false**. (default) Email forwarder uses the email addresses that are specified in the **recipients** attribute.

The following example creates an event forwarder for email services.

```
{
    "authenticationEmail": "none",
    "connectionEmail": ["SSL"],
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY","STATUS_CHANGE","STATUS_UPDATE","GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": ["none","support","user"],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "resourceGroupsUUIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "UNKNOWN"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
```

```
    },
    "forwardHidden": false,
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.20",
    "matchEverything": true,
    "name": "Email Forwarder",
    "port": "25",
    "protocol": "email_alert",
    "recipients": "user1@company.com",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    },
    "senderDomain": "company.com",
    "senderUserName": "LXCA1",
    "subjectFormat": "[[DeviceIPAddress]]-[[EventSeverity]]-[[EventMessage]]",
    "useSupportContact": false
}
```


Table 86. FTP server

Attributes	Required / Optional	Type	Description
authPasswordChanged	Optional	Boolean	Indicates a request to change the password. This can be one of the following values. • **true**. Change the password • **false**. Do not change the password
authUser	Required if **ftpAuthentication** is set to "Regular"	String	Authentication user ID if authentication is used
authPassword	Required if **ftpAuthentication** is set to "Regular"	String	Authentication password if authentication is used
characterEncoding	Optional	String	Character set. This can be one of the following values. • **UTF-8**. (default) • **Big5**
charactersToRemove	Optional	String	Sequence of characters to be removed from the file content
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.

Table 86. FTP server (continued)

eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
eventID	Optional	String	List of event IDs, separated by a comma, to be included
eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.

Table 86. FTP server (continued)

type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ftpAuthentication	Optional	String	Authentication type. This can be one of the following values. • **Regular**. Authenticates to the specified SMTP server using the specified user ID and password. This is the same as basic authentication. • **None**. (default) No authentication is used. This is the same as anonymous authentication.
ftpFileName	Optional	String	File-name format to use for the file that contains the forwarded event. The default format is `event_[[EventSequenceID]].txt`. **Note:** Each file contains information for a single event.
ftpPath	Required	String	Path on the remote FTP server where the file is to be uploaded
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.

Table 86. FTP server (continued)

port	Optional	String	TCP/UDP port used for the connection. For FTP, this value is always **21**.
protocol	Required	String	Type of event forwarder. For FTP, this value is always **ftp**.
requestTimeout	Optional	Integer	Amount of time, in seconds, that an event forwarderhas to forward events before the request times out. By default, the time-out value is 30 seconds.
scheduler	Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Required	Array of objects	List of event-fowarding schedules
calendar	Optional	String	Schedule name
daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
endingDate	Optional	String	Date when the schedule ends
endTime	Optional	String	Time when the schedule ends
id	Optional	Integer	Schedule ID
initialEndTime	Optional	String	
initialStartTime	Optional	String	
repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
seriesId	Optional	Integer	Schedule index
startingDate	Optional	String	Date when the schedule starts
startTime	Optional	String	Time when the schedule starts
summary	Optional	Boolean	
showSummary	Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example creates an event forwarder for FTP servers.

```
{
    "charactersToRemove": null,
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }],
        }
    },
    "forwardHidden": false,
    "ftpAuthentication": "None",
    "ftpFileName": "event_[[EventSequenceID]].txt",
    "ftpPath": "lxca_events",
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.30",
    "matchEverything": true,
    "name": "FTP Forwarder",
    "port": "21",
    "protocol": "ftp",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    }
}
```

Table 87. REST Web Services

Attributes	**Required / Optional**	**Type**	**Description**
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter

Table 87. REST Web Services (continued)

		categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
		componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
		eventID	Optional	String	List of event IDs, separated by a comma, to be included
		eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
		excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
		negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
		resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
		sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
		typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
			severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.

Table 87. REST Web Services (continued)

type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	Optional	String	TCP/UDP port used for the connection. For REST Web Services, this value is always **80**.
protocol	Required	String	Type of event forwarder. For REST Web Services, this value is always **rest**.
requestTimeout	Optional	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
restAuthentication	Optional	String	Authentication type. This can be one of the following values. • **basic**. Authenticates to the specified server using the specified user ID and password. • **none**. (default) No authentication is used.

Table 87. REST Web Services (continued)

restMethod		Optional	String	REST method. This can be one of the following values. • **POST**. (default) • **PUT**
restPath		Optional	String	Resource path on which the forwarder is to post the events (for example, /rest/test).
restProtocol		Optional	String	Protocol to use for forwarding events. This can be one of the following values. • **HTTP** • **HTTPS**. (default)
restRequestHeaders		Optional	Array of strings	REST header to use for forwarding events
scheduler		Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled	Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events	Required	Array of objects	List of event-fowarding schedules
		calendar	Optional	String	Schedule name
		daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	Optional	String	Date when the schedule ends
		endTime	Optional	String	Time when the schedule ends
		id	Optional	Integer	Schedule ID
		initialEndTime	Optional	String	
		initialStartTime	Optional	String	
		repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Optional	Integer	Schedule index
		startingDate	Optional	String	Date when the schedule starts
		startTime	Optional	String	Time when the schedule starts

Table 87. REST Web Services (continued)

	summary	Optional	Boolean	
showSummary		Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example creates an event forwarder for REST Web Services.

```
{
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "excludedEventIDs": "",
            "eventServices": [],
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.40",
    "matchEverything": true,
    "name": "REST Forwarder",
    "port": "80",
    "protocol": "rest",
    "requestTimeout": 30,
    "restAuthentication": "NONE",
    "restMethod": "POST",
    "restPath": "lxca_events",
    "restProtocol": "HTTP",
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    }
}
```

Table 88. Remote SNMPv1 or SNMPv3 manager

Attributes	Re-quired / Optional	Type	Description
authPasswordSet	Optional	String	Password string. This attribute is required if you specify **authUser**.
authProtocol		String	Authentication protocol. This can be one of the following value. • **MD5** • **SHA** This attribute is required if you specify **authUser**.
authUser	Optional	String	Authentication user ID if authentication is used
community	Optional	String	(SNMPv1 only) The community password that is sent with every SNMP request to the device.
contactName	Optional	String	User-defined contact name for XClarity Administrator traps
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
eventID	Optional	String	List of event IDs, separated by a comma, to be included
eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on

Table 88. Remote SNMPv1 or SNMPv3 manager (continued)

sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
location	Optional	String	Location information, such as site, address, and geography
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder . This name must be unique for all event forwarders.

Table 88. Remote SNMPv1 or SNMPv3 manager (continued)

outputFormat	Optional	String	Output format for the forwarded event
port	Optional	String	TCP/UDP port used for the connection. For SNMP, this value is always **162**.
privacyPasswordSet	Optional	String	Privacy password. This attribute is required if encryption is used.
privacyProtocol	Optional	String	Privacy protocol. This can be one of the following value. • **AES** • **DES** This attribute is required if you specify **privacyPassword**.
protocol	Required	String	Type of event forwarder . For SNMP, this can be one of the following values. • **snmpv1**. Events are forwarded to a remote SNMP manager using SNMPv1. • **snmpv3**. Events are forwarded to a remote SNMP manager using SNMPv3. The trap formats for each event are defined in the lenovoMgrAlert.mib file in the Lenovo XClarity Administrator online documentation.
requestTimeout	Optional	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler	Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Required	Array of objects	List of event-fowarding schedules
calendar	Optional	String	Schedule name
daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
endingDate	Optional	String	Date when the schedule ends
endTime	Optional	String	Time when the schedule ends
id	Optional	Integer	Schedule ID
initialEndTime	Optional	String	
initialStartTime	Optional	String	

Table 88. Remote SNMPv1 or SNMPv3 manager (continued)

repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
seriesId	Optional	Integer	Schedule index
startingDate	Optional	String	Date when the schedule starts
startTime	Optional	String	Time when the schedule starts
summary	Optional	Boolean	
showSummary	Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.
version	Optional	String	Version of SNMP. This can be one of the following values. • **V1** • **V3**

The following example creates an event forwarder for remote SNMP managers.

```
{
    "authPasswordSet": "false",
    "authProtocol": "NONE",
    "authUser": "",
    "community": "public",
    "contactName": "",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"],
            "sourceIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "UNKNOWN"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "SWITCH"
            }]
        }
    },
    "forwardHidden": false,
    "id": "SNMPv1:0",
    "ipAddress": "10.241.53.4",
    "location": "",
    "matchEverything": false,
    "name": "SNMP Forwarder",
    "port": "162",
    "privacyPasswordSet": "false",
    "privacyProtocol": "NONE",
    "protocol": "snmpv1",
    "requestTimeout": "500"
```

```
    "scheduler": {
        "enabled": false,
        "events": []
    },
    "version": "v1"
}
```

Table 89. Syslog

Attributes	Required / Optional	Type	Description
communicationProtocol	Optional	String	Identifies the type of protocol that the syslog monitor uses to send messages. This can be one of the following values. • **TCP** • **UDP**. This is the default value.
description	Optional	String	Description for the event forwarder
dateFormat	Optional	String	Format for the timestamp in the syslog. This can be one of the following values. • **Default_Format**. (default) The default format using local time, for example `Fri Mar 31 05:57:18 EDT 2017`. • **GMT**. International standard (ISO8601) for dates and times, for example `2017-03-31T05:58:20-04:00`.
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
eventID	Optional	String	List of event IDs, separated by a comma, to be included
eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.

Table 89. Syslog (continued)

resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.

Table 89. Syslog (continued)

outputFormat			Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port			Optional	String	TCP/UDP port used for the connection. For syslog, this value is always **514**.
protocol			Required	String	Type of event forwarder. For syslog, this value is always **syslog**.
requestTimeout			Optional	Integer	Amount of time, in seconds, that an event forwarderhas to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler			Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled		Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events		Required	Array of objects	List of event-fowarding schedules
		calendar	Optional	String	Schedule name
		daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	Optional	String	Date when the schedule ends
		endTime	Optional	String	Time when the schedule ends
		id	Optional	Integer	Schedule ID
		initialEndTime	Optional	String	
		initialStartTime	Optional	String	
		repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Optional	Integer	Schedule index
		startingDate	Optional	String	Date when the schedule starts
		startTime	Optional	String	Time when the schedule starts

Table 89. Syslog (continued)

	summary	Optional	Boolean	
showSummary		Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example creates an event forwarders for syslogs.

```
{
    "communicationProtocol": "UDP",
    "dateFormat": "Default_Format",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "ignoreExcluded": true,
    "ipAddress": "192.0.2.60",
    "matchEverything": true,
    "name": "syslog_forwarder",
    "port": "514",
    "protocol": "syslog",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	String	Event forwarder ID.

The following example is returned if the request is successful.

```
{
   "id": "AUG:SNMPv3:0"
}
```

/events/monitors?format=currentFormat&id={*monitor_id*}

Use this REST API to retrieve the current format of the output for a specific event forwarder.

HTTP methods

GET

GET /events/monitors?format=currentFormat&id={*monitor_id*}

Use this method to return the current format of the output for a specific event forwarder.

For the format of the email subject for a specific event forwarder for a email service, see GET /events/monitors?format=currentSubjectFormat&id={*monitor_id*}.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/monitors?format=currentFormat&id={monitor_id}`

where *{monitor_id}* is the ID of the event forwarder. To obtain the filter ID, use the GET /events/monitors method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
{monitor_id}	String	List of attributes (format keys) in the output format of the specified event forwarder Text between double square brackets are the attributes that which are replaced with actual values. For a description of each attribute, use GET /events/monitors?format=formatKeys.

The following example is returned if the request is successful for an event forwarder to a email service.

```
{
   "1507301877371": "Alert: [[EventDate]] [[EventMessage]]\n
                     \n
                     Hardware Information:\n
                      Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
                      Device name         : [[DeviceName]]\n
                      Product name        : [[DeviceProductName]]\n
                      Host name           : [[DeviceHostName]]\n
                      Machine Type        : [[DeviceMachineType]]\n
                      Machine Model       : [[DeviceMachineModel]]\n
                      Serial Number       : [[DeviceSerialNumber]]\n
                      DeviceHealthStatus  : [[DeviceHealthStatus]]\n
                      IPv4 addresses      : [[DeviceIPV4Addresses]]\n
                      IPv6 addresses      : [[DeviceIPV6Addresses]]\n
                      Chassis             : [[DeviceChassisName]]\n
                      DeviceBays          : [[DeviceBays]]\n
                     \n
                     LXCA is: [[ManagementServerIP]]\n
                     \n
                     Event Information:\n
                       Event ID        : [[EventID]]\n
                       Common Event ID : [[CommonEventID]]\n
                       EventSeverity   : [[EventSeverity]]\n
                       Event Class     : [[EventClass]]\n
                       Sequence ID     : [[EventSequenceID]]\n
                       Event Source ID : [[EventSourceUUID]]\n
                       Component ID    : [[EventComponentUUID]]\n
                       Serial Num      : [[EventSerialNumber]]\n
                       MTM             : [[EventMachineTypeModel]]\n
                       EventServices   : [[EventServices]]\n
                       Console link    : [[ConsoleLink]]\n
                       iOS link        : [[iOSLink]]\n
                       Android link    : [[AndroidLink]]\n
                       System Name     : [[DeviceFullPathName]]\n"
}
```

/events/monitors?format=currentSubjectFormat&id=*{monitor_id}*

Use this REST API to retrieve the current format of the email subject for a specific event forwarder for an email service.

HTTP methods

GET

GET /events/monitors?format=currentSubjectFormat&id=*{monitor_id}*

Use this mehod to retrieve the current format of the email subject for a specific event forwarder for an email service.

For the output (forwarded event) format for a specific event forwarder, see GET /events/monitors?format=currentFormat&id=*{monitor_id}*.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/monitors?format=currentSubjectFormat&id={monitor_id}
```

where *{monitor_id}* is the ID of the event forwarder. To obtain the filter ID, use the GET /events/monitors method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
{monitor_id}	String	Format of the email subject Text between double square brackets are the attributes that which are replaced with actual values. For a description of each attribute, use GET /events/monitors?format=formatKeys.

The following example is returned if the request is successful.

```
{
   "1507301877371": "[[DeviceName]]-[[EventMessage]]"
}
```

/events/monitors?format=defaultFormat

Use this REST API to retrieve the default output format for each type of event forwarder.

HTTP methods

GET

GET /events/monitors?format=defaultFormat

Use this method to return the default output format for each type of event forwarder.

For the default output (forwarded event) format for email recipients, see GET /events/monitors?format=defaultSubjectFormat.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/monitors?format=defaultFormat
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
defaultFormats	Object	Information about the output format for each type of event forwarder Text between double square brackets are the attributes that which are replaced with actual values. For a description of each attribute, use GET /events/monitors?format=formatKeys.
email_alert	String	Output format for email recipients
ftp	String	Output format for FTP recipients
oms_log_analytics	String	Output format for Azure Log Analytics recipients

Attributes		Type	Description
	rest	String	Output format for REST recipients
	syslog	String	Output format for syslog recipients

The following example is returned if the request is successful.

```
{
   "defaultFormats": {
      "email_alert": "Alert: [[EventDate]] [[EventMessage]]\n
                      \n
                      Hardware Information:\n
                       Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
                       Device name         : [[DeviceName]]\n
                       Product name        : [[DeviceProductName]]\n
                       Host name           : [[DeviceHostName]]\n
                       Machine Type        : [[DeviceMachineType]]\n
                       Machine Model       : [[DeviceMachineModel]]\n
                       Serial Number       : [[DeviceSerialNumber]]\n
                       DeviceHealthStatus  : [[DeviceHealthStatus]]\n
                       IPv4 addresses      : [[DeviceIPV4Addresses]]\n
                       IPv6 addresses      : [[DeviceIPV6Addresses]]\n
                       Chassis             : [[DeviceChassisName]]\n
                       DeviceBays          : [[DeviceBays]]\n
                      \n
                      LXCA is: [[ManagementServerIP]]\n
                      \n
                      Event Information:\n
                        Event ID        : [[EventID]]\n
                        Common Event ID : [[CommonEventID]]\n
                        EventSeverity   : [[EventSeverity]]\n
                        Event Class     : [[EventClass]]\n
                        Sequence ID     : [[EventSequenceID]]\n
                        Event Source ID : [[EventSourceUUID]]\n
                        Component ID    : [[EventComponentUUID]]\n
                        Serial Num      : [[EventSerialNumber]]\n
                        MTM             : [[EventMachineTypeModel]]\n
                        EventService    : [[EventService]]\n
                        Console link    : [[ConsoleLink]]\n
                        iOS link        : [[iOSLink]]\n
                        Android link    : [[AndroidLink]]\n
                        System Name     : [[DeviceFullPathName]]\n",
      "ftp": "Alert: [[EventDate]] [[EventMessage]]\n
              \n
               Hardware Information:\n
               Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
               Device name         : [[DeviceName]]\n
               Product name        : [[DeviceProductName]]\n
               Host name           : [[DeviceHostName]]\n
               Machine Type        : [[DeviceMachineType]]\n
               Machine Model       : [[DeviceMachineModel]]\n
               Serial Number       : [[DeviceSerialNumber]]\n
               DeviceHealthStatus  : [[DeviceHealthStatus]]\n
               IPv4 addresses      : [[DeviceIPV4Addresses]]\n
               IPv6 addresses      : [[DeviceIPV6Addresses]]\n
               Chassis             : [[DeviceChassisName]]\n
               DeviceBays          : [[DeviceBays]]\n
              \n
              LXCA is: [[ManagementServerIP]]\n
              \n
              Event Information:\n
```

```
                Event ID        : [[EventID]]\n
                Common Event ID : [[CommonEventID]]\n
                EventSeverity   : [[EventSeverity]]\n
                Event Class     : [[EventClass]]\n
                Sequence ID     : [[EventSequenceID]]\n
                Event Source ID : [[EventSourceUUID]]\n
                Component ID    : [[EventComponentUUID]]\n
                Serial Num      : [[EventSerialNumber]]\n
                MTM             : [[EventMachineTypeModel]]\n
                EventService    : [[EventService]]\n
                Console link    : [[ConsoleLink]]\n
                iOS link        : [[iOSLink]]\n
                Android link    : [[AndroidLink]]\n
                System Name     : [[DeviceFullPathName]]\n",
      "oms_log_analytics": "{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",
                           \"Serialnum\":\"[[EventSerialNumber]]\",\"SenderUUID\":
                           \"[[EventSenderUUID]]\",\"Flags\":\"[[EventFlags]]\",\"Userid\":
                           \"[[EventUserName]]\",\"LocalLogID\":\"[[EventLocalLogID]]\",
                           \"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
                           \"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
                           \"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",
                           \"SourceID\":\"[[EventSourceUUID]]\",\"SourceLogSequence\":
                           [[EventSourceLogSequenceNumber]],\"FailSNs\":
                           \"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
                           \"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",
                           \"ComponentID\":\"[[EventComponentUUID]]\",\"Mtm\":
                           \"[[EventMachineTypeModel]]\",\"MsgID\":\"[[EventMessageID]]\",
                           \"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
                           \"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],
                           \"Service\":\"[[EventService]]\",\"CommonEventID\":
                           \"[[CommonEventID]]\",\"EventDate\":\"[[EventDate]]\",
                           \"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
                           \"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":
                           \"[[DeviceIPAddress]]\",\"LXCA\":\"[[LXCA_IP]]\"}",
      "rest": "{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
               \"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
               \"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
               \"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
               [[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
               [[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
               \"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
               \"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
               \"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
               \"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
               \"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
               \"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
               \"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}",
      "syslog": "<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]]
                 severity=[[EventSeverity]] class=[[EventClass]] appladdr=[[LXCA_IP]]
                 user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
                 me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]]
                 systemName=[[DeviceFullPathName]] seq=[[EventSequenceID]] EventID=[[EventID]]
                 CommonEventID=[[CommonEventID]] [[EventMessage]]"
   }
}
```

/events/monitors?format=defaultSubjectFormat

Use this REST API to retrieve the default format of the email subject for a specific event forwarder.

HTTP methods

GET

GET /events/monitors?format=defaultSubjectFormat

Use this method to return the default format of the email subject for a specific event forwarder.

For the default output (forwarded event) format for a specific event forwarder, see GET /events/monitors?format=defaultFormat.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/monitors?format=defaultSubjectFormat
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
defaultFormats	Object	Information about the default formats Text between double square brackets are the attributes that which are replaced with actual values. For a description of each attribute, use GET /events/monitors?format=formatKeys.
email_alert	String	Default format of the email subject

The following example is returned if the request is successful.

```
{
   "defaultFormats": {
      "email_alert": "[[DeviceName]]-[[EventMessage]]"
   }
}
```

/events/monitors?format=formatKeys

Use this REST API to retrieve a description of the fields (format keys) in a forwarded event for each type of event forwarder.

HTTP methods

GET

GET /events/monitors?format=formatKeys

Use this method to return format keys for event forward recipients (event monitors).

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/monitors?format=formatKeys
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
formatKeys		Object	Information about the attributes in the output of each type of event forwarder Text between double square brackets are the attributes that which are replaced with actual values. For a description of each attribute, use GET /events/monitors?format=formatKeys.
	email_alert	String	List of attributes for email recipients
	ftp	String	List of attributes for FTP recipients
	oms_log_analytics	String	List of attributes for Azure Log Analytics recipients
	rest	String	List of attributes for REST recipients
	syslog	String	List of attributes for syslog recipients

The following example is returned if the request is successful.


```
{
   "formatKeys": {
      "email_alert": {
         "DeviceFullPathName": "The device full path in the device it is inserted.",
         "EventDate": "Time and date of when the event was created on source system.",
         "DeviceProductName": "The device product name.",
         "ConsoleLink": "Link to the events log page.",
         "DeviceSerialNumber": "The device serial number.",
         "ManagementServerIP": "The appliance ip address.",
         "iOSLink": "iOS link to the events log page.",
         "DeviceHealthStatus": "The device health status.",
         "EventComponentUUID": "The UUID of the component which caused the event.",
         "DeviceIPV4Addresses": "The device IPv4 address.",
         "EventMachineTypeModel": "System machine type and model of the managed system on which
                                   the event occurred.",
         "DeviceChassisName": "The device chassis name. (If the device is part of a chassis).",
         "EventSeverity": "Event severity in text format.",
         "EventSourceUUID": "The UUID of the component which caused the event.",
         "EventService": "Event service in text format.",
         "AndroidLink": "Android link to the events log page.",
         "DeviceIPAddress": "The IP address of the device.",
         "EventClass": "Event class in text format.",
         "EventMessage": "Event message string.",
         "DeviceHardwareType": "The device hardware type.",
         "DeviceIPV6Addresses": "The device IPV6 address.",
         "DeviceBays": "The device bay. (If the device is part of a chassis or enclosure).",
         "DeviceHostName": "The device hostname.",
         "EventID": "Event id is a unique identifier for each event supported by a product.",
         "CommonEventID": "Common event id.",
         "DeviceMachineType": "The device machine type.",
         "EventSerialNumber": "The serial number of system which caused the event.",
         "EventSequenceID": "Event sequence number.",
         "DeviceName": "The device name."
      },
      "ftp": {
         "DeviceFullPathName": "The device full path in the device it is inserted.",
         "EventDate": "Time and date of when the event was created on source system.",
         "DeviceProductName": "The device product name.",
         "ConsoleLink": "Link to the events log page.",
         "DeviceSerialNumber": "The device serial number.",
         "ManagementServerIP": "The appliance ip address.",
         "iOSLink": "iOS link to the events log page.",
         "DeviceHealthStatus": "The device health status.",
         "EventComponentUUID": "The UUID of the component which caused the event.",
         "DeviceIPV4Addresses": "The device IPv4 address.",
         "EventMachineTypeModel": "System machine type and model of the managed system on which
                                   the event occurred.",
         "DeviceChassisName": "The device chassis name. (If the device is part of a chassis).",
         "EventSeverity": "Event severity in text format.",
         "EventSourceUUID": "The UUID of the component which caused the event.",
         "EventService": "Event service in text format.",
         "AndroidLink": "Android link to the events log page.",
         "DeviceIPAddress": "The IP address of the device.",
         "EventClass": "Event class in text format.",
         "EventMessage": "Event message string.",
         "DeviceHardwareType": "The device hardware type.",
         "DeviceIPV6Addresses": "The device IPV6 address.",
         "DeviceBays": "The device bay. (If the device is part of a chassis or enclosure).",
         "DeviceHostName": "The device hostname.",
         "EventID": "Event id is a unique identifier for each event supported by a product.",
```

```
    "CommonEventID": "Common event id.",
    "DeviceMachineType": "The device machine type.",
    "EventSerialNumber": "The serial number of system which caused the event.",
    "EventSequenceID": "Event sequence number.",
    "DeviceName": "The device name."
},
"oms_log_analytics": {
    "DeviceFullPathName": "The device full path in the device it is inserted.",
    "EventDate": "Time and date of when the event was created on source system.",
    "EventSenderUUID": "The event sender universal unique identifier.",
    "EventFailFRUUUIDs": "The list of failing component universal unique identifier.",
    "DeviceSerialNumber": "The device serial number.",
    "EventFailFRUs": "For hardware fault events, includes one or more FRU numbers for FRUs
                      associated to the fault.",
    "LXCA_IP": "The LXCA appliance ip address.",
    "EventClassNumber": "Event class number.",
    "EventComponentUUID": "The UUID of the component which caused the event.",
    "SystemName": "The full path name of the system.",
    "EventMachineTypeModel": "System machine type and model of the managed system on
                              which the event occurred.",
    "EventTimeStamp": "The time and date of when the log entry was created for the
                       Lenovo XClarity Administrator log.",
    "EventSeverity": "Event severity in text format.",
    "EventUserName": "For internal audit events, this is the associated user id.",
    "EventMessageID": "The event message identifier.",
    "EventMessageArguments": "Dynamic arguments used in the event message string.",
    "EventSourceUUID": "The UUID of the component which caused the event.",
    "EventService": "Event service in text format.",
    "EventFailSerialNumbers": "For hardware fault events, includes one or more serial
                               numbers for FRUs associated to the fault.",
    "DeviceIPAddress": "The IP address of the device.",
    "EventLocalLogID": "The management server local log identifier.",
    "EventSourceLogSequenceNumber": "Source log sequence number which uniquely identifies
                                     this event in source Log id.",
    "EventSource": "The event source.",
    "EventMessage": "Event message string.",
    "EventFlags": "Proprietary event flag definitions.",
    "EventAction": "Event Action category name.",
    "EventID": "Event id is a unique identifier for each event supported by a product.",
    "CommonEventID": "Common event id.",
    "EventSerialNumber": "The serial number of system which caused the event.",
    "EventSequenceID": "Event sequence number."
},
"rest": {
    "DeviceFullPathName": "The device full path in the device it is inserted.",
    "EventDate": "Time and date of when the event was created on source system.",
    "EventSenderUUID": "The event sender universal unique identifier.",
    "EventFailFRUUUIDs": "The list of failing component universal unique identifier.",
    "EventActionNumber": "Event action category.",
    "EventFailFRUs": "For hardware fault events, includes one or more FRU numbers for FRUs
                      associated to the fault.",
    "EventClassNumber": "Event class number.",
    "EventComponentUUID": "The UUID of the component which caused the event.",
    "EventMachineTypeModel": "System machine type and model of the managed system on which
                              the event occurred.",
    "EventTimeStamp": "The time and date of when the log entry was created for the
                       Lenovo XClarity Administrator log.",
    "EventSeverityNumber": "The event severity as a number.",
    "EventUserName": "For internal audit events, this is the associated user id.",
    "EventMessageID": "The event message identifier.",
    "EventMessageArguments": "Dynamic arguments used in the event message string.",
```

```
         "EventSourceUUID": "The UUID of the component which caused the event.",
         "EventServiceNumber": "The event service flag as a number.",
         "EventFailSerialNumbers": "For hardware fault events, includes one or more serial
                                    numbers for FRUs associated to the fault.",
         "EventLocalLogID": "The management server local log identifier.",
         "EventSourceLogSequenceNumber": "Source log sequence number which uniquely identifies
                                          this event in source Log id.",
         "EventMessage": "Event message string.",
         "EventFlags": "Proprietary event flag definitions.",
         "EventID": "Event id is a unique identifier for each event supported by a product.",
         "CommonEventID": "Common event id.",
         "EventSerialNumber": "The serial number of system which caused the event.",
         "EventSequenceID": "Event sequence number."
      },
      "syslog": {
         "DeviceNameIdentifier": "The device name identifier.",
         "DeviceFullPathName": "The device full path in the device it is inserted.",
         "EventDate": "Time and date of when the event was created on source system.",
         "EventSeverity": "Event severity in text format.",
         "EventUserName": "For internal audit events, this is the associated user id.",
         "EventService": "Event service in text format.",
         "SysLogSource": "The syslog source.",
         "DeviceSerialNumber": "The device serial number.",
         "LXCA_IP": "The LXCA appliance ip address.",
         "DeviceIPAddress": "The IP address of the device.",
         "SysLogSeverity": "The syslog numeric severity.",
         "EventMessage": "Event message string.",
         "EventID": "Event id is a unique identifier for each event supported by a product.",
         "CommonEventID": "Common event id.",
         "EventTimeStamp": "The time and date of when the log entry was created for the
                            Lenovo XClarity Administrator log.",
         "UUID": "The universal unique identifier.",
         "EventSequenceID": "Event sequence number."
      },
   }
}
```

/events/monitors/*{monitor_id}*

Use this REST API to modify or delete a specific event forwarder.

Event forwarders define the remote location and protocol to which events are forwarded. Every generated event is monitored to see if it matches the configured filter criteria. If it matches, the event is forwarded to the specified location using the indicated protocol.

HTTP methods

DELETE

GET /events/monitors/*{monitor_id}*

Use this method to return information about a specific for event forwarder, sample content of a forwarded event for a specific event forwarder, or a description of each field in a specific forwarded event.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/monitors/{monitor_id}`

where *{monitor_id}* is the ID of the for event forwarder. To obtain the filter ID, use the GET /events/monitors method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Table 90. Azure Log Analytics

Attributes	Type	Description
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded

Table 90. Azure Log Analytics (continued)

Attributes	Type	Description
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder

Table 90. Azure Log Analytics (continued)

matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarder.
outputFormat	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	String	TCP/UDP port used for the connection. For Azure Log Analytics, this value is always **443**.
primaryKey	String	Primary key of the log-analytics device that is obtained from the Azure portal.
protocol	String	Type of event forwarder. For Azure Log Analytics, this value is always **oms_log_analytics**.
requestTimeout	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out. By default, the time-out value is 30 seconds.
scheduler	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Array of objects	List of event-fowarding schedules
calendar	String	Schedule name
daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
endingDate	String	Date when the schedule ends
endTime	String	Time when the schedule ends
id	Integer	Schedule ID
initialEndTime	String	
initialStartTime	String	
repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.

Table 90. Azure Log Analytics (continued)

			seriesId	Integer	Schedule index
			startingDate	String	Date when the schedule starts
			startTime	String	Time when the schedule starts
			summary	Boolean	
	showSummary			String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.
workspaceID				String	Workspace ID of the log-analytics device that is obtained from the Azure portal.

The following example is returned if the request is successful for event forwarders to Azure Log Analytics recipients.


```
{
    "createdBy": "ADMIN",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "resourceGroupsUUIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "id": "1520009819404",
    "ignoreExcluded": false,
    "ipAddress": "3268497b-7842-4a00-a9b8-8128e125e916.ods.opinsights.azure.com",
    "lastEditBy": "ADMIN",
    "matchEverything": true,
    "name": "ALA_forwarder",
    "outputFormat": "{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",
                        \"Serialnum\":\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",
                        \"Flags\":\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",
                \"LocalLogID\":\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",
                \"SystemName\":\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",
                \"FailFRUs\":\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",
                \"SourceID\":\"[[EventSourceUUID]]\",
                \"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
```

```
                    \"FailSNs\":\"[[EventFailSerialNumbers]]\",
                    \"FailFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",
                    \"ComponentID\":\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",
                    \"MsgID\":\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",
                    \"TimeStamp\":\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],
                    \"Service\":\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",
                    \"EventDate\":\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",
                    \"DeviceSerialNumber\":\"[[DeviceSerialNumber]]\",
                    \"DeviceIPAddress\":\"[[DeviceIPAddress]]\",\"LXCA\":\"[[LXCA_IP]]\"}",
    "port": "58443",
    "primaryKey": "BA7qbCEy7tsTVJ0S3LMATXKXeoHrdPvOx4CfzcnsgM3qKYjZgph64oIKWH9FuSO1xakjmasW0VGeNAUiGSomuQ==",
    "protocol": "oms_log_analytics",
    "requestTimeout": 30,
    "scheduler": {
        "showSummary": false,
        "enabled": false,
        "events": []
    },
    "workspaceID": "3268497b-7842-4a00-a9b8-8128e125e916"
}
```


Table 91. Email service using SMTP

Attributes	Type	Description
authenticationEmail	String	Authentication type. This can be one of the following values. • **Regular**. Authenticates to the specified SMTP server using the specified user ID and password. • **NTLM**. Uses the NT LAN Manager (NTLM) protocol to authentication to the specified SMTP server using the specified user ID, password, and domain name. • **OAUTH2**. Uses the Simple Authentication and Security Layer (SASL) protocol to authenticate to the specified SMTP server using the specified user name and security token. Typically, the user name is your email address. **Attention:** The security token expires after a short time. It is your responsibility to refresh the security token. • **None**. No authentication is used.
connectionEmail	Array of strings	Connection type to secure connection to the SMTP server. This can be one of the following values. • **SSL**. Use the SSL protocol while communicating. • **TLS**. Uses TLS to form a secure communication over an unsecure channel.
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder.
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter

Table 91. Email service using SMTP (continued)

Attributes			Type	Description
		categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
		componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
		eventID	String	List of event IDs, separated by a comma, to be included
		eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
		excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded
		negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
		resourceGroupsUUIDs	Array of strings	List of resource
		sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
		typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.

Table 91. Email service using SMTP (continued)

Attributes	Type	Description
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder
matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarder.
outputFormat	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	String	TCP/UDP port used for the connection. For email, this value is always **25**.

Table 91. Email service using SMTP (continued)

protocol	String	Type of event forwarder. For email, this value is always **email_alert**.
recipients	Array of strings	List of email addresses for the event forwarder, in the format *userid@domain* (for example, `XClarity1@company.com`)
requestTimeout	Integer	The amount of time, in seconds, that an event forwarder has to forward events before the request times out. By default, the time-out value is 30 seconds.
scheduler	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder recipient
enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Array of objects	List of event-fowarding schedules
calendar	String	Schedule name
daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
endingDate	String	Date when the schedule ends
endTime	String	Time when the schedule ends
id	Integer	Schedule ID
initialEndTime	String	
initialStartTime	String	
repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
seriesId	Integer	Schedule index
startingDate	String	Date when the schedule starts
startTime	String	Time when the schedule starts
summary	Boolean	
showSummary	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

Table 91. Email service using SMTP (continued)

senderDomain	String	Sender domain (for example, company.com) If you do not specify the **senderDomain** or **senderUserName**, this is `LXCA.`*{source_identifier}*`@`*{smtp_host}* by default. If you specify the **senderDomain** but not **senderUserName**, the format of the sender address is *{LXCA_host_name}@{sender_domain}* (for example, XClarity1@company.com).
senderUserName	String	Sender name
subjectFormat	String	Email subject For a description of fields that can be specified in the subject format, use GET /events/monitors?format=defaultFormat.
useSupportContact	Boolean	Indicates to use the email address that is defined for the support contact that is assigned to the device. This can be one of the following values. • **true**. Email forwarder uses the email address for the support contact. • **false**. (default) Email forwarder uses the email addresses that are specified in the **recipients** attribute.

The following example is returned if the request is successful for event forwarders to email recipients.


```
{
    "authenticationEmail": "none",
    "connectionEmail": ["SSL"],
    "createdBy": "ADMIN",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY","STATUS_CHANGE","STATUS_UPDATE","GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": ["none","support","user"],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "resourceGroupsUUIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "UNKNOWN"
            },
            {
                "severity": "WARNING",
                "type": "UNKNOWN"
            },
            {
                "severity": "MINOR",
                "type": "UNKNOWN"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
```

```
    "forwardHidden": false,
    "id": "1520009765759",
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.20",
    "lastEditBy": "ADMIN",
    "matchEverything": true,
    "name": "email forwarder",
    "outputFormat": "Alert: [[EventDate]] [[EventMessage]]\n
                    \n
                    Hardware Information:\n
                    Managed Endpoint      : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
                    Device name           : [[DeviceName]]\n
                    Product name          : [[DeviceProductName]]\n
                    Host name             : [[DeviceHostName]]\n
                    Machine Type          : [[DeviceMachineType]]\n
                    Machine Model         : [[DeviceMachineModel]]\n
                    Serial Number         : [[DeviceSerialNumber]]\n
                    DeviceHealthStatus    : [[DeviceHealthStatus]]\n
                    IPv4 addresses        : [[DeviceIPV4Addresses]]\n
                    IPv6 addresses        : [[DeviceIPV6Addresses]]\n
                    Chassis               : [[DeviceChassisName]]\n
                    DeviceBays            : [[DeviceBays]]\n
                    \n
                    LXCA is: [[ManagementServerIP]]\n
                    \n
                    Event Information:\n
                    Event ID          : [[EventID]]\n
                    Common Event ID : [[CommonEventID]]\n
                    EventSeverity     : [[EventSeverity]]\n
                    Event Class       : [[EventClass]]\n
                    Sequence ID       : [[EventSequenceID]]\n
                    Event Source ID : [[EventSourceUUID]]\n
                    Component ID      : [[EventComponentUUID]]\n
                    Serial Num        : [[EventSerialNumber]]\n
                    MTM               : [[EventMachineTypeModel]]\n
                    EventService      : [[EventService]]\n
                    Console link      : [[ConsoleLink]]\n
                    iOS link          : [[iOSLink]]\n
                    Android link      : [[AndroidLink]]\n
                    System Name       : [[DeviceFullPathName]]
                    \n",
    "port": "25",
    "protocol": "email_alert",
    "recipients": "user1@company.com",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    },
    "senderDomain": "company.com",
    "senderUserName": "LXCA1",
    "subjectFormat": "[[DeviceName]]-[[EventMessage]]",
    "useSupportContact": false
}
```

Table 92. FTP servers

Attributes	Type	Description
authUser	Boolean	Authentication user ID if authentication is used
characterEncoding	String	Character set. This can be one of the following values. • **UTF-8**. (default) • **Big5**
charactersToRemove	String	Sequence of characters to be removed from the file content
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.

Table 92. FTP servers (continued)

Attributes	Type	Description
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ftpAuthentication	String	Authentication type. This can be one of the following values. • **Regular**. Authenticates to the specified SMTP server using the specified user ID and password. This is the same as basic authentication. • **None**. (default) No authentication is used. This is the same as anonymous authentication.
ftpFileName	String	File-name format to use for the file that contains the forwarded event. The default format is `event_[[EventSequenceID]].txt`. **Note:** Each file contains information for a single event.
ftpPath	String	Path on the remote FTP server where the file is to be uploaded
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder

Table 92. FTP servers (continued)

matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	String	TCP/UDP port used for the connection. For FTP, this value is always **21**.
protocol	String	Type of event forwarder. For FTP, this value is always **ftp**.
requestTimeout	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Array of objects	List of event-forwarding schedules
calendar	String	Schedule name
daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
endingDate	String	Date when the schedule ends
endTime	String	Time when the schedule ends
id	Integer	Schedule ID
initialEndTime	String	
initialStartTime	String	
repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
seriesId	Integer	Schedule index
startingDate	String	Date when the schedule starts

Table 92. FTP servers (continued)

			startTime	String	Time when the schedule starts
			summary	Boolean	
	showSummary			String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example is returned if the request is successful for event forwarders to FTP recipients.


```
{
    "authUser": "admin",
    "characterEncoding": "UTF-8",
    "charactersToRemove": null,
    "createdBy": "ADMIN",
    "description": "",
    "enable": "false",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }],
        }
    },
    "forwardHidden": false,
    "ftpAuthentication": "REGULAR",
    "ftpFileName": "event_[[EventSequenceID]].txt",
    "ftpPath": "lxca_events",
    "id": "1534862502642",
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.30",
    "lastEditBy": "ADMIN",
    "matchEverything": true,
    "name": "FTP_forwarder",
    "outputFormat": "Alert: [[EventDate]] [[EventMessage]]\n\nHardware Information:\n
                        Managed Endpoint      : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
                          Device name           : [[DeviceName]]\n
                          Product name          : [[DeviceProductName]]\n
                          Host name             : [[DeviceHostName]]\n
                          Machine Type          : [[DeviceMachineType]]\n
                          Machine Model         : [[DeviceMachineModel]]\n
                          Serial Number         : [[DeviceSerialNumber]]\n
                          DeviceHealthStatus    : [[DeviceHealthStatus]]\n
                          IPv4 addresses        : [[DeviceIPV4Addresses]]\n
```

```
                        IPv6 addresses          : [[DeviceIPV6Addresses]]\n
                        Chassis                 : [[DeviceChassisName]]\n
                        DeviceBays              : [[DeviceBays]]\n
                       \n
                       LXCA is: [[ManagementServerIP]]\n
                       \n
                         Event Information:\n
                          Event ID            : [[EventID]]\n
                          Common Event ID : [[CommonEventID]]\n
                          EventSeverity     : [[EventSeverity]]\n
                          Event Class       : [[EventClass]]\n
                          Sequence ID       : [[EventSequenceID]]\n
                          Event Source ID : [[EventSourceUUID]]\n
                          Component ID      : [[EventComponentUUID]]\n
                          Serial Num        : [[EventSerialNumber]]\n
                          MTM               : [[EventMachineTypeModel]]\n
                          EventService      : [[EventService]]\n
                          Console link      : [[ConsoleLink]]\n
                          iOS link          : [[iOSLink]]\n
                          Android link      : [[AndroidLink]]\n
                          System Name       : [[DeviceFullPathName]]\n",
    "port": "21",
    "protocol": "ftp",
    "requestTimeout": 30,
    "scheduler": {
        "showSummary": false,
        "enabled": false,
        "events": []
    }
}
```

Table 93. REST Web Services

Attributes	Type	Description
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included

Table 93. REST Web Services (continued)

Attributes	Type	Description
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarderID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.

Table 93. REST Web Services (continued)

ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder
matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	String	TCP/UDP port used for the connection. For REST Web Services, this value is always **80**.
protocol	String	Type of event forwarder. For REST Web Services, this value is always **rest**.
requestTimeout	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
restAuthentication	String	Authentication type. This can be one of the following values. • **basic**. Authenticates to the specified server using the specified user ID and password. • **none**. No authentication is used.
restMethod	String	REST method to use for forwarding events. This can be one of the following values. • **POST** • **PUT**
restPath	String	Resource path on which the forwarder is to post the events (for example, /rest/test)
restProtocol	String	Protocol to use for forwarding events. This can be one of the following values. • **HTTP** • **HTTPS**
restRequestHeaders	Array of strings	REST header to use for forwarding events
scheduler	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Array of objects	List of event-forwarding schedules
calendar	String	Schedule name

Table 93. REST Web Services (continued)

			daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
			endingDate	String	Date when the schedule ends
			endTime	String	Time when the schedule ends
			id	Integer	Schedule ID
			initialEndTime	String	
			initialStartTime	String	
			repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
			seriesId	Integer	Schedule index
			startingDate	String	Date when the schedule starts
			startTime	String	Time when the schedule starts
			summary	Boolean	
	showSummary			String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example is returned if the request is successful for event forwarders to REST recipients.

```
{
    "createdBy": "ADMIN",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "excludedEventIDs": "",
            "eventServices": [],
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
```

```
        }
    },
    "forwardHidden": false,
    "id": "1520009679583",
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.40",
    "lastEditBy": "ADMIN",
    "matchEverything": true,
    "name": "REST_forwarder",
    "outputFormat": "{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",
                        \"serialnum\":\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",
                    \"flags\":\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",
                    \"localLogID\":\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",
                    \"action\":[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",
                    \"severity\":[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
                    \"sourceLogSequence\":[[EventSourceLogSequenceNumber]],
                    \"failFRUSNs\":\"[[EventFailSerialNumbers]]\",
                    \"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",\"eventClass\":[[EventClassNumber]],
                    \"componentID\":\"[[EventComponentUUID]]\",\"mtm\":\"[[EventMachineTypeModel]]\",
                    \"msgID\":\"[[EventMessageID]]\",\"sequenceNumber\":\"[[EventSequenceID]]\",
                    \"timeStamp\":\"[[EventTimeStamp]]\",\"args\":[[EventMessageArguments]],
                    \"service\":[[EventServiceNumber]],\"commonEventID\":\"[[CommonEventID]]\",
                    \"eventDate\":\"[[EventDate]]\"}",
    "port": "80",
    "protocol": "rest",
    "requestTimeout": 30,
    "restAuthentication": "NONE",
    "restMethod": "POST",
    "restPath": "lxca_events",
    "restProtocol": "HTTP",
    "restRequestHeaders": [],
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    }
}
```

Table 94. Remote SNMPv1 or SNMPv3 manager

Attributes	Type	Description
authPasswordSet	String	Password string. This attribute is required if you specify **authUser**.
authProtocol	String	Authentication protocol. This can be one of the following. • **MD5** • **SHA** This attribute is required if you specify **authUser**.
authUser	String	Authentication user ID if authentication is used
community	String	(SNMPv1 only) The community password that is sent with every SNMP request to the device.
contactName	String	The user-defined contact name for XClarity Administrator traps
createdBy	String	Name of the user that created the event forwarder
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.

Table 94. Remote SNMPv1 or SNMPv3 manager (continued)

Attributes	Type	Description
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.

Table 94. Remote SNMPv1 or SNMPv3 manager (continued)

Attributes	Type	Description
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder
location	String	Location information, such as site, address, and geography
matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices. • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
port	String	TCP/UDP port used for the connection. For SNMP, this value is always **162**.
privacyPasswordSet	String	Privacy password. This attribute is required if encryption is used.

Table 94. Remote SNMPv1 or SNMPv3 manager (continued)

privacyProtocol	String	Privacy protocol. This can be one of the following values. • **AES** • **DES** This attribute is required if you specify **privacyPassword**.
protocol	String	Type of event forwarder. For SNMP, this can be one of the following values. • **snmpv1**. Events are forwarded to a remote SNMP manager using SNMPv1. • **snmpv3**. Events are forwarded to a remote SNMP manager using SNMPv3. The trap formats for each event are defined in the lenovoMgrAlert.mib file in the Lenovo XClarity Administrator online documentation.
requestTimeout	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Array of objects	List of event-fowarding schedules
calendar	String	Schedule name
daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
endingDate	String	Date when the schedule ends
endTime	String	Time when the schedule ends
id	Integer	Schedule ID
initialEndTime	String	
initialStartTime	String	
repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
seriesId	Integer	Schedule index
startingDate	String	Date when the schedule starts
startTime	String	Time when the schedule starts

Table 94. Remote SNMPv1 or SNMPv3 manager (continued)

	summary	Boolean	
showSummary		String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example is returned if the request is successful for event forwarders to SNMPv3 recipients.


```
{
    "authPasswordSet": "false",
    "authProtocol": "NONE",
    "authUser": "",
    "contactName": "",
    "createdBy": "ADMIN",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "id": "1520009466990",
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.50",
    "lastEditBy": "ADMIN",
    "location": "",
    "matchEverything": true,
    "name": "SNMP_forwarder",
    "port": "162",
    "privacyPasswordSet": "false",
    "privacyProtocol": "NONE",
    "protocol": "snmpv3",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": true,
        "events": [{
            "calendar": "Calendar1",
            "daysOfWeek": ["1", "2", "3", "4", "5"],
            "endingDate": "2017-12-31T22:00:00.000Z",
            "endTime": "2017-10-06T21:00:00.000Z",
            "id": 0,
```

```
            "initialEndTime":  "2017-10-06T21:00:00.000Z",
            "initialStartTime":  "2017-10-06T12:00:00.000Z",
            "repeatable":  true,
            "seriesId":  1
            "startingDate":  "2017-10-06T12:00:00.000Z",
            "startTime":  "2017-10-06T12:00:00.000Z",
            "summary":  "Forwarder  (repeatable)",
        }],
        "showSummary":  false
    }
}
```

Table 95. Syslog

Attributes	Type	Description
communicationProtocol	String	Identifies the type of protocol that the syslog monitor uses to send messages. This can be one of the following values. • **TCP** • **UDP**. (default)
createdBy	String	Name of the user that created the event forwarder
dateFormat	String	Format for the timestamp in the syslog. This can be one of the following values. • **Default_Format**. The default format using local time, for example `Fri Mar 31 05:57:18 EDT 2017`. • **GMT**. International standard (ISO8601) for dates and times, for example `2017-03-31T05:58:20-04:00`.
description	String	Description for the event forwarder
enable	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Object	Information about the types of events to forward
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one or more of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
eventID	String	List of event IDs, separated by a comma, to be included
eventServices	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	String	List of event IDs, separated by a comma, to be excluded

Table 95. Syslog (continued)

Attributes	Type	Description
negateFilter	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Array of strings	List of resource
sourceIDs	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
id	String	Event forwarder ID
ignoreExcluded	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
lastEditBy	String	Name of the user that last edited the event forwarder

Table 95. Syslog (continued)

matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	String	TCP/UDP port used for the connection. For syslog, this value is always **514**.
protocol	String	Type of event forwarder. For syslog, this value is always **syslog**.
requestTimeout	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Array of objects	List of event-fowarding schedules
calendar	String	Schedule name
daysOfWeek	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
endingDate	String	Date when the schedule ends
endTime	String	Time when the schedule ends
id	Integer	Schedule ID
initialEndTime	String	
initialStartTime	String	
repeatable	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
seriesId	Integer	Schedule index
startingDate	String	Date when the schedule starts

Table 95. Syslog (continued)

			startTime	String	Time when the schedule starts
			summary	Boolean	
	showSummary			String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example is returned if the request is successful for event forwarders to syslog recipients.


```
{
    "communicationProtocol": "UDP",
    "createdBy": "ADMIN",
    "dateFormat": "Default_Format",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "id": "1520009382682",
    "ignoreExcluded": true,
    "ipAddress": "192.0.2.60",
    "lastEditBy": "ADMIN",
    "matchEverything": true,
    "name": "syslog_forwarder",
    "outputFormat": "<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]]
                        severity=[[EventSeverity]] class=[[EventClass]] appladdr=[[LXCA_IP]]
                    user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
                    me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]]
                    systemName=[[DeviceFullPathName]] seq=[[EventSequenceID]] EventID=[[EventID]]
                    CommonEventID=[[CommonEventID]] [[EventMessage]]",
    "port": "514",
    "protocol": "syslog",
    "requestTimeout": 30,
    "scheduler": {
        "showSummary": false,
        "enabled": false,
        "events": []
    },
```

}

PUT /events/monitors/*{forwarder_id}*

Use this method to modify event forwarders after they are configured without requiring that they be deleted and re-added.

All attributes except the protocol can be modified. For example, an event forwarder can be temporarily disabled using the PUT method, and then re-enabled at a later time.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/events/monitors/{forwarder_id}`

where *{forwarder_id}* is the ID of the event forwarder to be deleted. To obtain the filter ID, use the GET /events/monitors method.

Query parameters

None

Request body

The attributes vary depending on the type of recipient.

- Table 96 “Azure Log Analytics ” on page 1051
- Table 97 “Email service” on page 1055
- Table 98 “FTP server” on page 1060
- Table 99 “REST Web Service” on page 1064
- Table 100 “Remote SNMPv1 or SNMPv3 manager” on page 1069
- Table 101 “Syslog” on page 1073

Table 96. Azure Log Analytics

Attributes	Re-quired / Optional	Type	Description
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.

Table 96. Azure Log Analytics (continued)

		eventID	Optional	String	List of event IDs, separated by a comma, to be included
		eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
		excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
		negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
		resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
		sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
		typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
			severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
			type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden				Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.

Table 96. Azure Log Analytics (continued)

ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	Optional	String	TCP/UDP port used for the connection. For Azure Log Analytics, this value is always **443**.
primaryKey	Required	String	Primary key of the log-analytics device that is obtained from the Azure portal.
protocol	Required	String	Type of event forwarder. For Azure Log Analytics, this value is always **oms_log_analytics**.
requestTimeout	Optional	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler	Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Required	Array of objects	List of event-forwarding schedules
calendar	Optional	String	Schedule name
daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday

Table 96. Azure Log Analytics (continued)

			endingDate	Optional	String	Date when the schedule ends
			endTime	Optional	String	Time when the schedule ends
			id	Optional	Integer	Schedule ID
			initialEndTime	Optional	String	
			initialStartTime	Optional	String	
			repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
			seriesId	Optional	Integer	Schedule index
			startingDate	Optional	String	Date when the schedule starts
			startTime	Optional	String	Time when the schedule starts
			summary	Optional	Boolean	
		showSummary		Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.
workspaceID				Required	String	Workspace ID of the log-analytics device that is obtained from the Azure portal.

The following example modifies an event forwarder for an Azure Log Analytics recipient.

```
{
    "authenticationEmail": "none",
    "connectionEmail": ["SSL"],
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY","STATUS_CHANGE","STATUS_UPDATE","GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": ["none","support","user"],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "resourceGroupsUUIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "UNKNOWN"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
```

```
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.20",
    "matchEverything": true,
    "name": "Email Forwarder",
    "port": "25",
    "protocol": "email_alert",
    "recipients": "user1@company.com",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    },
    "senderDomain": "company.com",
    "senderUserName": "LXCA1",
    "subjectFormat": "[[DeviceIPAddress]]-[[EventSeverity]]-[[EventMessage]]",
    "useSupportContact": false
}
```

Table 97. Email service using SMTP

Attributes	Required / Optional	Type	Description
authenticationEmail	Optional	String	Authentication type. This can be one of the following values. • **Regular**. Authenticates to the specified SMTP server using the specified user ID and password. • **NTLM**. Uses the NT LAN Manager (NTLM) protocol to authentication to the specified SMTP server using the specified user ID, password, and domain name. • **OAUTH2**. Uses the Simple Authentication and Security Layer (SASL) protocol to authenticate to the specified SMTP server using the specified user name and security token. Typically, the user name is your email address. **Attention:** The security token expires after a short time. It is your responsibility to refresh the security token. • **None**. No authentication is used.
connectionEmail	Optional	Array of strings	Connection type to secure connection to the SMTP server. This can be one of the following values. • **SSL**. Use the SSL protocol while communicating. • **TLS**. (default) Uses TLS to form a secure communication over an unsecure channel.
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values: • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter

Table 97. Email service using SMTP (continued)

Attributes	Required / Optional	Type	Description
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
eventID	Optional	String	List of event IDs, separated by a comma, to be included
eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.

Table 97. Email service using SMTP (continued)

Attributes	Re-quired / Optional	Type	Description
severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.

Table 97. Email service using SMTP (continued)

port		Optional	String	TCP/UDP port used for the connection. For email, this value is always **25**.
protocol		Required	String	Type of event forwarder. For email, this value is always **email_alert**.
recipients		Required	Array of strings	List of email addresses for the event forwarder, in the format *userid@domain* (for example, `XClarity1@company.com`)
requestTimeout		Optional	Integer	Amount of time, in seconds, that a event forwarderhas to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler		Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled	Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events	Required	Array of objects	List of event-fowarding schedules
		calendar	Optional	String	Schedule name
		daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	Optional	String	Date when the schedule ends
		endTime	Optional	String	Time when the schedule ends
		id	Optional	Integer	Schedule ID
		initialEndTime	Optional	String	
		initialStartTime	Optional	String	
		repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Optional	Integer	Schedule index
		startingDate	Optional	String	Date when the schedule starts
		startTime	Optional	String	Time when the schedule starts

Table 97. Email service using SMTP (continued)

summary	Optional	Boolean	
showSummary	Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.
senderDomain	Optional	String	Sender domain (for example, company.com). If you do not specify the **senderDomain** or **senderUserName**, this is `LXCA.`*{source_identifier}*`@`*{smtp_host}* by default. If you specify the **senderDomain** but not **senderUserName**, the format of the sender address is *{LXCA_host_name}@{sender_domain}* (for example, `XClarity1@company.com`).
senderUserName	Optional	String	Sender name
subjectFormat	Optional	String	Email subject For a description of fields that can be specified in the subject format, use GET /events/monitors?format=defaultFormat.
useSupportContact	Optional	Boolean	Indicates to use the email address that is defined for the support contact that is assigned to the device. This can be one of the following values. • **true**. Email forwarder uses the email address for the support contact. • **false**. (default) Email forwarder uses the email addresses that are specified in the **recipients** attribute.

The following example modifies an event forwarder for an email recipient.

```
{
    "authenticationEmail": "none",
    "connectionEmail": ["SSL"],
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY","STATUS_CHANGE","STATUS_UPDATE","GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": ["none","support","user"],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "resourceGroupsUUIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "UNKNOWN"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
```

```
    },
    "forwardHidden": false,
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.20",
    "matchEverything": true,
    "name": "Email Forwarder",
    "port": "25",
    "protocol": "email_alert",
    "recipients": "user1@company.com",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    },
    "senderDomain": "company.com",
    "senderUserName": "LXCA1",
    "subjectFormat": "[[DeviceIPAddress]]-[[EventSeverity]]-[[EventMessage]]",
    "useSupportContact": false
}
```

Table 98. FTP server

Attributes	Required / Optional	Type	Description
authPasswordChanged	Optional	Boolean	Indicates a request to change the password. This can be one of the following values. • **true**. Change the password • **false**. Do not change the password
authUser	Required if **ftpAuthentication** is set to "Regular"	String	Authentication user ID if authentication is used
authPassword	Required if **ftpAuthentication** is set to "Regular"	String	Authentication password if authentication is used
characterEncoding	Optional	String	Character set. This can be one of the following values. • **UTF-8**. (default) • **Big5**
charactersToRemove	Optional	String	Sequence of characters to be removed from the file content
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.

Table 98. FTP server (continued)

eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
eventID	Optional	String	List of event IDs, separated by a comma, to be included
eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.

Table 98. FTP server (continued)

type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ftpAuthentication	Optional	String	Authentication type. This can be one of the following values. • **Regular**. Authenticates to the specified SMTP server using the specified user ID and password. This is the same as basic authentication. • **None**. (default) No authentication is used. This is the same as anonymous authentication.
ftpFileName	Optional	String	File-name format to use for the file that contains the forwarded event. The default format is `event_[[EventSequenceID]].txt`. **Note:** Each file contains information for a single event.
ftpPath	Required	String	Path on the remote FTP server where the file is to be uploaded
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.

Table 98. FTP server (continued)

port			Optional	String	TCP/UDP port used for the connection. For FTP, this value is always **21**.
protocol			Required	String	Type of event forwarder. For FTP, this value is always **ftp**.
requestTimeout			Optional	Integer	Amount of time, in seconds, that an event forwarderhas to forward events before the request times out. By default, the time-out value is 30 seconds.
scheduler			Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled		Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events		Required	Array of objects	List of event-fowarding schedules
		calendar	Optional	String	Schedule name
		daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	Optional	String	Date when the schedule ends
		endTime	Optional	String	Time when the schedule ends
		id	Optional	Integer	Schedule ID
		initialEndTime	Optional	String	
		initialStartTime	Optional	String	
		repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Optional	Integer	Schedule index
		startingDate	Optional	String	Date when the schedule starts
		startTime	Optional	String	Time when the schedule starts
		summary	Optional	Boolean	
	showSummary		Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example modifies an event forwarder for an FTP recipient.

```
{
    "charactersToRemove": null,
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }],
        }
    },
    "forwardHidden": false,
    "ftpAuthentication": "None",
    "ftpFileName": "event_[[EventSequenceID]].txt",
    "ftpPath": "lxca_events",
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.30",
    "matchEverything": true,
    "name": "FTP Forwarder",
    "port": "21",
    "protocol": "ftp",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    }
}
```

Table 99. REST Web Services

Attributes	Required / Optional	Type	Description
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter

Table 99. REST Web Services (continued)

		categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
		componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
		eventID	Optional	String	List of event IDs, separated by a comma, to be included
		eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
		excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
		negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
		resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
		sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
		typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
			severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.

Table 99. REST Web Services (continued)

type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
outputFormat	Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port	Optional	String	TCP/UDP port used for the connection. For REST Web Services, this value is always **80**.
protocol	Required	String	Type of event forwarder. For REST Web Services, this value is always **rest**.
requestTimeout	Optional	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
restAuthentication	Optional	String	Authentication type. This can be one of the following values. • **basic**. Authenticates to the specified server using the specified user ID and password. • **none**. (default) No authentication is used.

Table 99. REST Web Services (continued)

restMethod		Optional	String	REST method. This can be one of the following values. • **POST**. (default) • **PUT**
restPath		Optional	String	Resource path on which the forwarder is to post the events (for example, /rest/test).
restProtocol		Optional	String	Protocol to use for forwarding events. This can be one of the following values. • **HTTP** • **HTTPS**. (default)
restRequestHeaders		Optional	Array of strings	REST header to use for forwarding events
scheduler		Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled	Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events	Required	Array of objects	List of event-fowarding schedules
		calendar	Optional	String	Schedule name
		daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	Optional	String	Date when the schedule ends
		endTime	Optional	String	Time when the schedule ends
		id	Optional	Integer	Schedule ID
		initialEndTime	Optional	String	
		initialStartTime	Optional	String	
		repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Optional	Integer	Schedule index
		startingDate	Optional	String	Date when the schedule starts
		startTime	Optional	String	Time when the schedule starts

Table 99. REST Web Services (continued)

	summary	Optional	Boolean	
showSummary		Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example modifies an event forwarder for a REST recipient.

```
{
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "excludedEventIDs": "",
            "eventServices": [],
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "ignoreExcluded": false,
    "ipAddress": "192.0.2.40",
    "matchEverything": true,
    "name": "REST Forwarder",
    "port": "80",
    "protocol": "rest",
    "requestTimeout": 30,
    "restAuthentication": "NONE",
    "restMethod": "POST",
    "restPath": "lxca_events",
    "restProtocol": "HTTP",
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    }
}
```

Table 100. Remote SNMPv1 or SNMPv3 manager

Attributes	Re-quired / Optional	Type	Description
authPasswordSet	Optional	String	Password string. This attribute is required if you specify **authUser**.
authProtocol		String	Authentication protocol. This can be one of the following value. • **MD5** • **SHA** This attribute is required if you specify **authUser**.
authUser	Optional	String	Authentication user ID if authentication is used
community	Optional	String	(SNMPv1 only) The community password that is sent with every SNMP request to the device.
contactName	Optional	String	User-defined contact name for XClarity Administrator traps
description	Optional	String	Description for the event forwarder
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
eventID	Optional	String	List of event IDs, separated by a comma, to be included
eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.
resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on

Table 100. Remote SNMPv1 or SNMPv3 manager (continued)

sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server.
location	Optional	String	Location information, such as site, address, and geography
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	User-defined name for the event forwarder . This name must be unique for all event forwarders.

Table 100. Remote SNMPv1 or SNMPv3 manager (continued)

outputFormat	Optional	String	Output format for the forwarded event
port	Optional	String	TCP/UDP port used for the connection. For SNMP, this value is always **162**.
privacyPasswordSet	Optional	String	Privacy password. This attribute is required if encryption is used.
privacyProtocol	Optional	String	Privacy protocol. This can be one of the following value. • **AES** • **DES** This attribute is required if you specify **privacyPassword**.
protocol	Required	String	Type of event forwarder . For SNMP, this can be one of the following values. • **snmpv1**. Events are forwarded to a remote SNMP manager using SNMPv1. • **snmpv3**. Events are forwarded to a remote SNMP manager using SNMPv3. The trap formats for each event are defined in the lenovoMgrAlert.mib file in the Lenovo XClarity Administrator online documentation.
requestTimeout	Optional	Integer	Amount of time, in seconds, that an event forwarder has to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler	Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
enabled	Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
events	Required	Array of objects	List of event-fowarding schedules
calendar	Optional	String	Schedule name
daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
endingDate	Optional	String	Date when the schedule ends
endTime	Optional	String	Time when the schedule ends
id	Optional	Integer	Schedule ID
initialEndTime	Optional	String	
initialStartTime	Optional	String	

Table 100. Remote SNMPv1 or SNMPv3 manager (continued)

repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
seriesId	Optional	Integer	Schedule index
startingDate	Optional	String	Date when the schedule starts
startTime	Optional	String	Time when the schedule starts
summary	Optional	Boolean	
showSummary	Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.
version	Optional	String	Version of SNMP. This can be one of the following values. • **V1** • **V3**

The following example modifies an event forwarder for a SNMPv1 recipient.

```
{
    "authPasswordSet": "false",
    "authProtocol": "NONE",
    "authUser": "",
    "community": "public",
    "contactName": "",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"],
            "sourceIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "UNKNOWN"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "SWITCH"
            }]
        }
    },
    "forwardHidden": false,
    "id": "SNMPv1:0",
    "ipAddress": "10.241.53.4",
    "location": "",
    "matchEverything": false,
    "name": "SNMP Forwarder",
    "port": "162",
    "privacyPasswordSet": "false",
    "privacyProtocol": "NONE",
    "protocol": "snmpv1",
    "requestTimeout": "500"
```

```
    "scheduler": {
        "enabled": false,
        "events": []
    },
    "version": "v1"
}
```

Table 101. Syslog

Attributes	Required / Optional	Type	Description
communicationProtocol	Optional	String	Identifies the type of protocol that the syslog monitor uses to send messages. This can be one of the following values. • **TCP** • **UDP**. This is the default value.
description	Optional	String	Description for the event forwarder
dateFormat	Optional	String	Format for the timestamp in the syslog. This can be one of the following values. • **Default_Format**. (default) The default format using local time, for example `Fri Mar 31 05:57:18 EDT 2017`. • **GMT**. International standard (ISO8601) for dates and times, for example `2017-03-31T05:58:20-04:00`.
enable	Optional	Boolean	Indicates whether the event forwarder is enabled. This can be one of the following values. • **true**. (default) The event forwarder is enabled. • **false**. The event forwarder is disabled.
eventFilter	Required	Object	Information about the types of events to forward
filter	Required	Object	Information about each event filter
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are monitored.
eventID	Optional	String	List of event IDs, separated by a comma, to be included
eventServices	Optional	Array of strings	Service type. This can be one or both of the following values. • **none** • **support** • **user**
excludedEventIDs	Optional	String	List of event IDs, separated by a comma, to be excluded
negateFilter	Optional	Boolean	Indicates whether to exclude events that match the specified filter. This can be one of the following values. • **true**. Excludes (does not forward) events that match the specified filters. • **false**. Includes (forwards) events that match the specified filters.

Table 101. Syslog (continued)

resourceGroupsUUIDs	Optional	Array of strings	List of resource-group UUIDs to filter on
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are monitored.
typeSeverity	Required	Array of objects	Event severity and type. If both sourceIDs and componentsIDs are empty, all events that match the typeSeverity filter are forwarded.
severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
forwardHidden	Optional	Boolean	Specifies whether to forward hidden events. This can be one of the following values. • **true**. Hidden events are forwarded. • **false**. (default) Hidden events are not forwarded.
ignoreExcluded	Optional	Boolean	Specifies whether to disable the forwarding of excluded events. This can be one of the following values. • **true**. Ignores excluded events. • **false**. (default) Forwards excluded events.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the events. For email, this is the SMTP server
name	Required	String	User-defined name for the event forwarder. This name must be unique for all event forwarders.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.

Table 101. Syslog (continued)

outputFormat			Optional	String	Output format of the forwarded event Text between double square brackets are the fields that which are replaced with actual values. For a description of each field, use GET /events/monitors?format=formatKeys.
port			Optional	String	TCP/UDP port used for the connection. For syslog, this value is always **514**.
protocol			Required	String	Type of event forwarder. For syslog, this value is always **syslog**.
requestTimeout			Optional	Integer	Amount of time, in seconds, that an event forwarderhas to forward events before the request times out By default, the time-out value is 30 seconds.
scheduler			Optional	Object	Information about times and days when you want the specified events to be forwarded to this event forwarder
	enabled		Required	Boolean	Indicates whether the schedule is enabled. This can be one of the following values. • **true**. The schedule is enabled. Only events that occur during the specified time slot are forwarded. • **false**. The schedule is disabled. Events are forwarded 24x7.
	events		Required	Array of objects	List of event-fowarding schedules
		calendar	Optional	String	Schedule name
		daysOfWeek	Optional	Array of strings	Days of the week. This can be one or more of the following values. • **1**. Monday • **2**. Tuesday • **3**. Wednesday • **4**. Thursday • **5**. Friday • **6**. Saturday • **7**. Sunday
		endingDate	Optional	String	Date when the schedule ends
		endTime	Optional	String	Time when the schedule ends
		id	Optional	Integer	Schedule ID
		initialEndTime	Optional	String	
		initialStartTime	Optional	String	
		repeatable	Optional	Boolean	Indicates whether the schedule is recurring. This can be one of the following values. • **true**. The schedule is recurring. • **false**. The schedule occurs only once.
		seriesId	Optional	Integer	Schedule index
		startingDate	Optional	String	Date when the schedule starts
		startTime	Optional	String	Time when the schedule starts

Table 101. Syslog (continued)

	summary	Optional	Boolean	
showSummary		Optional	String	Indicates whether the schedule summary is enabled. The summary includes the time slot for schedule and which schedules are repeatable. This can be one of the following values. • **true**. The schedule summary is enabled. • **false**. The schedule summary is disabled.

The following example modifies an event forwarder for a syslog recipient.

```
{
    "communicationProtocol": "UDP",
    "dateFormat": "Default_Format",
    "description": "",
    "enable": "true",
    "eventFilter": {
        "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "eventID": "",
            "eventServices": [],
            "excludedEventIDs": "",
            "negateFilter": false,
            "sourceIDs": [],
            "typeSeverity": [{
                "severity": "INFORMATIONAL",
                "type": "AUDIT"
            },
            ...,
            {
                "severity": "FATAL",
                "type": "AUDIT"
            }]
        }
    },
    "forwardHidden": false,
    "ignoreExcluded": true,
    "ipAddress": "192.0.2.60",
    "matchEverything": true,
    "name": "syslog_forwarder",
    "port": "514",
    "protocol": "syslog",
    "requestTimeout": 30,
    "scheduler": {
        "enabled": false,
        "events": [],
        "showSummary": false
    }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /events/monitors/*{monitor_id}*

Use this method to delete a specific event forwarder.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/monitors/{monitor_id}`

where *{monitor_id}* is the ID of the event forwarder to be deleted. To obtain the filter ID, use the GET /events/monitors method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/monitors/certificate

Use this REST API to trust the certificate for a event forwarder.

HTTP methods

POST

POST /events/monitors/certificate

Use this method to download the certificate an event forwarder and add the certificate to the trusttore.

Attention: The certificate is downloaded and added to the truststore after the event forwarder is created or modified. A request to trust the certificate must be made **within 60 seconds** after making the request to create or modify the event forwarder.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/events/monitors/certificate`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
id	Required	String	ID of the event forwarder for which certificate approval is needed
trust	Required	Boolean	Indicates whether the trust the certificate. This can be one of the following values. • **true**. Trust the certificate. • **false**. Do not trust the certificate.

The following example trusts the certificate for an event forwarder.

```
{
   "id": "151554353",
   "trust": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/notifications

Use this REST API to retrieve configuration and subscription information for all push notification services or generate a test event that pushes to a specific push notification service or subscription.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, POST

GET /events/notifications

Use this method to return configuration and subscription information for all push notification services.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/notifications
```

Query parameters

Parameters	Required / Optional	Type	Definition
personalDataOnly=*{Boolean}*	Optional	Boolean	Indicates whether to return only subscriptions that were created by the user that is logged on. This can be one of the following values. • **true**. Returns only subscriptions that the user created. • **false**. Returns all subscriptions. This is the default value.
pusher=*{type}*	Optional	String	Returns information for a specific push notification service. This can be one of the following values. • **AndroidPusher**. Google device push service • **iOSPusher**. Apple device push service • **WebSocketPusher**. WebSocket servic
details=*{Boolean}*	Optional	Boolean	Indicates whether to include detailed information about each service type (pusher). This can be one of the following values. • **true**. Returns detailed information about each device type. • **false**. Returns only a list of device types. This is the default value.

The following example returns detailed configuration and subscription information for all push notification services that were created by the user that is logged on.

```
GET https://192.0.2.0/events/notifications?personalDataOnly=true&details=true
```

The following example returns detailed configuration and subscription information for all Google device push services that were created by the user that is logged on.

```
GET https://192.0.2.0/events/notifications?pusher=AndroidPusher&details=true
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
connectionIdle	Integer	(WebSocket push services only) Maximum amount of inactivity, in seconds. After this period the connection ends.
descriptionStr	String	Description of the push notification service
enable	Boolean	Indicates whether the push notification is enabled
maxBufferSize	Integer	(WebSocket push services only) Maximum size of a message, in KB
maxSubscribers	Integer	(WebSocket push services only) Maximum number of subscriptions
name	String	Name of the push notification service
nameStr	String	Displayable name of the push notification service
registerTimeout	Integer	(WebSocket push services only) Registration time-out, in seconds This is the number of seconds that the subscription has to sent a valid configuration JSON after the connection is initiated. If the JSON configuration is not sent within the time period, the connection ends.
subscriptions	Array of objects	List of subscriptions
filterList	Array of objects	Information about predefined and custom event filters
eventFilter	Array of objects	Information about the types of events to filter
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs, separated by a comma, that the event filter accepts in an event. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.

Attributes	Type	Definition
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted.
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by XClarity Administrator
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events
name	String	User-defined name of the event filter. This must be unique for all filters.
ipAddress	String	(WebSocket push services only) IP address
lastPushStatus	String	Status of the last push attempt
lastPushEventID	String	ID of the last pushed event
lastPushTimeStamp	String	Date of the last push attempt
phoneUID	String	(Android and iOS push services only) The displayable phone ID
registrationID	String	(Android and iOS push services only) The unique registration ID for a mobile device. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**.

Attributes		Type	Definition
	subscriberCategory	String	Subscription category
	subscriberCategoryExplanation	String	Description of the subscription category
	uid	String	Subscription UID
	userName	String	User that created the subscription

The following example is returned if the request is successful and when no query parameters are specified.


```
[{
   "descriptionStr": "The Google device push service",
   "enable": true,
   "name": "AndroidPusher",
   "nameStr": "Android Service"
},
{
   "descriptionStr": "The Apple device push service",
   "enable": true,
   "name": "iOSPusher",
   "nameStr": "iOS Service"
},
{
   "descriptionStr": "The XClarity WebSockets push service",
   "enable": true,
   "name": "WebSocketPusher",
   "nameStr": "WebSocket Service"
}]
```


The following example is returned if the request is successful and detailed information about the push notification services that were created by the user that is logged on.


```
{
   "enable": true,
   "descriptionStr": "The Apple device push service",
   "name": "iOSPusher",
   "nameStr": "iOS Service",
   "subscriptions": [{
      "filterList": [{
         "eventFilter": {
            "filter": {
               "typeSeverity": [{
                  "severity": "MAJOR",
                  "type": "UNKNOWN"
               },
               ...,
               {
                  "severity": "FATAL",
                  "type": "SWITCH"
               }],
               "sourceIDs": [],
               "categories": ["GENERAL"],
               "componentIDs": []
            }
         },
         "eventFilterDescription": "This filter will match all critical event generated in any
                                    of the managed endpoints or the manage server itself.",
         "eventFilterName": "Match All Critical",
         "isDeletable": false,
         "isEditable": false,
```

```
            "isUsed": true,
            "lockedPredefinedFilter": true,
            "matchEveryCoreEvent": false,
            "matchEverySystem": true,
            "matchEverything": false
         },
         {
            "eventFilter": {
               "filter": {
                  "typeSeverity": [{
                     "severity": "WARNING",
                     "type": "UNKNOWN"
                  },
                  ...,
                  {
                     "severity": "MINOR",
                     "type": "SWITCH"
                  }],
                  "sourceIDs": [],
                  "categories": ["GENERAL"],
                  "componentIDs": []
               }
            },
            "eventFilterDescription": "This filter will match all warning event generated in any
                                       of the managed endpoints or the manage server itself.",
            "eventFilterName": "Match All Warning",
            "isEditable": false,
            "isDeletable": false,
            "isUsed": true,
            "lockedPredefinedFilter": true,
            "matchEveryCoreEvent": false,
            "matchEverySystem": true,
            "matchEverything": false
         }],
         "subscriberCategoryExplanation": "This is a Apple Phone Subscriber",
         "lastPushEventID": "FQXHMEM0405I",
         "lastPushStatus": "Failure : java.net.SocketTimeoutException: Read timed out",
         "lastPushTimeStamp": "2017-03-29T15:16:30Z",
         "phoneUID": "5d57a0 ... 17b656",
         "registrationID": "5d57a05de25b7b91344931a91a64f0157bcaa834c8e6afe758e3f93da317b656",
         "subscriberCategory": "iOS Subscriber",
         "uid": "2",
         "userName": "USERID"
      }]
}
```


POST /events/notifications

Use this method to or generate a test event that pushes to a specific push notification service or subscription.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/events/notifications`

Query parameters

Parameters	Required / Optional	Description
includeAttributes=test	Required	Generate a test event that gets pushed to a specific push notification service or subscription

The following example generates a test event that gets pushed to the specified target.

```
POST https://192.0.2.0/events/notifications?includeAttributes=test
```

Request body

Attributes	Required / Optional	Type	Definition
targetID	Required	String	If **targetType** is `pusher`, this is the type of push notification service. This can be one of the following values. • **AndroidPusher**. Google device push service • **iOSPusher**. Apple device push service • **WebSocketPusher**. WebSocket servic If **targetType** is `subscriber`, this is the subscription UID. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.
targetType	Optional	Integer	Target of the test action. This can be one of the following values. • **pusher**. Push notification service • **subscriber**. Subscription

This example retrieves information about the Android the push notification service:

```
{
   "targetType":"pusher",
   "targetID":"AndroidPusher"
}
```

This example retrieves information for a subscription with UID 1.

```
{
   "targetType":"subscriber",
   "targetID":"1"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/notifications/*{pusher_type}*

Use this REST API to retrieve information about a specific push notification service.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET

GET /events/notifications/*{pusher_type}*

Use this method to return information about a specific push notification service.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/notifications/{pusher_type}`

where *{pusher_type}* is the type of push notification service. This can be one of the following values.
- **AndroidPusher**. Google device push service
- **iOSPusher**. Apple device push service
- **WebSocketPusher**. WebSocket servic

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
descriptionStr	String	Description of the push notification service
enable	Boolean	Indicates whether the push notification service is enabled

Attributes	Type	Definition
name	String	Type of push notification service
nameStr	String	Displayable name of the push notification service

The following example is returned if the request is successful for the Google push notification service (AndroidPusher).

```
{
   "descriptionStr": "The Google device push service",
   "enable": true
   "name": "AndroidPusher",
   "nameStr": "Android Service",
}
```

/events/notifications/*{pusher_type}*/subscriptions

Use this REST API to retrieve information about all subscriptions for a specific push notification service, modify a subscription that is used to forward events to mobile devices or WebSocket service, or delete all subscriptions for a specific push notification service.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, POST, DELETE

GET /events/notifications/*{pusher_type}*/subscriptions

Use this method to return information about all subscriptions for a specific push notification service.

If you are logged in as a user with one of the following roles, information that is associated with all subscriptions is returned; otherwise, information associated with subscriptions for only the logged-in user is returned.

- **lxc-admin**
- **lxc-supervisor**
- **lxc-security-admin**
- **lxc-sysmgr**

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions
```

where *{pusher_type}* is the type of push notification service. This can be one of the following values.

- **AndroidPusher**. Google device push service
- **iOSPusher**. Apple device push service
- **WebSocketPusher**. WebSocket servic

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
filterList	Array of objects	List of predefined and custom event filters
eventFilter	Array of objects	Information about the types of events to filter
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter are forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.

Attributes	Type	Definition
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted.
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by XClarity Administrator
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events
name	String	User-defined name of the event filter. This must be unique for all filters.
lastPushStatus	String	Status of the last push attempt
lastPushEventID	String	ID of the last pushed event
lastPushTimeStamp	String	Date of the last push attempt
phoneUID	String	(Android and iOS push services only) The displayable phone ID
registrationID	String	(Android and iOS push services only) Unique registration ID for a mobile device. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**
subscriberCategory	String	Subscription category
subscriberCategoryExplanation	String	Description of the subscription category
uid	String	Subscription UID
userName	String	User that created the subscription

The following example is returned if the request is successful.

```
[{
   "filterList": [{
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
```

```
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "MAJOR",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "FATAL",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all critical event generated in any
                                 of the managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Critical",
      "isDeletable": false,
      "isUsed": true,
      "isEditable": false,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   },
   {
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "WARNING",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "MINOR",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all warning event generated in any of the
                                 managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Warning",
      "isEditable": false,
      "isDeletable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   }],
   "lastPushEventID": "FQXHMEM04O6I",
   "lastPushStatus": "Success",
   "lastPushTimeStamp": "2017-03-29T15:09:16Z",
   "phoneUID": "cl8SqE ... KXbXR3",
   "registrationID": "cl8SqERZpSQ:APA91bGfoNOCAOsyHZTq4epEF8bOfYbx-hpJFRZqhDZ4SJwC5rQUmgZG8ZtzOFty2
                      VqaWIV_oU6GLnYeHNXJdPXjX8QRW9_blAwdiTVA_vtblMOxVYZUwP2OWYtFhi2CMb5RufKXbXR3",
   "subscriberCategory": "Android Subscriber",
   "subscriberCategoryExplanation": "This is a Google Phone Subscriber"
   "uid": "1",
```

```
   "userName": "USERID"
},
{
   "filterList": [{
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "MAJOR",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "FATAL",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all critical event generated in any of the
                                 managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Critical",
      "isDeletable": false,
      "isEditable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   },
   {
      "eventFilter": {
         "filter": {
            "typeSeverity": [{
               "severity": "WARNING",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "MINOR",
               "type": "SWITCH"
            }],
            "sourceIDs": [],
            "categories": ["GENERAL"],
            "componentIDs": []
         }
      },
      "eventFilterDescription": "This filter will match all warning event generated in any of the
                                 managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Warning",
      "isDeletable": false,
      "isEditable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   }],
   "lastPushEventID": "FQXHMEM0405I",
   "lastPushTimeStamp": "2017-03-29T15:16:30Z",
```

```
   "lastPushStatus": "Failure : java.net.SocketTimeoutException: Read timed out",
   "phoneUID": "5d57a0 … 17b656",
   "registrationID": "5d57a05de25b7b91344931a91a64f0157bcaa834c8e6afe758e3f93da317b656",
   "subscriberCategory": "iOS Subscriber",
   "subscriberCategoryExplanation": "This is a Apple Phone Subscriber"
   "uid": "2",
   "userName": "USERID"
}]
```

POST /events/notifications/*{pusher_type}*/subscriptions

Use this method to create a subscription that is used to forward events to mobile devices or WebSocket service.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions`

where *{pusher_type}* is the type of push notification service. This can be one of the following values.
- **AndroidPusher**. Google device push service
- **iOSPusher**. Apple device push service
- **WebSocketPusher**. WebSocket servic

Query parameters

None

Request body

Attributes	Required / Optional	Type	Definition
class	Required	String	Type of subscription. This can be one of the following values. • **AndroidSubscriber**. Forwards events to a Google device. • **iOSSubscriber** . Forwards events to an Apple device. • **WebSocketSubscriber** . Forwards events to a WebSocket service.
filterList	Required	Array of objects	One or more filters. This can be a predefined filter or a full description of a new filter.
filter	Required if **predefinedFilterName** is not specified	Object	Information about event filters
eventFilter	Optional	Array of objects	Information about the types of events to filter
filter	Optional	Object	Information about each event filter

Attributes	Re-quired / Optional	Type	Definition
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Optional	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.
severity	Optional	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Optional	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	Optional	String	Filter description
eventFilterName	Optional	String	Filter name
matchEveryCoreEvent	Optional	Boolean	Indicates whether this filter accepts all core events. This can be one of the following values. • **true**. Forward all core events • **false**
matchEverySystem	Optional	Boolean	Indicates whether this filter must match every event from every device. This can be one of the following values. • **true**. Forward events for all managed devices. • **false**

Attributes	Re-quired / Optional	Type	Definition
matchEverything	Optional	Boolean	Identifies whether the service forwarder is set to match any manageable device. This can be one of the following values. • **true**. The service forwarder is set to match any manageable device. • **false**. The service forwarder is not set to match any manageable device.
predefinedFilterName	Required if **filter** is not specified	String	Name of predefined event filter. This can be one of the following values. • **Match All Critical** • **Match All Warning**
phoneUID	Required	String	(Android and iOS push services only) Displayable phone ID
preferredLanguage	Optional	String	Preferred language for the push notification payload. This can be one of the following values. • **en**. English • **de**. German • **es**. Spanish • **fr**. French • **it**. Italian • **ja**. Japanese • **ko**. Korean • **pt**. Brazilian Portuguese • **zh**. Simplified Chinese • **zh-hant**. Traditional Chinese
registrationID	Optional	String	(Android and iOS push services only) Unique registration ID for a mobile device. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**.

The following example creates a subscription for an Android device:

```
{
   "class": "AndroidSubscriber",
   "filterList": [{
      "predefinedFilterName": "Match All Critical"
   }],
   "phoneUID": "P121",
   "preferredLanguage": "en",
   "registrationID": "df1dbe86bc811ddb57d76ca69804a56c8ba74a56a5231715304b95a67ec00fbe"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /events/notifications/*{pusher_type}*/subscriptions

Use this method to delete all subscriptions for a specific push notification service.

Authentication

Authentication with username and password is required.

Request URL

```
DELETE https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions
```

where *{pusher_type}* is the type of push notification service. This can be one of the following values.

- **AndroidPusher**. Google device push service
- **iOSPusher**. Apple device push service
- **WebSocketPusher**. WebSocket servic

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/notifications/*{pusher_type}*/subscriptions/*{subscription_ID}*

Use this REST API to retrieve information about a specific subscription for a specific push notification service or delete a specific subscription.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, DELETE

GET /events/notifications/*{pusher_type}*/subscriptions/*{subscription_ID}*

Use this method to return information about a specific subscription for a specific push notification service.

If you are logged in as a user with one of the following roles, information is associated with all subscriptions is returned; otherwise, information associated with subscriptions for only the logged-in user is returned.

- **lxc-admin**
- **lxc-supervisor**
- **lxc-security-admin**
- **lxc-sysmgr**

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions/{subscription_ID}`

where

- *{pusher_type}* is the type of push notification service. This can be one of the following values.
  - **AndroidPusher**. Google device push service
  - **iOSPusher**. Apple device push service
  - **WebSocketPusher**. WebSocket servic

  Tip: Because the subscription ID is unique, specifying the type of push notification service is optional
- *{subscription_ID}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
filterList	Array of objects	List of predefined and custom event filters
eventFilter	Array of objects	Information about the types of events to filter
filter	Object	Information about each event filter

Attributes	Type	Definition
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted.
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by XClarity Administrator
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events

Attributes	Type	Definition
matchEverything	Boolean	Indicates whether this event filter matches all events
name	String	User-defined name of the event filter. This must be unique for all filters.
lastPushStatus	String	Status of the last push attempt
lastPushEventID	String	ID of the last pushed event
lastPushTimeStamp	String	Date of the last push attempt
phoneUID	String	(Android and iOS push services only) The displayable phone ID
registrationID	String	(Android and iOS push services only) The unique registration ID for a mobile device. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**
subscriberCategory	String	Subscription category
subscriberCategoryExplanation	String	Description of the subscription category
uid	String	Subscription UID
userName	String	User that created the subscription

The following example is returned if the request is successful.

```
[{
   "filterList": [{
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "MAJOR",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "FATAL",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all critical event generated in any
                                 of the managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Critical",
      "isEditable": false,
      "isDeletable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   },
   {
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
```

```
            "typeSeverity": [{
               "severity": "WARNING",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "MINOR",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all warning event generated in any of
                                 the managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Warning",
      "isEditable": false,
      "isDeletable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   }],
   "lastPushEventID": "FQXHMEM0405I",
   "lastPushStatus": "Failure : java.net.SocketTimeoutException: Read timed out",
   "lastPushTimeStamp": "2017-03-29T15:16:30Z",
   "phoneUID": "5d57a0 ... 17b656",
   "registrationID": "5d57a05de25b7b91344931a91a64f0157bcaa834c8e6afe758e3f93da317b656",
   "subscriberCategory": "iOS Subscriber",
   "subscriberCategoryExplanation": "This is a Apple Phone Subscriber"
   "uid": "2",
   "userName": "USERID"
}]
```


DELETE /events/notifications/*{pusher_type}*/subscriptions/*{subscription_id}*

Use this method to delete a specific subscription.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions/{subscription_id}`

where

- *{pusher_type}* is the type of push notification service. This can be one of the following values.
  - **AndroidPusher**. Google device push service
  - **iOSPusher**. Apple device push service
  - **WebSocketPusher**. WebSocket servic

  Tip:

  - Because the subscription ID is unique, specifying the type of push notification service is optional.
  - You can delete the specified subscription even if it does not match the specified type of push notification service.
- *{subscription_ID}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/notifications/*{pusher_type}*/subscriptions/*{subscription_id}*/filters

Use this REST API to retrieve information about all event filters that are associated with a specific push notification service, to create an event filter for a specific subscription, or to delete all event filters for a specific subscription.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, POST, DELETE

GET /events/notifications/*{pusher_type}*/subscriptions/*{subscription_ID}*/filters

Use this method to return information about all event filters that are associated with a specific push notification service.

If you are logged in as a user with one of the following roles, information that is associated with all subscriptions is returned; otherwise, information associated with subscriptions for only the logged-in user is returned.

- **lxc-admin**
- **lxc-supervisor**
- **lxc-security-admin**
- **lxc-sysmgr**

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions/{subscription_ID}/filters`

where

- *{pusher_type}* is the type of push notification service. This can be one of the following values.
  - **AndroidPusher**. Google device push service
  - **iOSPusher**. Apple device push service
  - **WebSocketPusher**. WebSocket servic

  Tip: Because the subscription ID is unique, specifying the type of push notification service is optional
- *{subscription_ID}* is the UID of the subscription is retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
eventFilter	Array of objects	Information about the types of events to filter.
filter	Object	Information about each event filter.
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.

Attributes	Type	Definition
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by XClarity Administrator
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events
name	String	User-defined name of the event filter. This must be unique for all filters.

The following example is returned if the request is successful.

```
[{
   "eventFilter": {
      "filter": {
         "categories": ["GENERAL"],
         "componentIDs": [],
         "sourceIDs": [],
         "typeSeverity": [{
            "severity": "MAJOR",
            "type": "UNKNOWN"
         },
         ...,
         {
            "severity": "FATAL",
```

```
            "type": "SWITCH"
         }]
      }
   },
   "eventFilterDescription": "This filter will match all critical event generated in any
                              of the managed endpoints or the manage server itself.",
   "eventFilterName": "Match All Critical",
   "isDeletable": false,
   "isEditable": false,
   "isUsed": true,
   "lockedPredefinedFilter": true,
   "matchEveryCoreEvent": false,
   "matchEverySystem": true,
   "matchEverything": false
},
{
   "eventFilter": {
      "filter": {
         "categories": ["GENERAL"],
         "componentIDs": [],
         "sourceIDs": [],
         "typeSeverity": [{
            "severity": "WARNING",
            "type": "UNKNOWN"
         },
         ...,
         {
            "severity": "MINOR",
            "type": "SWITCH"
         }]
      }
   },
   "eventFilterDescription": "This filter will match all warning event generated in any of the
                              managed endpoints or the manage server itself.",
   "eventFilterName": "Match All Warning",
   "isDeletable": false,
   "isEditable": false,
   "isUsed": true,
   "lockedPredefinedFilter": true,
   "matchEveryCoreEvent": false,
   "matchEverySystem": true,
   "matchEverything": false
}]
```

POST /events/notifications/*{pusher_type}*/subscriptions/*{subscription_ID}*/filters

Use this method to create an event filter for a specific subscription.

If you are logged in as a user with one of the following roles, information that is associated with all subscriptions is returned; otherwise, information associated with subscriptions for only the logged-in user is returned.

- **lxc-admin**
- **lxc-supervisor**
- **lxc-security-admin**
- **lxc-sysmgr**

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions/{subscription_ID}/filters`

where

- *{pusher_type}* is the type of push notification service. This can be one of the following values.
  - **AndroidPusher**. Google device push service
  - **iOSPusher**. Apple device push service
  - **WebSocketPusher**. WebSocket servic

  Tip: Because the subscription ID is unique, specifying the type of push notification service is optional
- *{subscription_ID}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Definition
eventFilter	Required	Array of objects	Information about the types of events to filter
filter	Required	Object	Information about each event filter
categories	Required	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Required	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Required	Array of strings	List of source IDs. If empty, all sources are accepted..
typeSeverity	Required	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.
severity	Required	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.

Attributes	Required / Optional	Type	Definition
type	Required	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	Required	String	Event filter description
eventFilterName	Required	String	Event filter name
matchEveryCoreEvent	Optional	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Optional	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Optional	Boolean	Indicates whether this event filter matches all events

The following example creates an event filter for a specific subscription.

```
{
   "eventFilterName": "example2",
   "eventFilterDescription": "Description",
   "eventFilter": {
      "filter": {
         "componentIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
         "500C0FF286F98000"],
         "sourceIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
         "500C0FF286F98000"],
         "typeSeverity": [{
            "severity": "fatal",
            "type": "all"
         },
         ...,
         {
            "severity": "informational",
            "type": "audit"
         }],
         "categories": ["WARRANTY",
         "GENERAL"]
      }
   },
   "matchEverySystem": false,
   "matchEveryCoreEvent": false
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /events/notifications/*{pusher_type}*/subscriptions/*{subscription_id}*/filters

Use this method to delete all event filters for a specific subscription.

If you are logged in as a user with one of the following roles, information that is associated with all subscriptions is returned; otherwise, information associated with subscriptions for only the logged-in user is returned.

- **lxc-admin**
- **lxc-supervisor**
- **lxc-security-admin**
- **lxc-sysmgr**

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions/{subscription_id}/filters`

where

- *{pusher_type}* is the type of push notification service. This can be one of the following values.
  - **AndroidPusher**. Google device push service
  - **iOSPusher**. Apple device push service
  - **WebSocketPusher**. WebSocket servic

  Tip: Because the subscription ID is unique, specifying the type of push notification service is optional
- *{subscription_ID}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/notifications/*{pusher_type}*/subscriptions/*{subscription_id}*/filters/*{filter_name}*

Use this REST API to retrieve information about a specific event filter that is associated with a specific subscription or to delete one or more event filters from a specific subscription.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, DELETE

GET /events/notifications/*{pusher_type}*/subscriptions/*{subscription_ID}*/filters/*{filter_name}*

Use this method to return information about a specific event filter that is associated with a specific subscription.

If you are logged in as a user with one of the following roles, information that is associated with all subscriptions is returned; otherwise, information associated with subscriptions for only the logged-in user is returned.

- **lxc-admin**
- **lxc-supervisor**
- **lxc-security-admin**
- **lxc-sysmgr**

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions/{subscription_ID}/filters/{filter_name}`

where

- *{pusher_type}* is the type of push notification service. This can be one of the following values.
  - **AndroidPusher**. Google device push service
  - **iOSPusher**. Apple device push service
  - **WebSocketPusher**. WebSocket servic

Tip: Because the subscription ID is unique, specifying the type of push notification service is optional

- *{subscription_ID}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.
- *{filter_name}* is the name of the event filter to be retrieved. To obtain the event filter name, use the GET /events/notifications/subscriptions/*{subscription_id}*/filters method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
eventFilter	Array of objects	Information about the types of events to filter
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.

Attributes	Type	Definition
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted.
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by XClarity Administrator
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events
name	String	User-defined name of the event filter. This must be unique for all filters.

The following example is returned if the request is successful.

```
[{
   eventFilter: {
      filter: {
         typeSeverity: [{
            severity: "MAJOR",
            type: "UNKNOWN"
         },
         ..............{
            severity: "FATAL",
            type: "SWITCH"
         }],
         sourceIDs: ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
         "500C0FF286F98000"],
```

```
        categories: ["WARRANTY",
        "GENERAL"],
        componentIDs: ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
        "500C0FF286F98000"]
      }
   },
   eventFilterDescription: "",
   eventFilterName: "example2",
   isDeletable: true,
   isEditable: true,
   isUsed: true,
   matchEveryCoreEvent: false,
   matchEverySystem: false,
   matchEverything: false,
}]
```

DELETE /events/notifications/*{pusher_type}*/subscriptions/*{subscription_id}*/filters/*{filter_list}*

Use this method to delete one or more event filters from a specific subscription.

If you are logged in as a user with one of the following roles, information that is associated with all subscriptions is returned; otherwise, information associated with subscriptions for only the logged-in user is returned.

- **lxc-admin**
- **lxc-supervisor**
- **lxc-security-admin**
- **lxc-sysmgr**

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/notifications/{pusher_type}/subscriptions/{subscription_ID}/filters/{filter_list}`

where

- *{pusher_type}* is the type of push notification service. This can be one of the following values.
  - **AndroidPusher**. Google device push service
  - **iOSPusher**. Apple device push service
  - **WebSocketPusher**. WebSocket servic

  Tip: Because the subscription ID is unique, specifying the type of push notification service is optional
- *{subscription_id}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.
- *{filter_list}* is a list of one or more names, separated by a comma, of the event filters to be deleted (for example, `All Storage Events`,`All Switch Events`). To obtain the event filter names, use the GET /events/notifications/subscriptions/*{subscription_id}*/filters method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/notifications/subscriptions

Use this REST API to retrieve information about all subscriptions or delete all subscriptions for all push notification services.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, DELETE

GET /events/notifications/subscriptions

Use this method to return information about all subscriptions.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/notifications/subscriptions
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
filterList	Array of objects	List of predefined and custom event filters
eventFilter	Array of objects	Information about the types of events to filter
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted.
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription

Attributes	Type	Definition
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by Lenovo XClarity Administrator
name	String	User-defined name of the event filter. This must be unique for all filters.
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events
lastPushEventID	String	ID of the last pushed event
lastPushStatus	String	Status of the last push attempt
lastPushTimeStamp	String	Date of the last push attempt
phoneUID	String	(Android and iOS push services only) The displayable phone ID
registrationID	String	(Android and iOS push services only) The unique registration ID for a mobile device. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**.
subscriberCategory	String	Subscription category
subscriberCategoryExplanation	String	Description of the subscription category
uid	String	Subscription UID
userName	String	User that created the subscription

The following example is returned if the request is successful.

```
[{
   "filterList": [{
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "MAJOR",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "FATAL",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all critical event generated in any
                                 of the managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Critical",
      "isDeletable": false,
      "isEditable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
```

```
   },
   {
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "WARNING",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "MINOR",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all warning event generated in any of
                                 the managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Warning",
      "isDeletable": false,
      "isEditable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   }],
   "lastPushEventID": "FQXHMEM0406I",
   "lastPushStatus": "Success",
   "lastPushTimeStamp": "2017-03-29T15:09:16Z",
   "phoneUID": "cl8SqE ... KXbXR3",
   "registrationID": "cl8SqERZpSQ:APA91bGfoNOCAOsyHZTq4epEF8bOfYbx-hpJFRZqhDZ4SJwC5rQUmgZG8ZtzOFty
                      2VqaWIV_oU6GLnYeHNXJdPXjX8QRW9_blAwdiTVA_vtblMOxVYZUwP2OWYtFhi2CMb5RufKXbXR3",
   "subscriptionCategory": "Android Subscription",
   "subscriptionCategoryExplanation": "This is a Google Phone Subscription",
   "uid": "1",
   "userName": "USERID"
},
{
   "filterList": [{
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "MAJOR",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "FATAL",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all critical event generated in any of the
                                 managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Critical",
```

```
      "isDeletable": false,
      "isEditable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   },
   {
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "WARNING",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "MINOR",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all warning event generated in any of the
                                 managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Warning",
      "isDeletable": false,
      "isEditable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   }],
   "lastPushEventID": "FQXHMEM0405I",
   "lastPushStatus": "Failure : java.net.SocketTimeoutException: Read timed out",
   "lastPushTimeStamp": "2017-03-29T15:16:30Z",
   "phoneUID": "5d57a0 … 17b656",
   "registrationID": "5d57a05de25b7b91344931a91a64f0157bcaa834c8e6afe758e3f93da317b656",
   "subscriptionCategory": "iOS Subscription",
   "subscriptionCategoryExplanation": "This is a Apple Phone Subscription",
   "uid": "2",
   "userName": "USERID"
}]
```


PUT /events/notifications/subscriptions

Use this method to modify a subscription that is used to forward events to mobile devices or WebSocket service.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/events/notifications/subscriptions`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Definition
action	Required	String	Action to perform. This can be one of the following values. • **edit**. Modify the subscription properties
class	Required	String	Type of subscription. This can be one of the following values. • **AndroidSubscriber**. Forwards events to a Google device. • **iOSSubscriber** . Forwards events to an Apple device. • **WebSocketSubscriber** . Forwards events to a WebSocket service.
filterList	Required	Array of objects	One or more filters. This can be a predefined filter or a full description of a new filter.
filter	Required if **predefinedFilterName** is not specified	Object	Information about the filters
eventFilter	Optional	Array of objects	Information about the types of events to filter.
filter	Optional	Object	Information about each event filter
categories	Optional	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Optional	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.

Attributes	Re-quired / Optional	Type	Definition
severity	Optional	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Optional	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	Optional	String	Filter description
eventFilterName	Optional	String	Filter name
matchEveryCoreEvent	Optional	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Optional	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Optional	Boolean	Indicates whether this event filter matches all events
predefinedFilterName	Required if **filter** is not specified	String	The name of predefined event filter. This can be one of the following values: • **Match All Critical** • **Match All Warning**
phoneUID	Required	String	(Android and iOS push services only) The displayable phone ID

Attributes	Required / Optional	Type	Definition
preferredLanguage	Optional	String	Preferred language for the push notification payload. This can be one of the following values: • **en**. English • **de**. German • **es**. Spanish • **fr**. French • **it**. Italian • **ja**. Japanese • **ko**. Korean • **pt**. Brazilian Portuguese • **zh**. Simplified Chinese • **zh-hant**. Traditional Chinese
registrationID	Optional	String	(Android and iOS push services only) The unique registration ID for a mobile device. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**.

The following example modifies a subscription that is used to forward events to mobile devices or WebSocket service.

```
{
    "action": "add"
    "class": "AndroidSubscriber",
    "filterList": [{
      "predefinedFilterName": "Match All Critical"
   }],
   "phoneUID": "fr2Z6X ... mwgqqs",
   "preferredLanguage": "en",
   "registrationID": "fr2Z6X5_w38:APA91bEkN1JOnMFxZmcLuT4NMOWvFGJOTTZsUTrXmYmmCzLddf
                      _iD7tfnovHqzBOwqIz5mfwg9JBSLLOA96DdqDRby92ld2_FfwRf4T8ef_AGLydq
                      DOfd3F_faIXYmWQmWOFymwgqqs"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /events/notifications/subscriptions

Use this method to delete all subscriptions for all push notification services.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/notifications/subscriptions`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/notifications/subscriptions/*{subscription_id}*

Use this REST API to retrieve information about or delete a specific subscription.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, DELETE

GET /events/notifications/subscriptions/*{subscription_id}*

Use this method to return information about a specific subscription.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/notifications/subscriptions/{subscription_id}`

where *{subscription_id}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
filterList	Array of objects	List of predefined and custom event filters
eventFilter	Array of objects	Information about the types of events to filter
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.

Attributes	Type	Definition
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted.
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by XClarity Administrator
name	String	User-defined name of the event filter. This must be unique for all filters.
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events
lastPushStatus	String	Status of the last push attempt
lastPushEventID	String	ID of the last pushed event
lastPushTimeStamp	String	Date of the last push attempt
phoneUID	String	(Android and iOS push services only) The displayable phone ID
registrationID	String	(Android and iOS push services only) The unique registration ID for a mobile device. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**.
subscriberCategory	String	Subscription category
subscriberCategoryExplanation	String	Description of the subscription category
uid	String	Subscription UID
userName	String	User that created the subscription

The following example is returned if the request is successful.

```
[{
   "filterList": [{
      "eventFilter": {
         "filter": {
```

```
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "MAJOR",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "FATAL",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all critical event generated in any
                                 of the managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Critical",
      "isEditable": false,
      "isDeletable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   },
   {
      "eventFilter": {
         "filter": {
            "categories": ["GENERAL"],
            "componentIDs": [],
            "sourceIDs": [],
            "typeSeverity": [{
               "severity": "WARNING",
               "type": "UNKNOWN"
            },
            ...,
            {
               "severity": "MINOR",
               "type": "SWITCH"
            }]
         }
      },
      "eventFilterDescription": "This filter will match all warning event generated in any
                                 of the managed endpoints or the manage server itself.",
      "eventFilterName": "Match All Warning",
      "isEditable": false,
      "isDeletable": false,
      "isUsed": true,
      "lockedPredefinedFilter": true,
      "matchEveryCoreEvent": false,
      "matchEverySystem": true,
      "matchEverything": false
   }],
   "lastPushEventID": "FQXHMEM0405I",
   "lastPushStatus": "Failure : java.net.SocketTimeoutException: Read timed out",
   "lastPushTimeStamp": "2017-03-29T15:16:30Z",
   "phoneUID": "5d57a0 ... 17b656",
   "registrationID": "5d57a05de25b7b91344931a91a64f0157bcaa834c8e6afe758e3f93da317b656",
   "subscriberCategory": "iOS Subscriber",
   "subscriberCategoryExplanation": "This is a Apple Phone Subscriber"
   "uid": "2",
```

```
   "userName": "USERID"
}]
```

DELETE /events/notifications/subscriptions/*{subscription_id}*

Use this method to delete a specific subscription.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/notifications/subscriptions/{subscription_id}`

where *{subscription_id}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/notifications/subscriptions/*{subscription_id}*/filters

Use this REST API to retrieve information about all event filters that are associated with a specific subscription or to delete all event filters for a specific subscription.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, DELETE

GET /events/notifications/subscriptions/*{subscription_id}*/filters

Use this method to return information about all event filters that are associated with a specific subscription.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/notifications/subscriptions/{subscription_id}/filters`

where *{subscription_id}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
eventFilter	Array of objects	Information about the types of events to filter
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.

Attributes	Type	Definition
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted.
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by XClarity Administrator
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events
name	String	User-defined name of the event filter. This must be unique for all filters.

The following example is returned if the request is successful.

```
[{
   "eventFilter": {
      "filter": {
         "categories": ["GENERAL"],
         "componentIDs": [],
         "sourceIDs": [],
         "typeSeverity": [{
            "severity": "MAJOR",
            "type": "UNKNOWN"
         },
         ...,
         {
            "severity": "FATAL",
```

```
            "type": "SWITCH"
         }]
      }
   },
   "eventFilterDescription": "This filter will match all critical event generated in any
                              of the managed endpoints or the manage server itself.",
   "eventFilterName": "Match All Critical",
   "isDeletable": false,
   "isEditable": false,
   "isUsed": true,
   "lockedPredefinedFilter": true,
   "matchEveryCoreEvent": false,
   "matchEverySystem": true,
   "matchEverything": false
},
{
   "eventFilter": {
      "filter": {
         "categories": ["GENERAL"],
         "componentIDs": [],
         "sourceIDs": [],
         "typeSeverity": [{
            "severity": "WARNING",
            "type": "UNKNOWN"
         },
         ...,
         {
            "severity": "MINOR",
            "type": "SWITCH"
         }]
      }
   },
   "eventFilterDescription": "This filter will match all warning event generated in any of the
                              managed endpoints or the manage server itself.",
   "eventFilterName": "Match All Warning",
   "isDeletable": false,
   "isEditable": false,
   "isUsed": true,
   "lockedPredefinedFilter": true,
   "matchEveryCoreEvent": false,
   "matchEverySystem": true,
   "matchEverything": false
}]
```

PUT /events/notifications/subscriptions/*{subscription_id}*/filters

Use this method to modify an event filter.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/events/notifications/subscriptions/{subscription_id}/filters`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Definition
action	Required	String	Action to perform. This can be one of the following values. • **edit**. Modify an event filter.
filter	Required	Object	List of event filters
eventFilter	Required	Array of objects	Information about the types of events to filter
filter	Required	Object	Information about each event filter
categories	Required	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Required	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.
severity	Optional	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Optional	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	Optional	String	Event filter description

Attributes	Required / Optional	Type	Definition
eventFilterName	Optional	String	Event filter name
matchEveryCoreEvent	Optional	Boolean	Indicates whether this event filter accepts all core events.
matchEverySystem	Optional	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Optional	Boolean	Indicates whether this event filter matches all events
uid	Required	String	Subscription ID

The following example modifies an event filter.

```
{
   "action": "edit",
   "filter": {
      "eventFilter": {
         "filter": {
            "categories": ["WARRANTY", "GENERAL"],
            "componentIDs": [],
            "sourceIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"],
            "typeSeverity": [{
               "severity": "fatal",
               "type": "all"
            },
            ...,
            {
               "severity": "informational",
               "type": "audit"
            }]
         }
      },
      "eventFilterDescription": "sadfasdf",
      "eventFilterName": "asdfasdf",
      "matchEveryCoreEvent": false,
      "matchEverySystem": false
   },
   "uid": "1"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /events/notifications/subscriptions/*{subscription_id}*/filters

Use this method to delete all event filters for a specific subscription.

Authentication

Authentication with username and password is required.

Request URL

```
DELETE https://{management_server_IP}/events/notifications/subscriptions/{subscription_id}/filters
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/notifications/subscriptions/*{subscription_id}*/filters/*{filter_name}*

Use this REST API to retrieve information about a specific event filter that is associated with a specific subscription or to delete one or more event filters from a specific subscription.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, DELETE

GET /events/notifications/subscriptions/*{subscription_id}*/filters/*{filter_name}*

Use this method to return information about a specific event filter that is associated with a specific subscription.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/events/notifications/subscriptions/{subscription_id}/filters/{filter_name}
```

where

- *{subscription_id}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.
- *{filter_name}* is the name of the event filter to be retrieved. To obtain the event filter name, use the GET /events/notifications/subscriptions/*{subscription_id}*/filters method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
eventFilter	Array of objects	Information about the types of events to filter
filter	Object	Information about each event filter
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.

Attributes	Type	Definition
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted.
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by Lenovo XClarity Administrator
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events
name	String	User-defined name of the event filter. This must be unique for all filters.

The following example is returned if the request is successful.

```
[{
   eventFilter: {
      filter: {
         typeSeverity: [{
            severity: "MAJOR",
            type: "UNKNOWN"
         },
         ..............{
            severity: "FATAL",
            type: "SWITCH"
         }],
         sourceIDs: ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
         "500C0FF286F98000"],
```

```
         categories: ["WARRANTY",
         "GENERAL"],
         componentIDs: ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
         "500C0FF286F98000"]
      }
   },
   eventFilterDescription: "",
   eventFilterName: "example2",
   isDeletable: true,
   isEditable: true,
   isUsed: true,
   matchEveryCoreEvent: false,
   matchEverySystem: false,
   matchEverything: false,
}]
```

DELETE /events/notifications/subscriptions/*{subscription_id}*/filters/*{filter_list}*

Use this method to delete one or more event filters from a specific subscription.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/notifications/subscriptions/{subscription_id}/filters/{filter_list}`

where

- *{subscription_id}* is the UID of the subscription to be retrieved. To obtain the subscription UID, use the GET /events/notifications/subscriptions method.
- *{filter_list}* is a list of one or more names, separated by a comma, of the event filters to be deleted (for example, `All Storage Events,All Switch Events`). To obtain the event filter names, use the GET /events/notifications/subscriptions/*{subscription_id}*/filters method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/predefinedFilters

Use this REST API to retrieve, create, modify predefined event filters or to delete all predefined event filters.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

GET, PUT, POST, DELETE

GET /events/predefinedFilters

Use this method to return information about the predefined event filters.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/predefinedFilters`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Definition
eventFilter	Array of objects	List of predefined and custom event filters
filter	Object	Information about the types of events to filter
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.

Attributes	Type	Definition
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
isDeletable	Boolean	Indicates whether the event filter can be deleted
isEditable	Boolean	Indicates whether this event filter can be modified
isUsed	Boolean	Indicates whether this event filter is used by at least one subscription
lockedPredefinedFilter	Boolean	Indicates whether this is a predefined event filter that is provided by default by XClarity Administrator
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events
name	String	User-defined name of the event filter. This must be unique for all filters.

The following example is returned if the request is successful.

```
[{
   "eventFilter": {
       "filter": {
          "categories": ["GENERAL"],
          "componentIDs": [],
          "sourceIDs": [],
          "typeSeverity": [{
```

```
            "severity": "MAJOR",
            "type": "UNKNOWN"
         },
         ..,
         {
            "severity": "FATAL",
            "type": "BLADE"
         }]
      }
   }
   "eventFilterDescription": "This filter matches all critical events that are generated
                              in managed device or the management server itself."
   "eventFilterName": "Match All Critical",
   "isDeletable": false,
   "isEditable": false,
   "isUsed": true,
   "lockedPredefinedFilter": true,
   "matchEveryCoreEvent": false,
   "matchEverySystem": true,
   "matchEverything": false,
},
...,
{
   "eventFilter": {
      "filter": {
         "categories": ["WARRANTY", "GENERAL"],
         "componentIDs": [],
         "sourceIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"],
         "typeSeverity": [{
            "severity": "INFORMATIONAL",
            "type": "UNKNOWN"
         },
         ..,
         {
            "severity": "FATAL",
            "type": "BLADE"
         }]
      }
   }
   "eventFilterDescription": "",
   "eventFilterName": "sadfasdf",
   "isDeletable": true,
   "isEditable": true,
   "isUsed": false,
   "lockedPredefinedFilter": false,
   "matchEveryCoreEvent": false,
   "matchEverySystem": false,
   "matchEverything": false
}]
```


PUT /events/predefinedFilters

Use this method to modify the properties of a predefined event filter.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/events/predefinedFilters`

Query parameters

None

Response body

Attributes	Required / Optional	Type	Definition
eventFilter	Required	Array of objects	List of predefined and custom event filters
filter	Required	Object	Information about the types of events to filter
categories	Required	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Optional	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Optional	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Required	Array of objects	Event severity and type. If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.
severity	Optional	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
type	Optional	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	Required	String	Event filter description

Attributes	Required / Optional	Type	Definition
eventFilterName	Required	String	Event filter name
matchEveryCoreEvent	Optional	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Optional	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Optional	Boolean	Indicates whether this event filter matches all events

The following example modifies a predefined event filter.

```
{
   "action": "edit",
   "eventFilter": {
      "filter": {
         "componentIDs": [],
         "sourceIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"],
         "typeSeverity": [
            {
               "severity": "fatal",
               "type": "all"
            },
            ...,
            {
               "severity": "informational",
               "type": "audit"
            }
         ],
         "categories": [
            "WARRANTY",
            "GENERAL"
         ]
      }
   },
   "eventFilterDescription": "Fatal and informational events",
   "eventFilterName": "FatalInfoEvents ",
   "matchEveryCoreEvent": false,
   "matchEverySystem": false
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

POST /events/predefinedFilters

Use this method to create a predefined event filter.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/events/predefinedFilters`

Query parameters

None

Response body

Attributes	Type	Definition
eventFilter	Array of objects	list of predefined and custom event filters
filter	Object	Information about the types of events to filter
categories	Array of strings	Event categories. This can be one of the following values. • **BULLETIN**. Sends notification about new bulletins. • **GENERAL**. Sends notifications about audit events, based on the selected event classes and severities • **STATUS_CHANGE**. Sends notifications about changes in status. • **STATUS_UPDATE** • **WARRANTY**. Send notifications about warranties.
componentIDs	Array of strings	List of component IDs. If empty, all components are accepted.
sourceIDs	Array of strings	List of source IDs. If empty, all sources are accepted.
typeSeverity	Array of objects	Event severity and type If both **sourceIDs** and **componentsIDs** are empty, all events that match the **typeSeverity** filter is forwarded.
severity	String	Event severity. This can be one of the following values. • **Unknown**. The severity is unknown. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.

Attributes	Type	Definition
type	String	Event type. This can be one of the following values. • **Unknown** • **Audit** • **Cooling** • **Power** • **Disks**. Storage • **Memory** • **Processor** • **System**. Rack or tower server • **Test** • **Adaptor**. Adapter card • **Expansion**. Expansion board • **IOModule**. Flex System switch • **Blade**. Flex System server • **Switch**. switch
eventFilterDescription	String	Event filter description
eventFilterName	String	Event filter name
matchEveryCoreEvent	Boolean	Indicates whether this event filter accepts all core events
matchEverySystem	Boolean	Indicates whether this event filter must match every event from every managed device
matchEverything	Boolean	Indicates whether this event filter matches all events

The following example creates a predefined event filter.

```
{
   "action": "edit",
   "eventFilter": {
      "filter": {
         "componentIDs": [],
         "sourceIDs": ["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"],
         "typeSeverity": [
            {
               "severity": "fatal",
               "type": "all"
            },
            ...,
            {
               "severity": "informational",
               "type": "audit"
            }
         ],
         "categories": [
            "WARRANTY",
            "GENERAL"
         ]
      }
   },
   "eventFilterDescription": "Fatal and informational events",
   "eventFilterName": "FatalInfoEvents ",
   "matchEveryCoreEvent": false,
   "matchEverySystem": false
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /events/predefinedFilters

Use this method to delete all predefined event filters.

Authentication

Authentication with username and password is required.

Request URL

```
DELETE https://{management_server_IP}/events/predefinedFilters
```

Query parameters

None

Response body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/predefinedFilters/*{filters_id}*

Use this REST API to delete one or more predefined event filters.

Note: This REST API requires Lenovo XClarity Administrator v1.3.0 or later.

HTTP methods

DELETE

DELETE /events/predefinedFilters/*{filter_list}*

Use this method to delete one or more predefined event filters.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/events/predefinedFilters/{filter_list}`

where *{filter_list}* is a list of one or more names, separated by a comma, of the event filters to be deleted (for example, `All Storage Events,All Switch Events`). To obtain the event filter names, use the GET /events/notifications/subscriptions/*{subscription_id}*/filters method.

Query parameters

None

Response body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/events/snmp/mib

Use this REST API to download the management information base (MIB) file, which describes the SNMP traps that Lenovo XClarity Administrator generates.

HTTP methods

GET

GET /events/snmp/mib

Use this method to download the management information base (MIB) file, which describes the SNMP traps that Lenovo XClarity Administrator generates.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/events/snmp/mib`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

Chapter 12. Jobs

The following resources are available for performing task and job management functions.

/flows/settings

Use this REST API to retrieve the activity-flow status and to enable or disable activity flows.

HTTP methods

GET, PUT

GET /flows/settings

Use this method to return the activity-flow status.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/flows/settings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
enabled	Boolean	Indicates whether activity flows are enabled. This can be one of the following values. • **true**. Activity flows are enabled. • **False**. Activity flows are disabled.

The following example is returned if the request is successful.

```
{
   "enabled": true
}
```

PUT /flows/settings

Use this method to enable or disable activity flows.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/flows/settings`

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
enabled	Required	Boolean	Indicates whether activity flows are enabled. This can be one of the following values. • **true**. Activity flows are enabled. • **False**. Activity flows are disabled.

The following example enables activity flows.

```
{
   "enabled": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/tasks

Use this REST API to cancel a list of jobs (tasks) or to retrieve information about all jobs (tasks) and their subtasks.

HTTP methods

GET, PUT, POST

GET /tasks

Use this method to return information about all jobs (tasks) and their subtasks.

For message-description and user-action text in the job summary, you can specify the text directly in the request body if no translations are needed, or you can reference the text from a translated bundle file (for example, `com.lenovo.lxca.server.jobs.bundle.jobsSummary`).

When the job description and recovery actions require formatted text, you must specify the text as an array of objects in JSON format. You cannot use HTML.

Tip: In the translated bundle files, braces {} must be escaped by a single quote for help text (for example, '{').

Attribute	Required / Optional	Type	Description
format	Required	Array of strings	List of formats for the text. This can be one of the following values. • **bold**. Corresponds to the <b> HTML tag. • **italic**. Corresponds to the <i> HTML tag. • **underline**. Corresponds to the <u> HTML tag. • **link**. Corresponds to the <a> HTML tag. • **newline**. Corresponds to the HTML tag. • **paragraph**. Corresponds to the <p> HTML tag. • **quotation**. Corresponds to the <q> HTML tag. • **orderedList**. Corresponds to the HTML tag. • **bulletList**. Corresponds to the HTML tag. • **listElement**. Corresponds to the HTML tag. If no format is needed, use an empty array.
link	Optional	String	URL to be linked to
text	Required	String or array of strings	Text to be formatted

The following example has formatted text in the user action. It includes paragraphs, ordered list, unordered list, link, and formatted text. Note that braces {} *are not* escaped by a single quote.

```
[{
   "text": "To display the text correctly, the following steps are made.",
   "format": []
},
{
   "text": [],
   "format": ["newline"]
},
{
   "text": [{
      "text": "Segment the text into pieces between HTML tags.",
      "format": ["listElement"]
   },
   {
      "text": [{
         "text": "If the segmented text contains ",
         "format": []
      },
      {
         "text": "multiple tags",
         "format": ["bold"]
      },
      {
         "text": ", segment them as well.",
         "format": []
      }],
      "format": ["listElement"]
   },
   {
```

```
      "text": [ {
         "text": "After having all segments, add the tags as follows:",
         "format": []
      },
      {
         "text": [{
            "text": "Add the text between the tags in the text field of JSON. If multiple tags are found,
                      text field is an array of JSON Objects.",
            "format": ["listElement"]
         },
         {
            "text": "Add the format for each text between tags.",
            "format": ["listElement"]
         }],
         "format": ["bulletList"]
      }],
      "format": ["listElement"]
   },
   {
      "text": "Make sure this is a json format.",
      "format": ["listElement", "bold", "underline"]
   }],
   "format": ["orderedList"]
},
{
   "text": [],
   "format": ["newline"]
},
{
   "text": [{
      "text": "This is how a paragraph looks like with a ",
      "format": []
   },
   {
      "text": "link",
      "format": ["link"],
      "link": "https://www3.lenovo.com/"
   }],
   "format": ["paragraph"]
},
{
   "text": "This is how the result should look.",
   "format": ["paragraph", "italic"]
}]
```

This example correlates to the following HTML format

```
To display the text correctly, the following steps are made.
<br></br>
<ol>
<li>Segment the text into pieces between HTML tags.</li>
<li>If the segmented text contains <b>multiple tags</b>, segment them as well.</li>
<li>After having all segments, add the tags as follows:
<ul>
<li>Add the text between the tags in the text field of JSON. If multiple tags are found,
text field is an array of JSON Objects.</li>
<li>Add the format for each text between tags.</li>
</ul></li>
<li><b><u>Make sure this is a json format.</u></b></li>
</ol>
<br></br>
<p>This is how a paragraph looks like with a <a href="https://www3.lenovo.com/">link</a></p>
```

```
<p><i>This is how the result should look.</i></p>
```

This example correlates to the following formatted output:

To display the text correctly, the following steps are made.

1. Segment the text into pieces between HTML tags.
2. If the segmented text contains **multiple tags**, segment them as well.
3. After having all segments, add the tags as follows:
   - Add the text between the tags in the text field of JSON. If multiple tags are found, text field is an array of JSON Objects.
   - Add the format for each text between tags.
4. **Make sure this is a json format.**

This is how a paragraph looks like with a link

This is how the result should look.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/tasks
```

Query parameters

Parameters	Required / Optional	Description
uuid=*{uuids}*	Optional	Returns task information only for one or more specific groups and devices To obtain the group or device UUIDs, use GET /resourceGroups, GET /chassis, GET /cmms, GET /nodes, GET /storage, and GET /switches.
compact=*{Boolean}*	Optional	Indicates whether to return information about each subtask in the job. This can be one of the following values. • **true**. Does not return information about subtasks. • **false**. (default) Returns information about subtasks.

The following example returns information for tasks that are associated with two specific devices.

```
GET https://192.0.2.0/tasks?uuid=["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA","BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"]
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
children	Array of objects	Information about each subtask in the job
children	Array of objects	Information about each subtask in the subtask. The properties in this object are the same as the top-level children object.
complete	String	Date and time that the subtask was completed
create	String	Date and time that the subtask was created
createdBy	String	User name that created the subtask
filterStatusKey	String	This can be one of the following values. • **Complete** • **Error**
hasNotes	Boolean	Indicates whether the subtask has notes. This can be one of the following values. • **true**. The job has notes. • **false**. The job does not have notes.
hasNotesString	Boolean	Indicates whether the subtask has notes. This can be one of the following values. • **yes**. The job has notes. • **no**. The job does not have notes.
hidden	Boolean	Indicates whether the alert is hidden in the web interface. This can be one of the following values. • **true**. The alert is not displayed in the web interface. • **false**. (default) The alert is displayed in the web interface.
isDeletable	Boolean	Indicates whether the subtask can be deleted. This can be one of the following values. • **true**. The subtask can be deleted. • **false**. The subtask cannot be deleted.
isStoppable	Boolean	Indicates whether the subtask can be stopped. This can be one of the following values. • **true**. The subtask can be stopped. • **false**. The subtask cannot be stopped.

Attributes	Type	Description
jobCategory	String	Subtask category. This can be one of the following values. • **Backup** • **Configuration** • **Custom** • **Firmware** • **Health** • **Inventory** • **Management** • **OsDeployment** • **OsDriverUpdates** • **OsImport** • **OsProfileExport** • **Power** • **RemoteAccess** • **SelfMaintenance** • **Service** • **SwitchConfiguration** • **SystemID** • **Unknown**
jobCategoryKey	String	Subtask category key. This can be one of the following values. • **Backup** • **Configuration** • **Custom** • **Firmware** • **Health** • **Inventory** • **Management** • **OsDeployment** • **OsDriverUpdates** • **OsImport** • **OsProfileExport** • **Power** • **RemoteAccess** • **SelfMaintenance** • **Service** • **SwitchConfiguration** • **SystemID** • **Unknown**
jobTitle	String	
jobUID	String	Subtask UUID
noteAdd	Boolean	Identifies whether notes can be added to this subtask. This can be one of the following values: • **true**. Notes can be added to this job • **false**. Notes cannot be added to this job
percentage	Integer	Percentage complete of the subtask. This can be an integer from **0** - **100**.
start	Date	Date and time that the subtask started

Attributes	Type	Description
stateIconKey	String	Status icon. This can be one of the following values. • **BlueComplete**  • **Complete**  • **Error**  • **Investigating**  • **Running**  • **Spinning**  • **Stopped**  • **Warning** 
status	String	State of the subtask. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
stoppableString	String	Indicates whether the subtask can be stopped. This can be one of the following values. • **yes** • **no**
stoppedBy	String	User name that canceled the subtask
summary	Object	Information about the subtask summary.
severity	String	Severity of the subtask. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).

Attributes	Type	Description
severityText	String	Severity of the job. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).
summaryAction	Array of objects	Information about the recovery actions
format	Array of strings	
text	String	Recovery actions to resolve the subtask
summaryDescription	String	Short descriptions of the subtask
target	String	Name of the group or device that is the target for the subtask or “Not Available”
targetUUID	String	UUID of the group or device that is the target for the subtask
translatedStatus	String	Translated state of the subtask. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **Cancelled With Error** • **Cancelled With Warning** • **Cancelling** • **Complete** • **Complete With Errors** • **Complete With Warning** • **Expired** • **Initializing** • **Interrupted** • **Interrupted With Error** • **Interrupted With Warning** • **Investigating** • **Pending** • **Resolved** • **Running** • **Running With Error** • **Running With Warning** • **Skipped** • **Stop** • **Stopped With Error** • **Stopped With Warning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
complete	String	Date and time that the subtask was completed
create	String	Date and time that the subtask was created
createdBy	String	User name that created the subtask
filterStatusKey	String	This can be one of the following values. • **Complete** • **Error**

Attributes	Type	Description
hasNotes	Boolean	Indicates whether the job has notes. This can be one of the following values. • **true**. The job has notes. • **false**. The job does not have notes.
hasNotesString	String	Indicates whether the job has notes. This can be one of the following values. • **yes**. The job has notes. • **no**. The job does not have notes.
hidden	Boolean	Indicates whether the alert is hidden in the web interface. This can be one of the following values. • **true**. The alert is not displayed in the web interface. • **false**. (default) The alert is displayed in the web interface.
isDeletable	Boolean	Indicates whether the subtask can be deleted. This can be one of the following values. • **true**. The subtask can be deleted. • **false**. The subtask cannot be deleted.
isStoppable	Boolean	Indicates whether the subtask can be stopped. This can be one of the following values. • **true**. The subtask can be stopped. • **false**. The subtask cannot be stopped.
jobCategory	String	Subtask category. This can be one of the following values. • **Backup** • **Configuration** • **Custom** • **Firmware** • **Health** • **Inventory** • **Management** • **OsDeployment** • **OsDriverUpdates** • **OsImport** • **OsProfileExport** • **Power** • **RemoteAccess** • **SelfMaintenance** • **Service** • **SwitchConfiguration** • **SystemID** • **Unknown**

Attributes	Type	Description
jobCategoryKey	String	Subtask category key. This can be one of the following values. • **Backup** • **Configuration** • **Custom** • **Firmware** • **Health** • **Inventory** • **Management** • **OsDeployment** • **OsDriverUpdates** • **OsImport** • **OsProfileExport** • **Power** • **RemoteAccess** • **SelfMaintenance** • **Service** • **SwitchConfiguration** • **SystemID** • **Unknown**
jobTitle	String	
jobUID	String	Subtask UUID
noteAdd	Boolean	Identifies whether notes can be added to this job. This can be one of the following values. • **true**. Notes can be added to this job • **false**. Notes cannot be added to this job
percentage	Integer	Percentage complete of the subtask. This can be an integer from **0 - 100**.
scheduleId	String	(Scheduled jobs only) ID of the schedule that started the job
scheduleType	String	(Scheduled jobs only) Type of schedule. This can be one of the following values. • **ONE_TIME**. The job runs one time on all target devices. If the specified start and end date are in the past, the job runs imminently. • **RECURRING**. The job runs on the specified dates and times on all target devices. • **EVENT_TRIGGERED**. The job runs when a specified event occurs. This job runs only on the device that generated the event.
start	String	Date and time that the subtask started
stateIconKey	Date	Status icon. This can be one of the following values. • **BlueComplete**  • **Complete**  • **Error**  • **Investigating**  • **Running**  • **Spinning**  • **Stopped**  • **Warning** 

Attributes	Type	Description
status	String	State of the job. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
stoppableString	String	Indicates whether this job can be stopped. This can be one of the following values. • **yes** • **no**
stoppedBy	String	User name that canceled the job
summary	Object	Information about the job summary
severity	String	Severity of the job. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).
severityText	String	Severity of the job. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).
summaryAction	Array of objects	Information about the recovery actions
format	Array of strings	

Attributes	Type	Description
text	String	Recovery actions to resolve the job
summaryDescription	String	Short descriptions of the job
target	String	Name of the group or device that is the target for the subtask or “Not Available”
targetUUID	String	UUID of the group or device that is the target for the subtask
translatedStatus	String	Translated job status. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **Cancelled With Error** • **Cancelled With Warning** • **Cancelling** • **Complete** • **Complete With Errors** • **Complete With Warning** • **Expired** • **Initializing** • **Interrupted** • **Interrupted With Error** • **Interrupted With Warning** • **Investigating** • **Pending** • **Resolved** • **Running** • **Running With Error** • **Running With Warning** • **Skipped** • **Stop** • **Stopped With Error** • **Stopped With Warning** • **Unknown** • **Uploading** • **Validating** • **Waiting**

The following example is returned if the request is successful.


```
[{
    "children": [{
        "children": [],
        "complete": "2019-02-26T16:52:55Z",
        "create": "2019-02-26T16:52:54Z",
        "createdBy": "ADMIN",
        "filterStatusKey": "Complete",
        "hidden": false,
        "isDeletable": true,
        "isStoppable": false,
        "jobCategory": "Management",
        "jobCategoryKey": "Management",
        "jobTitle": "Verifying network connectivity.",
        "jobUID": "18",
        "noteAdd": true,
        "percentage": 100,
        "start": "2019-02-26T16:52:55Z",
        "stateIconKey": "Complete",
        "status": "Complete",
        "stoppableString": "No",
```

```
    "stoppedBy": "",
    "summary": null,
    "target": "Not Available",
    "targetUUID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "translatedStatus": "Complete"
},
...,
{
    "children": [],
    "complete": "2019-02-26T16:52:58Z",
    "create": "2019-02-26T16:52:54Z",
    "createdBy": "ADMIN",
    "filterStatusKey": "Complete",
    "hidden": false,
    "isDeletable": true,
    "isStoppable": false,
    "jobCategory": "Management",
    "jobCategoryKey": "Management",
    "jobTitle": "UnManaging the server is complete",
    "jobUID": "11",
    "noteAdd": true,
    "percentage": 100,
    "start": "2019-02-26T16:52:57Z",
    "stateIconKey": "Complete",
    "status": "Complete",
    "stoppableString": "No",
    "stoppedBy": "",
    "summary": null,
    "target": "Not Available",
    "targetUUID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "translatedStatus": "Complete"
}],
"complete": "2019-02-26T16:52:58Z",
"create": "2019-02-26T16:52:54Z",
"createdBy": "ADMIN",
"filterStatusKey": "Complete",
"hasNotes": false,
"hasNotesString": "No",
"hidden": false,
"isDeletable": true,
"isStoppable": false,
"jobCategory": "Management",
"jobCategoryKey": "Management",
"jobTitle": "Unmanage job for 169.254.1.23",
"jobUID": "10",
"noteAdd": true,
"percentage": 100,
"start": "2019-02-26T16:52:55Z",
"stateIconKey": "Complete",
"status": "Complete",
"stoppableString": "No",
"stoppedBy": "",
"summary": {
    "severity": "Informational",
    "severityText": "Informational",
    "summaryAction": [{
        "format": [],
        "text": ""
    }],
    "summaryDescription": "The request to unmanage the server was successful."
},
```

```
    "target": "Not Available",
    "targetUUID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "translatedStatus": "Complete"
}]
```

PUT /tasks

Use this method to cancel one or more jobs (tasks).

Note: Deleting one or more task using this API is no longer supported. Use DELETE /tasks/*{job_list}* instead.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/tasks`

Query parameters

None

Request body

Table 102. Cancel one or more jobs

Attributes	Required / Optional	Type	Description
action	Required	String	Action to take. This can be the following value. • **cancel**. Cancels the specified jobs.
list	Required	Array of strings	One or more job IDs

The following example cancels a single job.

```
{
   "action": "cancel",
   "list": ["83"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.

Code	Description	Comments
412	Precondition failed	Specified data is invalid because of missing values. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/tasks/*{job_list}*

Use this REST API to retrieve information about all jobs (tasks) and its subtasks or to retrieve information about, cancel, or delete one or more specific jobs.

HTTP methods

GET, PUT, DELETE

GET /tasks/*{job_list}*

Use this method to return information about one or more jobs (tasks) and their subtasks.

For message-description and user-action text in the job summary, you can specify the text directly in the request body if no translations are needed, or you can reference the text from a translated bundle file (for example, `com.lenovo.lxca.server.jobs.bundle.jobsSummary`).

When the job description and recovery actions require formatted text, you must specify the text as an array of objects in JSON format. You cannot use HTML.

Tip: In the translated bundle files, braces {} must be escaped by a single quote for help text (for example, `'{'`).

Attribute	Required / Optional	Type	Description
format	Required	Array of strings	List of formats for the text. This can be one of the following values. • **bold**. Corresponds to the <b> HTML tag. • **italic**. Corresponds to the <i> HTML tag. • **underline**. Corresponds to the <u> HTML tag. • **link**. Corresponds to the <a> HTML tag. • **newline**. Corresponds to the HTML tag. • **paragraph**. Corresponds to the <p> HTML tag. • **quotation**. Corresponds to the <q> HTML tag. • **orderedList**. Corresponds to the HTML tag. • **bulletList**. Corresponds to the HTML tag. • **listElement**. Corresponds to the HTML tag. If no format is needed, use an empty array.
link	Optional	String	URL to be linked to
text	Required	String or array of strings	Text to be formatted

The following example has formatted text in the user action. It includes paragraphs, ordered list, unordered list, link, and formatted text. Note that braces {} *are not* escaped by a single quote.

```
[{
   "text": "To display the text correctly, the following steps are made.",
   "format": []
},
{
   "text": [],
   "format": ["newline"]
},
{
   "text": [{
      "text": "Segment the text into pieces between HTML tags.",
      "format": ["listElement"]
   },
   {
      "text": [{
         "text": "If the segmented text contains ",
         "format": []
      },
      {
         "text": "multiple tags",
         "format": ["bold"]
      },
      {
         "text": ", segment them as well.",
         "format": []
      }],
      "format": ["listElement"]
   },
   {
      "text": [ {
         "text": "After having all segments, add the tags as follows:",
         "format": []
      },
      {
         "text": [{
            "text": "Add the text between the tags in the text field of JSON. If multiple tags are found,
                      text field is an array of JSON Objects.",
            "format": ["listElement"]
         },
         {
            "text": "Add the format for each text between tags.",
            "format": ["listElement"]
         }],
         "format": ["bulletList"]
      }],
      "format": ["listElement"]
   },
   {
      "text": "Make sure this is a json format.",
      "format": ["listElement", "bold", "underline"]
   }],
   "format": ["orderedList"]
},
{
   "text": [],
   "format": ["newline"]
},
{
   "text": [{
```

```
      "text": "This is how a paragraph looks like with a ",
      "format": []
   },
   {
      "text": "link",
      "format": ["link"],
      "link": "https://www3.lenovo.com/"
   }],
   "format": ["paragraph"]
},
{
   "text": "This is how the result should look.",
   "format": ["paragraph", "italic"]
}]
```

This example correlates to the following HTML format

```
To display the text correctly, the following steps are made.
<br></br>
<ol>
<li>Segment the text into pieces between HTML tags.</li>
<li>If the segmented text contains <b>multiple tags</b>, segment them as well.</li>
<li>After having all segments, add the tags as follows:
<ul>
<li>Add the text between the tags in the text field of JSON. If multiple tags are found,
text field is an array of JSON Objects.</li>
<li>Add the format for each text between tags.</li>
</ul></li>
<li><b><u>Make sure this is a json format.</u></b></li>
</ol>
<br></br>
<p>This is how a paragraph looks like with a <a href="https://www3.lenovo.com/">link</a></p>
<p><i>This is how the result should look.</i></p>
```

This example correlates to the following formatted output:

To display the text correctly, the following steps are made.

1. Segment the text into pieces between HTML tags.
2. If the segmented text contains **multiple tags**, segment them as well.
3. After having all segments, add the tags as follows:
   - Add the text between the tags in the text field of JSON. If multiple tags are found, text field is an array of JSON Objects.
   - Add the format for each text between tags.
4. **Make sure this is a json format.**

This is how a paragraph looks like with a link

This is how the result should look.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/tasks/{job_list}`

where *<job_list}* is a list of one or more job IDs, separated by a comma (for example, `10,11,12`). To obtain the job IDs, use the GET /tasks method.

Specify a job ID is optional. If a job ID *is not* specified, information about all jobs and their subtasks is returned.

Query parameters

Parameters	Required / Optional	Description
includeLogs=*{boolean}*	Optional	Indicates whether to return job log. This can be one of the following values: • **true**. Returns the jobs log. • **false**. (default) Do not return the jobs log. This is the default value.
compact=*{boolean}*	Optional	Indicates whether to return information about each subtask in the job. This can be one of the following values: • **true**. Does not return information about subtasks. • **false**. (default) Returns information about subtasks.

The following example returns information about a list of jobs and their subtasks.

```
GET https://192.0.2.0 /tasks/52,69,86,103?includeChildren=true
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
children	Array of objects	Information about each subtask in the job
children	Array of objects	Information about each subtask in the subtask. The properties in this object are the same as the top-level children object.

Attributes		Type	Description
	complete	String	Date and time that the subtask was completed
	create	String	Date and time that the subtask was created
	createdBy	String	User name that created the subtask
	filterStatusKey	String	This can be one of the following values. • **Complete** • **Error**
	hasNotes	Boolean	Indicates whether the subtask has notes. This can be one of the following values. • **true**. The job has notes. • **false**. The job does not have notes.
	hasNotesString	Boolean	Indicates whether the subtask has notes. This can be one of the following values. • **yes**. The job has notes. • **no**. The job does not have notes.
	hidden	Boolean	Indicates whether the alert is hidden in the web interface. This can be one of the following values. • **true**. The alert is not displayed in the web interface. • **false**. (default) The alert is displayed in the web interface.
	isDeletable	Boolean	Indicates whether the subtask can be deleted. This can be one of the following values. • **true**. The subtask can be deleted. • **false**. The subtask cannot be deleted.
	isStoppable	Boolean	Indicates whether the subtask can be stopped. This can be one of the following values. • **true**. The subtask can be stopped. • **false**. The subtask cannot be stopped.
	jobCategory	String	Subtask category. This can be one of the following values. • **Backup** • **Configuration** • **Custom** • **Firmware** • **Health** • **Inventory** • **Management** • **OsDeployment** • **OsDriverUpdates** • **OsImport** • **OsProfileExport** • **Power** • **RemoteAccess** • **SelfMaintenance** • **Service** • **SwitchConfiguration** • **SystemID** • **Unknown**

Attributes		Type	Description
	jobCategoryKey	String	Subtask category key. This can be one of the following values. • **Backup** • **Configuration** • **Custom** • **Firmware** • **Health** • **Inventory** • **Management** • **OsDeployment** • **OsDriverUpdates** • **OsImport** • **OsProfileExport** • **Power** • **RemoteAccess** • **SelfMaintenance** • **Service** • **SwitchConfiguration** • **SystemID** • **Unknown**
	jobTitle	String	
	jobUID	String	Subtask UUID
	noteAdd	Boolean	Identifies whether notes can be added to this subtask. This can be one of the following values: • **true**. Notes can be added to this job • **false**. Notes cannot be added to this job
	percentage	Integer	Percentage complete of the subtask. This can be an integer from **0** - **100**.
	start	Date	Date and time that the subtask started
	stateIconKey	String	Status icon. This can be one of the following values. • **BlueComplete**  • **Complete**  • **Error**  • **Investigating**  • **Running**  • **Spinning**  • **Stopped**  • **Warning** 

Attributes	Type	Description
status	String	State of the subtask. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
stoppableString	String	Indicates whether the subtask can be stopped. This can be one of the following values. • **yes** • **no**
stoppedBy	String	User name that canceled the subtask
summary	Object	Information about the subtask summary.
severity	String	Severity of the subtask. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).
severityText	String	Severity of the job. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).
summaryAction	Array of objects	Information about the recovery actions
format	Array of strings	

Attributes	Type	Description
text	String	Recovery actions to resolve the subtask
summaryDescription	String	Short descriptions of the subtask
target	String	Name of the group or device that is the target for the subtask or “Not Available”
targetUUID	String	UUID of the group or device that is the target for the subtask
translatedStatus	String	Translated state of the subtask. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **Cancelled With Error** • **Cancelled With Warning** • **Cancelling** • **Complete** • **Complete With Errors** • **Complete With Warning** • **Expired** • **Initializing** • **Interrupted** • **Interrupted With Error** • **Interrupted With Warning** • **Investigating** • **Pending** • **Resolved** • **Running** • **Running With Error** • **Running With Warning** • **Skipped** • **Stop** • **Stopped With Error** • **Stopped With Warning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
complete	String	Date and time that the subtask was completed
create	String	Date and time that the subtask was created
createdBy	String	User name that created the subtask
filterStatusKey	String	This can be one of the following values. • **Complete** • **Error**
hasNotes	Boolean	Indicates whether the job has notes. This can be one of the following values. • **true**. The job has notes. • **false**. The job does not have notes.
hasNotesString	String	Indicates whether the job has notes. This can be one of the following values. • **yes**. The job has notes. • **no**. The job does not have notes.

Attributes	Type	Description
hidden	Boolean	Indicates whether the alert is hidden in the web interface. This can be one of the following values. • **true**. The alert is not displayed in the web interface. • **false**. (default) The alert is displayed in the web interface.
isDeletable	Boolean	Indicates whether the subtask can be deleted. This can be one of the following values. • **true**. The subtask can be deleted. • **false**. The subtask cannot be deleted.
isStoppable	Boolean	Indicates whether the subtask can be stopped. This can be one of the following values. • **true**. The subtask can be stopped. • **false**. The subtask cannot be stopped.
jobCategory	String	Subtask category. This can be one of the following values. • **Backup** • **Configuration** • **Custom** • **Firmware** • **Health** • **Inventory** • **Management** • **OsDeployment** • **OsDriverUpdates** • **OsImport** • **OsProfileExport** • **Power** • **RemoteAccess** • **SelfMaintenance** • **Service** • **SwitchConfiguration** • **SystemID** • **Unknown**
jobCategoryKey	String	Subtask category key. This can be one of the following values. • **Backup** • **Configuration** • **Custom** • **Firmware** • **Health** • **Inventory** • **Management** • **OsDeployment** • **OsDriverUpdates** • **OsImport** • **OsProfileExport** • **Power** • **RemoteAccess** • **SelfMaintenance** • **Service** • **SwitchConfiguration** • **SystemID** • **Unknown**
jobTitle	String	
jobUID	String	Subtask UUID

Attributes	Type	Description
noteAdd	Boolean	Identifies whether notes can be added to this job. This can be one of the following values. • **true**. Notes can be added to this job • **false**. Notes cannot be added to this job
percentage	Integer	Percentage complete of the subtask. This can be an integer from **0 - 100**.
scheduleId	String	(Scheduled jobs only) ID of the schedule that started the job
scheduleType	String	(Scheduled jobs only) Type of schedule. This can be one of the following values. • **ONE_TIME**. The job runs one time on all target devices. If the specified start and end date are in the past, the job runs imminently. • **RECURRING**. The job runs on the specified dates and times on all target devices. • **EVENT_TRIGGERED**. The job runs when a specified event occurs. This job runs only on the device that generated the event.
start	String	Date and time that the subtask started
stateIconKey	Date	Status icon. This can be one of the following values. • **BlueComplete**  • **Complete**  • **Error**  • **Investigating**  • **Running**  • **Spinning**  • **Stopped**  • **Warning** 

Attributes	Type	Description
status	String	State of the job. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
stoppableString	String	Indicates whether this job can be stopped. This can be one of the following values. • **yes** • **no**
stoppedBy	String	User name that canceled the job
summary	Object	Information about the job summary
severity	String	Severity of the job. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).
severityText	String	Severity of the job. This can be one of the following values. • **Informational**. The request started or ended successfully. • **Warning**. The request completed, but there are some problems that you must be aware of . You can decide if action is needed. • **Critical**. The request failed. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result).
summaryAction	Array of objects	Information about the recovery actions
format	Array of strings	

Attributes	Type	Description
text	String	Recovery actions to resolve the job
summaryDescription	String	Short descriptions of the job
target	String	Name of the group or device that is the target for the subtask or “Not Available”
targetUUID	String	UUID of the group or device that is the target for the subtask
translatedStatus	String	Translated job status. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **Cancelled With Error** • **Cancelled With Warning** • **Cancelling** • **Complete** • **Complete With Errors** • **Complete With Warning** • **Expired** • **Initializing** • **Interrupted** • **Interrupted With Error** • **Interrupted With Warning** • **Investigating** • **Pending** • **Resolved** • **Running** • **Running With Error** • **Running With Warning** • **Skipped** • **Stop** • **Stopped With Error** • **Stopped With Warning** • **Unknown** • **Uploading** • **Validating** • **Waiting**

The following example is returned if the request is successful.


```
[{
    "children": [{
        "children": [],
        "complete": "2019-02-26T16:52:55Z",
        "create": "2019-02-26T16:52:54Z",
        "createdBy": "ADMIN",
        "filterStatusKey": "Complete",
        "hidden": false,
        "isDeletable": true,
        "isStoppable": false,
        "jobCategory": "Management",
        "jobCategoryKey": "Management",
        "jobTitle": "Verifying network connectivity.",
        "jobUID": "18",
        "noteAdd": true,
        "percentage": 100,
        "start": "2019-02-26T16:52:55Z",
        "stateIconKey": "Complete",
        "status": "Complete",
        "stoppableString": "No",
```

```
    "stoppedBy": "",
    "summary": null,
    "target": "Not Available",
    "targetUUID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "translatedStatus": "Complete"
},
...,
{
    "children": [],
    "complete": "2019-02-26T16:52:58Z",
    "create": "2019-02-26T16:52:54Z",
    "createdBy": "ADMIN",
    "filterStatusKey": "Complete",
    "hidden": false,
    "isDeletable": true,
    "isStoppable": false,
    "jobCategory": "Management",
    "jobCategoryKey": "Management",
    "jobTitle": "UnManaging the server is complete",
    "jobUID": "11",
    "noteAdd": true,
    "percentage": 100,
    "start": "2019-02-26T16:52:57Z",
    "stateIconKey": "Complete",
    "status": "Complete",
    "stoppableString": "No",
    "stoppedBy": "",
    "summary": null,
    "target": "Not Available",
    "targetUUID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "translatedStatus": "Complete"
}],
"complete": "2019-02-26T16:52:58Z",
"create": "2019-02-26T16:52:54Z",
"createdBy": "ADMIN",
"filterStatusKey": "Complete",
"hasNotes": false,
"hasNotesString": "No",
"hidden": false,
"isDeletable": true,
"isStoppable": false,
"jobCategory": "Management",
"jobCategoryKey": "Management",
"jobTitle": "Unmanage job for 169.254.1.23",
"jobUID": "10",
"noteAdd": true,
"percentage": 100,
"start": "2019-02-26T16:52:55Z",
"stateIconKey": "Complete",
"status": "Complete",
"stoppableString": "No",
"stoppedBy": "",
"summary": {
    "severity": "Informational",
    "severityText": "Informational",
    "summaryAction": [{
        "format": [],
        "text": ""
    }],
    "summaryDescription": "The request to unmanage the server was successful."
},
```

```
    "target": "Not Available",
    "targetUUID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "translatedStatus": "Complete"
}]
```

PUT /tasks/*{job_list}*

Use this method to cancel one or more jobs (tasks).

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/tasks/{job_list}`

where *{job_list}* is a list of one or more job IDs, separated by a comma (for example, `10,11,12`). To obtain the job IDs, use the GET /tasks method.

Query parameters

None

Request body

Table 103. Add a cancel callback to a created job

Attributes	Required / Optional	Type	Description
cancelRESTBody	Required when cancel-REST-Method is PUT or POST	Object	Request body for the cancel action, specified as a JSON key-value pair (for example, "a":"b"). JSON formatted request body that is required to cancel the job, specified as a key-value pairs
cancelRESTMethod	Required	String	REST method to cancel the job. This can be one of the following values. • **GET** • **POST** • **PUT** • **DELETE**
cancelURL	Required	String	URL to cancel the job
expirationTimeOut	Required	Integer	Number of seconds after which the job expires. Use -1 for jobs that do not expire.

The following example cancels the specified jobs.

```
{
   "cancelRESTBody": {
      "DeviceList": [{
         "ServerList": [{
            "UUID": "8BFBADCC33CB11E499F740F2E9903640",
            "Components": [{
               "Fixid": "lnvgy_fw_imm2_tcoo17g-3.00_anyos_noarch",
               "Component": "IMM2 (Backup)"
            },
            {
```

```
                "Fixid": "lnvgy_fw_imm2_tcoo17g-3.00_anyos_noarch",
                "Component": "IMM2 (Primary)"
            }]
        }]
    }]
  },
  "cancelRESTMethod":"PUT",
  "cancelURL":"/updatableComponents?action=cancelApply&jobID=1",
  "expirationTimeOut": 60
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
412	Precondition failed	Specified data is invalid because of missing values. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

The following example is returned when you create a subtask without using the custom ID.

```
["152", "153"]
```

The following example is returned when you create a subtask using the custom ID.

```
[{
   "customUid": "D",
   "uid": "70"
},
...,
{
   "customUid": "C",
   "uid": "69"
}]
```

DELETE /tasks/*{job_list}*

Use this method to delete one or more jobs (tasks).

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/tasks/{job_list}`

where *{job_list}* is a list of one or more job IDs, separated by a comma (for example, `10,11,12`). To obtain the job IDs, use the GET /tasks method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
413	Request Entity Too Large	Clients might impose limitations on the length of the request URI, and the request URI is too long to be handled. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/tasks/*{job_id}*/notes

Use this REST API to retrieve the note history, create a note, delete all notes, and change the job state of a specific job (task).

HTTP methods

GET, POST, DELETE

GET /tasks/*{job_id}*/notes

Use this method to return the notes history for a specific job (task).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/tasks/{job_id}/notes`

where *{job_id}* is the job ID To obtain the job IDs, use GET /tasks method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
createdBy	String	Name of the user that added the note or changed the state
id	String	Note ID
jobUID	String	Job ID
newState	String	Current Job state. This can be one of the following values. • **Aborted** • **Investigating** • **Resolved**
previousState	String	Previous state of the job • **Aborted** • **CancelledWithErrors** • **CompleteWithErrors** • **InterruptedWithError** • **Investigating** • **Resolved** • **StoppedWithError**
text	String	Note text
timeStamp	String	Timestamp when the note was entered or the state was changed
translatedNewState	String	Translated current state
translatedPrevState	String	Translated previous state

The following example is returned if the request is successful.

```
[{
   "createdBy": "USERID",
   "id": "1",
   "jobUID": "4778",
```

```
   "newState": "Working",
   "previousState": "StoppedWithError",
   "text": " Investigating the problem.",
   "timeStamp": "2017-12-14T12:00:56Z",
   "translatedNewState": "Working",
   "translatedPrevState": "StoppedWithError"
}
{
   "createdBy": "USERID",
   "id": "2",
   "jobUID": "4778",
   "newState": "Resolved",
   "previousState": " Working",
   "text": "The issue was fixed.",
   "timeStamp": "2017-12-14T12:59:56Z",
   "translatedNewState": "Resolved",
   "translatedPrevState": "Working"
}]
```

POST /tasks/*{job_id}*/notes

Use this method to create a note and change the state of a specific job (task).

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/tasks/{job_id}/notes`

where *{job_id}* is the job ID To obtain the job IDs, use GET /tasks method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
newState	Required if **text** is not specified; otherwise, optional.	Strings	Job state. This can be one of the following values: • **Aborted** • **Investigating** • **Resolved**
text	Required if **newState** is not specified; otherwise, optional.	Strings	Note text

The following example creates a note.

```
{
   "newState": "Working",
   "text": "Investigating the problem."
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /tasks/*{job_id}*/notes

Use this method to delete all notes for a specific job (task).

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/tasks/{job_id}/notes`

where *{job_id}*is the job ID To obtain the job IDs, use GET /tasks method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/tasks/locks

Use this REST API to retrieve information about job (task) locks for all managed devices. *Job locks* are a mechanism for checking whether a resource is being occupied by a job. Use this API if you are performing an operation against a device, and you do not want other operations to use the same device while you are using it.

HTTP methods

GET

GET /tasks/locks

Use this method to return information about all job (task) locks for all managed devices.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/tasks/locks`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response body is an array of one or more JSON objects with the following attributes. Each object represents a specific device. Each device can also contain a JSON array of jobs that have a lock on that device.

If a device has been locked by a previous operation, but does not currently possess any locks, it will show an empty JSON array of jobs. If a device has not yet been locked by a job, the device will not show up in the list.

Attributes	Type	Description
jobs	Array of objects	Information about each job lock
id	Integer	Job ID of each job that has a lock on the device
uuid	String	UUID of the device that has been locked by a job

The following example is returned if the request is successful.

```
[{
   "jobs": [
      {"id": 3},
      {"id":7},
      {"id": 12}
   ],
   "uuid": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
},
...,
{
   "jobs": [
      {"id": 3},
      {"id": 5},
      {"id": 34}
   ],
   "uuid": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
}]
```

/tasks/schedules

Use this REST API to retrieve information about scheduled jobs (tasks) or create a scheduled job.

HTTP methods

GET, POST

GET /tasks/schedules

Use this method to return information about all scheduled jobs.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/tasks/schedules`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
componentIDs	Array of strings	List of UUIDs of the devices or resource groups that are the target for the action. To obtain the device and resource group IDs, use GET /chassis, GET /nodes, GET /storage, GET /switches, and GET /resourceGroups.
createdBy	String	User name that created the scheduled job
creationDate	String	Timestamp when the scheduled job was created
description	String	Description of the scheduled job
execDate	String	Timestamp when the scheduled job is to run next.
id	String	ID of the scheduled job
jobIDs	Array of strings	List of IDs for all jobs that were started from the schedule
lastExecDate	String	Timestamp when the scheduled job was last run
matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	Name of the scheduled job
nextExecDate	String	Timestamp for the next scheduled run time of the job
state	String	State of the scheduled job. This can be one of the following values: • **ACTIVE** • **ENDED** • **PAUSED**
targets	String	Device or resource group name that is the target for the job. If not application, the value is **NONE**. If more there is more than one target, the value is **Multiple Targets**.

Attributes	Type	Description
triggerAction	Object	Information about the action that you want to schedule.
actionBundleKey	String	The bundle in which the user action is declared
actionBundleTitle	String	The bundle in which the translated user action is located
actionID	String	ID of the action to be performed. To obtain the action IDs, use GET /tasks/schedules/actions.
actionType	String	Type of action to be performed. This can be one of the following value: • **CUSTOM_REST** • **REST**
restBody	String	REST request body for the action to be run.
restHeaders	Array of objects	REST request header for the action to be run.
headerKey	String	
headerValue	String	
restMethod	String	REST method of the action to be run. This can be one of the following values: • **GET** • **PUT** • **POST** • **DELETE**
restURL	String	REST URL of the job to be run.
type	String	Type of schedule. This can be one of the following values. • **ONE_TIME**. The job runs one time on all target devices. If the specified start and end date are in the past, the job runs imminently. • **RECURRING**. The job runs on the specified dates and times on all target devices. • **EVENT_TRIGGERED**. The job runs when a specified event occurs. This job runs only on the device that generated the event.

The following example is returned if the request is successful.


```
[{
    "componentIDs": [
        "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
        "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB",
        "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"],
    "createdBy": "ADMIN",
    "creationDate": "2017-10-26T15:14:44Z",
    "description": "",
    "execDate": "2017-10-26T04:00:00Z",
    "id": "1509030884611",
    "jobIDs": [],
    "lastExecDate": "2017-10-26T15:15:13Z",
    "matchEverything": false,
    "name": "Power off",
    "nextExecDate": "Not Available",
    "state": "ENDED"
    "targets": " Multiple Targets",
    "triggerAction": {
        "bundleTitle": "com.lenovo.lxca.discovery.bundle.jobs.jobActions",
        "bundleKey": "PowerOff1",
```

```
        "id": "PowerOff001",
        "restBody": "{}",
        "restHeaders": [],
        "restMethod": "PUT",
        "restURL": "/manage/power",
        "type": "REST"
    },
    "type": "ONE_TIME"
}]
```

POST /tasks/schedules

Use this method to create a scheduled job (task).

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/tasks/schedules`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
action	Optional	String	Action to take. This can be one of the following values. • **CREATE** (default) Creates a scheduled job that can be run now. • **CLONE**. Creates a copy of a scheduled job. • **POSTPONE**. Creates a scheduled job that can be run later. If you specify this value, you must also specify the **triggerActions** attribute.
componentIDs	Required	Array of strings	List of UUIDs of the devices or resource groups that are the target for the action. To obtain the device and resource group IDs, use GET /chassis, GET /nodes, GET /storage, GET /switches, and GET /resourceGroups.
execDate	Required when schedule **type** is ONE_TIME	String	Timestamp when the scheduled job is to run next.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Required	String	Name of the scheduled job

Attributes	Re-quired / Optional	Type	Description
rule	Required when schedule **type** is RECUR-RING	Object	Information about the scheduling rules
dayOfWeek	Required when rule **type** is weekly or monthly, or yearly	String	Day of each week when the job is to run. This can be one of the following values. • **monday** • **tuesday** • **wednesday** • **thursday** • **friday** • **saturday** • **sunday**
days	Required when rule **type** is daily	Array of strings	Days when the job is to run. This can be one or more of the following values. • **monday** • **tuesday** • **wednesday** • **thursday** • **friday** • **saturday** • **sunday**
endDate	Required when **noEnd** is false	String	Date and time when the job stops running
monthOfYear	Required when rule **type** is yearly	String	Month of each year when the job is to run. This can be one of the following values. • **january** • **february** • **march** • **april** • **june** • **july** • **august** • **september** • **october** • **november** • **december**
noEnd	Optional	Boolean	Indicates whether the schedule has no end date. This can be one of the following values. • **true**. The schedule has no end date. • **false**. (default) The schedule has an end date.
recurEvery	Optional when rule **type** is weekly, monthly, or yearly	Integer	Interval for running the job (for example, specify 2 for every two weeks) The default is 1.

Attributes	Re-quired / Optional	Type	Description
startDate	Required	String	Date and time when the job starts running
timeZone	Required	String	Time zone for the schedule (for example, GMT-0)
type	Required	String	Type of recurring schedule. This can be one of the following values. • **daily** • **weekly** • **monthly** • **yearly**
weekOfMonth	Required when rule **type** is monthly or yearly	Integer	Week of each month when the job is to run. This can be one of the following values. • **1** • **2** • **3** • **4** • **5**
eventFilter	Required when schedule **type** is EVENT_TRIG-GERED	Object	Information about the events that trigger the job to run
eventID	Optional	String	List of IDs, separated by a comma, for events that trigger the job to run
eventService	Optional	Array of strings	Service type. This can be one or both of the following values. • **support** • **user** •
eventClass	Optional	Array of objects	Information about the event class - severity mapping.
name	Required	String	Name of the event class. This can be one of the following values. • **unknown** • **audit** • **cooling** • **power** • **disks** • **memory** • **processor** • **rackserver** • **test** • **adapter_card** • **expansion_board** • **flexswitch** • **computenode** • **rackswitch**

Attributes	Required / Optional	Type	Description
severities	Required	Array of strings	List of severities that trigger the job to run. This can be one or more of the following values. • **Unknown**. Unknown severity. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
scope	Required when schedule **type** is EVENT_TRIGGERED	Object	Date interval on which the event triggered scheduler will be active
startDate	Required	String	Date and time when the schedule starts, in the GMT-0 time zone
endDate	Required if **noEnd** is true	String	Date and time when the schedule ends, in the GMT-0 time zone
noEnd	Optional	Boolean	Indicates whether the schedule has no end date. This can be one of the following values. • **true**. The schedule has no end date. • **false**. (default) The schedule has an end date.
triggerAction	Required	Object	Information about the action to run on the target devices • You can run a predefined action by specifying the **id** attribute. • You can create a custom action based on a REST API by specifying the **options**, **restBody**, **restMethod**, **restURL**, and **type** attributes.
id	Required if **options**, **restBody**, **restMethod**, **restURL**, and **type** are not specified	String	ID of the action to run To obtain the action IDs, use GET /tasks/schedules/actions.

Attributes	Re-quired / Optional	Type	Description
options	Required if **id** is not specified	String	Schedule type. This can be one of the following values. • **ONE_TIME**. The action runs one time on all target devices. If the specified start and end date are in the past, the job runs imminently. • **RECURRING**. The job runs on the specified dates and times on all target devices.
restBody	Required if **id** is not specified	Object	Response body of the REST API
{response_body}	Required	*varies*	List of attributes in the response body of the specified REST API
restMethod	Required if **id** is not specified	String	Method of the REST API. This can be one of the following values. • **GET** • **POST** • **PUT** • **DELETE**
restURL	Required if **id** is not specified	String	URL of the REST API
type	Required if **id** is not specified	String	Action type. This value is always “CUSTOM_REST”.
type	Required	String	Type of schedule. This can be one of the following values. • **ONE_TIME**. The job runs one time on all target devices. If the specified start and end date are in the past, the job runs imminently. • **RECURRING**. The job runs on the specified dates and times on all target devices. • **EVENT_TRIGGERED**. The job runs when a specified event occurs. This job runs only on the device that generated the event.

The following example create a schedule to collect service data one time.

```
{
   "componentIDs" : ["784A050844A0E5119A9E008CFAE82560"],
   "execDate" : "2017-09-19T12:22:00.000Z",
   "matchEverything": false,
   "name": "CollectServiceData - One-time",
   "triggerAction": {
      "id": "ServiceDataCollect",
   },
   "type": "ONE_TIME"
}
```

The following example create a schedule to collect service data daily.

```
{
   "componentIDs": ["784A050844A0E5119A9E008CFAE82560"],
   "matchEverything": false,
```

```
   "name": "CollectServiceData - Daily",
   "rule": {
      "days": ["monday","wednesday"],
      "endDate": "2017-10-27 18:39:00"
      "startDate": "2017-10-18 18:39:00",
      "timeZone": "Europe/Bucharest",
      "type": "daily"
   },
   "triggerAction": {
      "id": "ServiceDataCollect",
   },
   "type": "RECURRING"
}
```

The following example create a schedule to backup the management server every other week.

```
{
   "action": "postpone"
   "name": "BackupCreation",
   "rule": {
      "dayOfWeek": "monday",
      "noEnd": true,
      "recurEvery": 2,
      "startDate": "2020-06-17 10:30:00",
      "timeZone": "America/New_York",
      "type": "weekly"
   },
   "triggerAction": {
      "restMethod": "POST",
      "restURL": "/managementServer/data",
      "restBody": {
         "action": "start",
         "includeOS": false,
         "includeFW": false,
         "label": "test",
         "operation": "backup",
         "passphrase": "CME44lenovo",
         "remoteShareDestination": ""
      },
      "options": ["ONE_TIME","RECURRING"],
      "type": "CUSTOM_REST"
   },
   "type": "RECURRING",
}
```

The following example create a schedule to collect service data monthly.

```
{
   "componentIDs": ["784A050844A0E5119A9E008CFAE82560"],
   "matchEverything": false,
   "name": "CollectServiceData - Monthly",
   "rule": {
      "dayOfWeek": "monday",
      "endDate": "2017-10-27 18:39:00",
      "recurEvery": 1,
      "startDate": "2017-10-18 18:39:00",
      "timeZone": "Europe/Bucharest",
      "type": "monthly",
      "weekOfMonth": 1
   },
   "triggerAction": {
      "id": "ServiceDataCollect",
   },
```

```
   "type": "RECURRING"
}
```

The following example create a schedule to collect service data yearly.

```
{
   "componentIDs": ["784A050844A0E5119A9E008CFAE82560"],
   "matchEverything": false,
   "name": "CollectServiceData - Yearly",
   "rule": {
      "endDate": "2017-10-27 18:39:00",
      "dayOfWeek": "monday",
      "monthOfYear": "january",
      "recurEvery": 1,
      "startDate": "2017-10-18 18:39:00",
      "timeZone": "Europe/Bucharest",
      "type": "yearly",
      "weekOfMonth": 1
   },
   "triggerAction": {
      "id": "ServiceDataCollect",
   },
   "type": "RECURRING"
}
```

The following example create a schedule to collect service data for a device when a specific event occurs.

```
{
   "componentIDs": ["72075DA6ADAC11E5868702E0EC2EC4F3"],
   "eventFilter": {
      "eventID": "0001D600"
   },
   "matchEverything": false,
   "name": "Collect device service data - Event-triggered",
   "scope": {
      "endDate": "2017-11-02T22:00:00.000Z",
      "noEnd": false
      "startDate": "2017-10-17T21:00:00.000Z",
   },
   "type": "EVENT_TRIGGERED",
      "id": "FfdcCollect1"
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
scheduleId	String	ID of the job schedule

The following example is returned if the request is successful.

```
{
   "scheduleId": "1505827038623"
}
```

/tasks/schedules/*{job_id}*

Use this REST API to retrieve information about or modify a specific scheduled job (task) or delete one or more scheduled jobs.

HTTP methods

GET, PUT, DELETE

GET /tasks/schedules*{job_id}*

Use this method to return information about a specific scheduled job.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/tasks/schedules{job_id}`

where *{job_id}* is the ID of the scheduled job. To obtain the scheduled job IDs, use GET /tasks/schedules.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.

Code	Description	Comments
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
componentIDs	Array of strings	List of UUIDs of the devices or resource groups that are the target for the action. To obtain the device and resource group IDs, use GET /chassis, GET /nodes, GET /storage, GET /switches, and GET /resourceGroups.
createdBy	String	User name that created the scheduled job
creationDate	String	Timestamp when the scheduled job was created
description	String	Description of the scheduled job
execDate	String	Timestamp when the scheduled job is to run next.
id	String	ID of the scheduled job
jobIDs	Array of strings	List of IDs for all jobs that were started from the schedule
lastExecDate	String	Timestamp when the scheduled job was last run
matchEverything	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	String	Name of the scheduled job
nextExecDate	String	Timestamp for the next scheduled run time of the job
state	String	State of the scheduled job. This can be one of the following values: • **ACTIVE** • **ENDED** • **PAUSED**
targets	String	Device or resource group name that is the target for the job. If not application, the value is **NONE**. If more there is more than one target, the value is **Multiple Targets**.
triggerAction	Object	Information about the action that you want to schedule.
actionBundleKey	String	The bundle in which the user action is declared
actionBundleTitle	String	The bundle in which the translated user action is located
actionID	String	ID of the action to be performed. To obtain the action IDs, use GET /tasks/schedules/actions.

Attributes	Type	Description
actionType	String	Type of action to be performed. This can be one of the following value: • **CUSTOM_REST** • **REST**
restBody	String	REST request body for the action to be run.
restHeaders	Array of objects	REST request header for the action to be run.
headerKey	String	
headerValue	String	
restMethod	String	REST method of the action to be run. This can be one of the following values: • **GET** • **PUT** • **POST** • **DELETE**
restURL	String	REST URL of the job to be run.
type	String	Type of schedule. This can be one of the following values. • **ONE_TIME**. The job runs one time on all target devices. If the specified start and end date are in the past, the job runs imminently. • **RECURRING**. The job runs on the specified dates and times on all target devices. • **EVENT_TRIGGERED**. The job runs when a specified event occurs. This job runs only on the device that generated the event.

The following example is returned if the request is successful.


```
{
    "componentIDs": [
        "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
        "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB",
        "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"],
    "createdBy": "ADMIN",
    "creationDate": "2017-10-26T15:14:44Z",
    "description": "",
    "execDate": "2017-10-26T04:00:00Z",
    "id": "1509030884611",
    "jobIDs": [],
    "lastExecDate": "2017-10-26T15:15:13Z",
    "matchEverything": false,
    "name": "Power off",
    "nextExecDate": "Not Available",
    "state": "ENDED"
    "targets": " Multiple Targets",
    "triggerAction": {
        "bundleTitle": "com.lenovo.lxca.discovery.bundle.jobs.jobActions",
        "bundleKey": "PowerOff1",
        "id": "PowerOff001",
        "restBody": "{}",
        "restHeaders": [],
        "restMethod": "PUT",
        "restURL": "/manage/power",
        "type": "REST"
    },
    "type": "ONE_TIME"
```

}

PUT /tasks/schedules/*{job_id}*

Use this method to modify a scheduled job (task).

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/tasks/schedules/{job_id}`

where *{job_id}* is the ID of the scheduled job. To obtain the scheduled job IDs, use GET /tasks/schedules.

Query parameters

None

Request body

Table 104. Disabling, enabling, or running a scheduled job

Attributes	Required / Optional	Type	Description
action	Required	String	The action to take. This can be one of the following values: • **PAUSE**. Disables the scheduled job. The job will not run at the next scheduled time. • **PLAY**. Enables the job to run at the next scheduled time. • **RUN**. Runs the job immediately.

The following example enables a schedule job.

```
{
   "action ": "PLAY"
}
```

Table 105. Modifying a scheduled job

Attributes	Required / Optional	Type	Description
action	Optional	String	The action to take. This can be one of the following values. • **EDIT** (default) Creates a scheduled job that can be run now.
componentUUIDs	Optional	Array of strings	List of UUIDs of the devices or resource groups that are the target for the action. To obtain the device and resource group IDs, use GET /chassis, GET /nodes, GET /storage, GET /switches, and GET /resourceGroups.

Table 105. Modifying a scheduled job (continued)

Attributes	Required / Optional	Type	Description
execDate	Required when schedule **type** is changed to ONE_TIME	String	(ONE_TIME schedule types only) Timestamp when the scheduled job is to run next.
matchEverything	Optional	Boolean	Indicates whether the action is to be run against all managed devices. This can be one of the following values. • **true**. The action is to be run against all managed devices • **false**. The action is run against only the managed device that is specified by the **target** attribute.
name	Optional	String	Name of the scheduled job
rule	Required when schedule **type** is changed to RECURRING	Object	(RECURRING schedule types only) Information about the scheduling rules.
dayOfWeek	Required when rule **type** is changed to weekly or monthly, or yearly	String	Day of each week when the job is to run. This can be one of the following values. • monday • tuesday • wednesday • thursday • friday • **saturday** • **sunday**
days	Required when rule **type** is changed to daily	Array of strings	Days when the job is to run. This can be one or more of the following values. • **monday** • **tuesday** • **wednesday** • **thursday** • **friday** • **saturday** • **sunday**
endDate	Required when **noEnd** is changed to false	String	Date and time when the job stops running

Table 105. Modifying a scheduled job (continued)

Attributes	Required / Optional	Type	Description
monthOfYear	Required when rule **type** is changed to yearly	String	Month of each year when the job is to run. This can be one of the following values. • **january** • **february** • **march** • **april** • **june** • **july** • **august** • **september** • **october** • **november** • **december**
noEnd	Optional	Boolean	Specifies whether the schedule has no end date. This can be one of the following values. • **true**. The schedule has no end date. • **false**. (default) The schedule has an end date.
recurEvery	Optional when rule **type** is changed to weekly, monthly, or yearly	Integer	Interval for running the job (for example, specify 2 for every two weeks). The default is 1.
startDate	Optional	String	Date and time when the job starts running
timeZone	Optional	String	Time zone for the schedule, for example, GMT-0.
type	Optional	String	The type of recurring schedule. This can be one of the following values. • **daily** • **weekly** • **monthly** • **yearly**
weekOfMonth	Required when rule **type** is monthly or yearly	Integer	Week of each month when the job is to run. This can be one of the following values • **1** • **2** • **3** • **4** • **5**
eventFilter	Required when schedule **type** is changed to EVENT_TRIG-GERED	Object	(EVENT_TRIGGERED schedule types only) Information about the events that trigger the job to run

Table 105. Modifying a scheduled job (continued)

Attributes	Required / Optional	Type	Description
eventID	Optional	String	A list of IDs, separated by a comma, for events that trigger the job to run.
eventService	Optional	Array of strings	The service type. This can be one or both of the following values. • **support** • **user**
eventClass	Optional	Array of objects	Information about the event class - severity mapping.
name	Optional	String	The name of the event class. This can be one of the following values. • **unknown** • **audit** • **cooling** • **power** • **disks** • **memory** • **processor** • **rackserver** • **test** • **adapter_card** • **expansion_board** • **flexswitch** • **computenode** • **rackswitch**
severities	Optional	Array of strings	List of severities that trigger the job to run. This can be one or more of the following values: • **Unknown**. Unknown severity. • **Informational**. Informational • **Warning**. User can decide if action is needed. • **Minor**. Action is needed, but the situation is not serious at this time. • **Major**. Action is needed now. • **Critical**. Action is needed now and the scope is broad (perhaps an imminent outage to a critical resource will result). • **Fatal**. A non-recoverable error has occurred.
scope	Required when schedule **type** is changed to EVENT_TRIG-GERED	Object	(EVENT_TRIGGERED schedule types only) A date interval on which the event triggered scheduler will be active.
startDate	Optional	String	Date and time when the schedule starts, in the GMT-0 time zone.

Table 105. Modifying a scheduled job (continued)

Attributes	Re-quired / Optional	Type	Description
endDate	Required if **noEnd** is changed to true	String	Date and time when the schedule ends, in the GMT-0 time zone.
noEnd	Optional	Boolean	Specifies whether the schedule has no end date. This can be one of the following values. • **true**. The schedule has no end date. • **false**. (default) The schedule has an end date.
triggerAction	Required	Object	Information about the action to run on the target devices.
id	Required	String	ID of the action to run. To obtain the action IDs, use GET /tasks/schedules/actions.
type	Required	String	Type of schedule. This can be one of the following values. • **ONE_TIME**. The job runs one time on all target devices. If the specified start and end date are in the past, the job runs imminently. • **RECURRING**. The job runs on the specified dates and times on all target devices. • **EVENT_TRIGGERED**. The job runs when a specified event occurs. This job runs only on the device that generated the event.

The following example modifies the specified schedule to run on a daily basis.

```
{
   "componentIDs": ["784A050844A0E5119A9E008CFAE82560"],
   "matchEverything": false,
   "name": "Daily schedule",
   "rule": {
      "days": ["monday","wednesday"],
      "endDate": "2017-10-27 18:39:00"
      "startDate": "2017-10-18 18:39:00",
      "timeZone": "Europe/Bucharest",
      "type": "daily"
   },
   "triggerAction": {
      "id": "ServiceDataCollect",
   },
   "type": "RECURRING"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /tasks/schedules/*{job_list}*

Use this method to delete one or more scheduled jobs (tasks).

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/tasks/schedules/{job_list}`

where *{job_list}* is a list of one or more schedule IDs, separated by a comma (for example, `1505826124198,1505826124191`). To obtain the schedule IDs, use GET /tasks/schedules.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request. For XClarity Administrator advanced functions, ensure that you have active licenses for each managed server that supports the advanced functions.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
413	Request Entity Too Large	Clients might impose limitations on the length of the request URI, and the request URI is too long to be handled. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/tasks/schedules/actions

Use this REST API to retrieve a list of actions that can be scheduled as jobs and to register a new predefined action at the runtime.

HTTP methods

GET, POST

GET /tasks/schedules/actions

Use this method to return a list of actions that can be scheduled as jobs.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/tasks/schedules/actions`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	String	Action ID
title	String	Action name

The following example is returned if the request is successful.

```
[
   { "id": "PowerOff001",  "title": "Power OFF device" },
   { "id": "Restart001",   "title": "Restart device" },
   { "id": "PowerOn001",   "title": "Power ON device" },
   { "id": "FfdcCollect1", "title": "Collect Service Data from Device" }
]
```

POST /tasks/schedules/actions

Use this method to register a new predefined action at the runtime.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/tasks/schedules/actions`

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
bundleKey	Required	String	The bundle in which the user action is declared
bundleTitle	Required	String	The bundle in which the translated user action is located
id	Required	String	ID of the job to be performed. To obtain the action IDs, use GET /tasks/schedules/actions.
restBody	Optional	String	REST request body for the job to be run.
restHeaders	Optional	Array of objects	REST request header for the job to be run.
headerKey	Required	String	
headerValue	Required	String	
restMethod	Required	String	REST method of the job to be run. This can be one of the following values: • **GET** • **PUT** • **POST** • **DELETE**
restURL	Required	String	REST URL of the job to be run.

The following example registers a new predefined action at the runtime..

```
{
   "bundleKey": "ActionBundleKey",
   "bundleTitle": "com.lenovo.lxca.job.bundle.scheduleTest",
   "id": "actionID",
   "restBody": "{\"key1\":\"keyValue\", \"key2\":2, \"key3\":true}",
   "restHeaders": [{
      "headerKey": "aaa",
      "headerValue": "bbb"
   },
   {
      "headerKey": "ccc",
      "headerValue": "ddd"
   }],
   "restMethod": "PUT",
   "restURL": "/path/to/job"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

Chapter 13. Security

The following resources are available for performing security functions.

/certificateRevocationList

Use this REST API to download all certificate revocation lists (CRLs) or to upload a CRL. A CRL is a list of certificates that have been revoked and are no longer trusted. A certificate might be revoked if it was incorrectly issued by the CA or if its key is compromised, lost, or stolen.

HTTP methods

GET, POST

GET /certificateRevocationList

Use this method to download all certificate revocation list (CRLs).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/certificateRevocationList`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
response		Array	
	crl	String	Contents of the CRL file in PEM format
	issuerDn	String	LDAP Distinguished Name of the issuer(for example `"CN=demo server, OU=CS,O=Com Ltd.,ST=QLD,C=AU"`)
	next_update	String	Date and time for the next update. The timestamp is returned in ISO 8601 format (for example `2014-02-05T15:54:13Z`)

Attributes	Type	Description
signatureAlgorithm	String	Algorithm used to sign the CRL (for example "MD5withRSA")
type	String	CRL type (for example "X.509")
update	String	Date and time for this update. The timestamp is returned in ISO 8601 format(for example 2014-02-05T15:54:13Z).
version	Integer	CRL version
result	String	Results of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
explanation	String	Additional information to clarify the reason for the message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.


```
{
   "response": [{
      "crl": "-----BEGIN X509 CRL-----\r\n
            MIIBODCB4zANBgkqhkiG9w0BAQQFADBgMQswCQYDVQQGEwJBVTEMMAoGA1UECBMD\r\n
            UUxEMRkwFwYDVQQKExBNaW5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEbMBkG\r\n
            A1UEAxMSU1NMZWF5IGRlbW8gc2VydmVyFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQx\r\n
            NjI2NTdaMFIwEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMTAwMDBa\r\n
            MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCSqG\r\n
            SIb3DQEBBAUAA0EAHPjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/E6MYBPFVQFYo/Gp\r\n
            UZexfjSVo5CIyySOtYscz8oO7avwBxTiMpDEQg==\r\n
            -----END X509 CRL-----\r\n",
      "issuerDn": "CN=SSLeay demo server,OU=CS,O=Mincom Pty. Ltd.,ST=QLD,C=AU",
      "next_update": "2001-02-14T16:26:57Z",
      "signatureAlgorithm": "MD5withRSA",
      "type": "X.509",
      "update": "2001-01-15T16:26:57Z",
      "version": 1
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```

POST /certificateRevocationList

Use this method to upload a certificate revocation list (CRL).

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/certificateRevocationList`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
crl	Required	String	CRL contents in PEM format

The following example uploads a CRL.

```
{
   "crl":"-----BEGIN X509 CRL-----\n
          MIIDFDCCAfwCAQEwDQYJKoZIhvcNAQEFBQAwXzEjMCEGA1UEChMaU2FtcGxlIFNp\n
          Z25lciBPcmdhbml6YXRpb24xGzAZBgNVBAsTElNhbXBsZSBTaWduZXIgVW5pdDEb\n
          MBkGA1UEAxMSU2FtcGxlIFNpZ25lciBDZXJ0FwOxMzAyMTgxMDMyMDBaFwOxMzAy\n
          MTgxMDQyMDBaMIIBNjA8AgMUeUcXDTEzMDIxODEwMjIxMlowJjAKBgNVHRUEAwoB\n
          AzAYBgNVHRgEERgPMjAxMzAyMTgxMDIyMDBaMDwCAxR5SBcNMTMwMjE4MTAyMjIy\n
          WjAmMAoGA1UdFQQDCgEGMBgGA1UdGAQRGA8yMDEzMDIxODEwMjIwMFowPAIDFHlJ\n
          FwOxMzAyMTgxMDIyMzJaMCYwCgYDVR0VBAMKAQQwGAYDVR0YBBEYDzIwMTMwMjE4\n
          MTAyMjAwWjA8AgMUeUoXDTEzMDIxODEwMjIOMlowJjAKBgNVHRUEAwoBATAYBgNV\n
          HRgEERgPMjAxMzAyMTgxMDIyMDBaMDwCAxR5SxcNMTMwMjE4MTAyMjUxWjAmMAoG\n
          A1UdFQQDCgEFMBgGA1UdGAQRGA8yMDEzMDIxODEwMjIwMFqgLzAtMB8GA1UdIwQY\n
          MBaAFL4SAcyq6hGA2i6tsurHtfuf+aOOMAoGA1UdFAQDAgEDMAOGCSqGSIb3DQEB\n
          BQUAA4IBAQBCIb6B8cN5dmZbziETimiotDy+FsOvS93LeDWSkNjXTG/+bGgnrm3a\n
          QpgB7heT8L2o7s2QtjX2DaTOSYL3nZ/Ibn/R8SOg+EbNQxdk5/la6CERxiRp+E2T\n
          UG8LDb14YVMhRGKvCguSIyUGOMwGW6waqVtd6K71u7vhIU/Tidf6ZSdsTMhpPPFu\n
          PUid4j29U3q1OSGFF6cCt1DzjvUcCwHGhHAO2Men7OEgZFADPLWmLgOHglKUh1iZ\n
          WcBGtev/8VsUijyjsMO72C6Ut5TwNyrrthb952+eKlmxLNgTOo5hVYxjXhtwLQsL\n
          7QZhrypAM1DlYqQjkiDI7hlvt7QuDGTJ\n
          -----END X509 CRL-----"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```

/certificateRevocationList/*{CRL_id}*

Use this REST API to download or delete a specific certificate revocation list (CRL). A CRL is a list of certificates that have been revoked and are no longer trusted. A certificate might be revoked if it was incorrectly issued by the CA or if its key is compromised, lost, or stolen.

HTTP methods

GET, DELETE

GET /certificateRevocationList/*{CRL_id}*

Use this method to download a specific certificate revocation list (CRL).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/certificateRevocationList/{CRL_id}`

where *{CRL_id}* is the distinguished name of the CRL issuer to be retrieved. To obtain the Distinguished Name, use the GET /certificateRevocationList method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	
crl	String	Contents of the CRL file in PEM format
issuerDn	String	LDAP Distinguished Name of the issuer(for example `"CN=demo server, OU=CS,O=Com Ltd.,ST=QLD,C=AU"`)
next_update	String	Date and time for the next update. The timestamp is returned in ISO 8601 format (for example `2014-02-05T15:54:13Z`)
signatureAlgorithm	String	Algorithm used to sign the CRL (for example `"MD5withRSA"`)
type	String	CRL type (for example `"X.509"`)
update	String	Date and time for this update. The timestamp is returned in ISO 8601 format(for example `2014-02-05T15:54:13Z`).
version	Integer	CRL version
result	String	Results of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
explanation	String	Additional information to clarify the reason for the message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": [{
      "crl": "-----BEGIN X509 CRL-----\r\n
            MIIBODCB4zANBgkqhkiG9w0BAQQFADBgMQswCQYDVQQGEwJBVTEMMAoGA1UECBMD\r\n
            UUxEMRkwFwYDVQQKExBNaW5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEbMBkG\r\n
            A1UEAxMSU1NMZWF5IGRlbW8gc2VydmVyFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQx\r\n
            NjI2NTdaMFIwEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMTAwMDBa\r\n
            MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCSqG\r\n
            SIb3DQEBBAUAA0EAHPjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/E6MYBPFVQFYo/Gp\r\n
            UZexfjSVo5CIyySOtYscz8oO7avwBxTiMpDEQg==\r\n
            -----END X509 CRL-----\r\n",
      "issuerDn": "CN=SSLeay demo server,OU=CS,O=Mincom Pty. Ltd.,ST=QLD,C=AU",
      "next_update": "2001-02-14T16:26:57Z",
      "signatureAlgorithm": "MD5withRSA",
      "type": "X.509",
      "update": "2001-01-15T16:26:57Z",
      "version": 1
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```


DELETE /certificateRevocationList/*{CRL_id}*

Use this method to remove a specific certificate revocation list (CRL).

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/certificateRevocationList/{CRL_id}`

where *{CRL_id}* is the distinguished name of the CRL issuer to be deleted. To obtain the Distinguished Name, use the GET /certificateRevocationList method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "id": "FQXHMSE0001I",
        "explanation": "",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

/certificatePolicy

Use this REST API to return or modify the certificate policy type for the management server. This policy applies to all parts of the certificate, including the root CA certificate, server certificate, and CSR for externally signed certificates.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

HTTP methods

GET, PUT

GET /certificatePolicy

Use this method to return the certificate policy type for the management server. This policy applies to all parts of the certificate, including the root CA certificate, server certificate, and CSR for externally signed certificates.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/certificatePolicy`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	Information about response
specName	String	Certificate policy. This can be one of the following values. • **DEFAULT**. (default) The certificate key length is 2048 bits, and the signing algorithm is SHA256RSA (SHA256/2048). • **CNSA.** The certificate key length must be 3072 bits, and the signing algorithm is SHA384RSA (SHA384/3072).
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information

Attributes	Type	Description
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "response": {
      "specName": "CNSA"
   },
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```

PUT /certificatePolicy

Use this method to modify the certificate policy type for the management server. This policy applies to all parts of the certificate, including the root CA certificate, server certificate, and CSR for externally signed certificates.

Note: This REST API requires Lenovo XClarity Administrator v4.0.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/certificatePolicy`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
specName	Required	String	Certificate policy. This can be one of the following values. • **DEFAULT**. (default) The certificate key length is 2048 bits, and the signing algorithm is SHA256RSA (SHA256/2048). • **CNSA.** The certificate key length must be 3072 bits, and the signing algorithm is SHA384RSA (SHA384/3072).

The following example sets the certificate policy to CNSA (SHA384/3072).

```
{
   "specName": "CNSA"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```

/certificateSettings

Use this REST API to retrieve the saved certificate values from the most recent certificate creation.

HTTP methods

GET

GET /certificateSettings

Use this method to return the saved certificate values from the most recent certificate creation.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/certificateSettings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
response		Array	Information about certificate settings
	CommonName	String	Name of the certificate owner. Typically, this is the fully-qualified domain name (FQDN) or IP address of the server that is using the certificate (for example, `www.domainname.com` or `10.15.23.99`).
	Country	String	Two-letter ISO 3166 code for the country or region of origin associated with the certificate organization (for example, `US for the United States`)
	notBefore	String	UTC date and time before which the created certificate is not valid The date and time is specified in ISO 8601 format `YYYY-MM-DDTHH:MM:SSZ` (for example, 2017-01-25T18:00:00Z).
	notAfter	String	UTC date and time after which the created certificate is not valid The date and time is specified in ISO 8601 format `YYYY-MM-DDTHH:MM:SSZ` (for example, 2017-01-25T18:00:00Z).
	Organization	String	Organization (company) that will own the certificate. Typically, this is the legal incorporate name of a company. It should include any suffixes, such as Ltd., Inc., or Corp (for example, `ACME International Ltd.`).
	OrganizationUnit	String	Organizational unit that will own the certificate (for example, `ABC Division`)

Attributes	Type	Description
StateLocality	String	Full name of the locality (city) to be associated with the certificate (for example, `San Jose`)
StateProvince	String	Full name of the state or province to be associated with the certificate (for example, `California` or `New Brunswick`)
subjectAlternativeNames	Object	Information about the Subject Alternative Names (SANs) to be included in Certificate Signing Requests
generalNames	Array of objects	List of Subject Alternative Names to be included in Certificate Signing Requests
name	String	Subject Alternative Name
type	String	RFC 5280 GeneralName type of this Subject Alternative Name
possibleGeneralNameTypes	Array of strings	List of supported RFC 5280 GeneralName type strings
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed, a descriptive error message was returned.
messages	Array	Information about one or more messages
id	String	The message identifier of a returned message
explanation	String	Additional information to clarify the reason for the message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": {
      "CommonName": "Generated by Lenovo System Management Software",
      "Country": "US",
      "notBefore": "2017-06-01T12:30:00Z",
      "notAfter": "2018-06-01T12:30:00Z",
      "Organization": "Lenovo",
      "OrganizationUnit": "DCG",
      "StateLocality": "Raleigh",
      "StateProvince": "North Carolina",
      "subjectAlternativeNames": {
         "generalNames": [{
            "name": "LXCA-1",
            "type": "dNSName"
         },
         {
            "name": "192.0.2.0",
            "type": "iPAddress"
         }],
         "possibleGeneralNameTypes": ["dNSName", "iPAddress", "rfc822Name", "directoryName",
                                      "uniformResourceIdentifier", "registeredID"]
      }
   },
   "result": "success",
```

```
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```


/certificateSigningRequest

Use this REST API to generate, download , or delete a Certificate Signing Request (CSR).

HTTP methods

GET, DELETE

GET /certificateSigningRequest

Use this method to download or retrieve detailed information about a Certificate Signing Request (CSR).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/certificateSigningRequest`

Query parameters

Parameters	Required / Optional	Description
details=*{Boolean}*	Optional	Indicates whether to include message content in the response body. This can be one of the following values. • **true**. Includes message content in the response body. • **true**. (default) Excludes message content in the response body.
path=*{string}*	Required	ID value obtained from a previous POST /certificateSigningRequest request

The following example downloads only the CSR.

```
GET /certificateSigningRequest?path=1
```

The following example retrieves detailed information about the CSR.

```
GET /certificateSigningRequest?path=1&details=true
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	
CSR	String	Certificate
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful and **details=true** was not specified.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDjDCCAnQCAQAwgYoxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3JOaCBDYXJv
bGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5IFNl
cnZlciBGaXJtd2FyZTEaMBgGA1UECxMRT3JnYW5pemFOaW9uIHVuaXQxDTALBgNV
BAMTBExYQOEwggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCMwy8q5PrW
hHtLv1cOOdVJiXTHK3JNcQXicWXzL3/+vhGkgfd8rqqCvvxjTg7N2hYaFlQghEFT
EWDhMmxvMFZtAhQfBnzcdiWj23I3MSRqDWBa8NsqHWffxyqcOEqhoGiOMCjHW9zd
kSkJOfZvFJ5RTPmhY+Xnt92lZgSGwmnTcGq9dxNvV6ixMvnHzWE9+MguTxsfGMSR
ZJ4Rf+d35X9ovQHEge1jMaqOcoBuqVMK9TkWsb1O1GJ2tggDR5tp8YHws7wakp1i
sXc4AtDDIzrKfhxvxqTHqsAppREQD79srzsG+jNsOYvg7Jd7bm2/zP9gxMwVFUYO
m7DYg8HF6mZ9AgMBAAGggbswgbgGCSqGSIb3DQEJDjGBqjCBpzCBpAYDVR0RBIGc
MIGZhxD+gAAAAAAAAAoAJ//+zQ6Dgh5mZTgwOjA6MDowOmEwMDoyN2ZmOmZlY2Q6
ZTgzJTKHBArxieCCIGlwMTAtMjQxLTEzNyOyMjQubGFicy5sZW5vdm8uY29thxAA
AAAAAAAAAAAAAAAAAAABgglsb2NhbGhvc3SHBH8AAAGCCWxvY2FsaG9zdIIJbG9j
YWxob3NOggRMWENBMAOGCSqGSIb3DQEBCwUAA4IBAQACBKc6nxzo/8NBQOxuRe+w
OMNzrAg9cIyh7cFCcTbSVmamOxAauRHvVIsgE/x/xQP3tQFvfJOqYr4eyJvEqHIN
Y71ZgQjIunMVX9Oqf5MEdbYEsQE7g/2WzVXIDZ6p1qewjW85YeunHVS3fgWfD3jX
Z66BXZyEB4l7xRtOr85E6bCkhlymj3O6OLHCdmeCewT/rOaOKnR9trSBB2zSkqTP
SaxJQXB+6rKS+DGu+lSCNHYLr8cKYloLaGO8GaRZF4kedPQ1JSoz4jXOdgkPzqAX
JlOJVWPUEkKLpGUomBBBUK5PwBN1OkuB8c/wXhB9+ki3CpcolGXoBpJk+fM6ij/8
-----END CERTIFICATE REQUEST-----
```

The following example is returned if the request is successful and **details=true** was specified.


```
{
   "response": {
      "CSR": "-----BEGIN CERTIFICATE REQUEST-----\n
              MIIDjDCCAnQCAQAwgYoxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3JOaCBDYXJv\n
              bGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5IFNl\n
              cnZlciBGaXJtd2FyZTEaMBgGA1UECxMRT3JnYW5pemFOaW9uIHVuaXQxDTALBgNV\n
              BAMTBExYQOEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCDeldS5sla\n
              KMP5nxp1UyC233r2G3AOFnaAuFCmObgkCgfOuAfDmLvFva2P2/FGN5AfBw2ToLMC\n
              A7tdExvPqawg/ByFIikn5J35Uei7j12jJjLnYAoddUKu1+OVh5wv/iWEHnZAaVZl\n
              qNJbBVUGot2hl+9KCxrgphoq7uuJ9ZVVK617IkiwzQN+D5INIJRkXIQdoPxAyW53\n
              J9ohkTFWDW2JOMoqSAXNOnSKOjtnzB8JVf823pb1IcmYWOpFSK+tn9mbKIo5YtzB\n
              4ik9SO8y3yAnMRPR1YM4UwMZi2S5MIhC+rKVd47VRpYFVS53ySGqIUY2EynEztA+\n
              qucd8gS1JfItAgMBAAGggbswgbgGCSqGSIb3DQEJDjGBqjCBpzCBpAYDVR0RBIGc\n
              MIGZhxD+gAAAAAAAAAoAJ//+zQ6Dgh5mZTgwOjA6MDowOmEwMDoyN2ZmOmZlY2Q6\n
              ZTgzJTKHBArxieCCIGlwMTAtMjQxLTEzNyOyMjQubGFicy5sZW5vdm8uY29thxAA\n
              AAAAAAAAAAAAAAAAAAABgglsb2NhbGhvc3SHBH8AAAGCCWxvY2FsaG9zdIIJbG9j\n
              YWxob3NOggRMWENBMA0GCSqGSIb3DQEBCwUAA4IBAQB5FTkUlxQ8NbcoTlUNzGzg\n
              XQQM2GxfIDOxzd+ZiOQpuXEdKoTc+ehGXUCOKx5Shs2rkNAeyf5KWbWIewKOwh3v\n
              SuNK4JMFguaD1oOV21XqEBEN5OHOA759mN3HuKHnbWJCEERp2OZmZAJqJfAdNVY/\n
              n+CC+Hsaluy4aJI2fFRJ9jod/bFVKxkvsn8XangntQK9UIUGmqhUBMFTrQfqu/i9\n
              YM+8zhPJlJFL18jiqHOhMyMfDznRQQl1c9943HYJxXRFs/HWlHkpTlSovv2h4a3k\n
              F3rlvLdPsd5ym97fVO/oIDPm6e27lv9B3QfSuwk6BtCYFy3evp78/daptOOKBuf6\n
              -----END CERTIFICATE REQUEST-----\n"
   },
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```


POST /certificateSigningRequest

Use this method to generate a Certificate Signing Request (CSR).

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/certificateSigningRequest`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
CommonName	Optional	String	Name of the certificate owner. Typically, this is the fully-qualified domain name (FQDN) or IP address of the server that is using the certificate (for example, `www.domainname.com` or `10.15.23.99`) The length of this value cannot exceed 63 characters. The default is `LXCA`.
Country	Optional	String	Two-letter ISO 3166 code for the country or region of origin associated with the certificate organization (for example, `US for the United States`) The default is `US`.
Organization	Optional	String	Organization (company) that is to own the certificate. Typically, this is the legal incorporate name of a company. It should include any suffixes, such as Ltd., Inc., or Corp (for example, `ACME International Ltd.`) The length of this value cannot exceed 60 characters. The default is generated by the server firmware.
OrganizationUnit	Optional	String	Organizational unit that will own the certificate (for example, `ABC Division`) The length of this value cannot exceed 60 characters. The default is `None`.
StateLocality	Optional	String	Full name of the locality (city) to be associated with the certificate (for example, `San Jose`) The length of the value cannot exceed 50 characters. The default is `Raleigh`.
StateProvince	Optional	String	Full name of the state or province to be associated with the certificate (for example, `California` or `New Brunswick`) The length of this value cannot exceed 60 characters. The default is `North Carolina`.
subjectAlternativeNames	Optional	Object	Information about the Subject Alternative Names (SANs) to be included in Certificate Signing Requests
generalNames	Required	Array of objects	List of Subject Alternative Names to be included in Certificate Signing Requests
name	Required	String	Subject Alternative Name
type	Required	String	RFC 5280 GeneralName type of this Subject Alternative Name

The following example generates a CSR.

```
{
   "CommonName": "LXCA"
   "Country": "US",
   "Organization": "ACME International Ltd.",
   "OrganizationUnit": "ABC Division",
   "StateLocality": "Raleigh",
   "StateProvince": "North Carolina",
```

```
   "subjectAlternativeNames": {
      "generalNames": [{
         "type": "dNSName",
         "name": "New-LXCA"
      },
      {
         "type": "iPAddress",
         "name": "192.0.2.0"
      }]
   }
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	
path	String	Identifier that can used to reference the generated CSR on subsequent GET and DELETE requests
result	String	Results of the request . This can be one of the following values: • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": {
       "path": "1"
   },
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
```

```
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```

/cryptoSettings

Use this REST API to retrieve or modify the current cryptography settings on Lenovo XClarity Administrator. The *cryptographic settings* determine how secure communications are handled between Lenovo XClarity Administrator and all managed systems. It sets the encryption-key lengths to be used if secure communications are implemented.

HTTP methods

GET, PUT

GET /cryptoSettings

Use this method to return information about current cryptographic settings on Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/cryptoSettings`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Information about each cryptography setting
cipherSuite	String	**Attention:** This attribute will be deprecated in a future release. Minimum cipher suite version to use for server connections. This can be one of the following values. • **tls1.2**. TLS v1.2 or v1.3 cipher suite is required for both servers and clients. Specify `tls1.2` for the **minTlsVersionClient** and **minTlsVersionServer** attributes instead. • **tls1.2-flexcat**. TLS v1.2 compliance with exceptions for deploying operating systems from the XClarity Administrator. Specify `tls1.2` for the **minTlsVersionClient**, **minTlsVersionServer**, **minTlsVersionOsDeploy** attributes instead.

Attributes	Type	Description
minTlsVersionClient	String	Minimum TLS protocol version to use for client connections to other servers (such as the LDAP client). This can be one of the following values. • **TLS1.2**. Enforces TLS v1.2 cryptography protocols. • **TLS1.3**. Enforces TLS v1.3 cryptography protocols.
minTlsVersionOsDeploy	String	Minimum TLS protocol version to for the Lenovo XClarity Administrator operating-system deployment server. This can be one of the following values. • **TLS1.2**. Enforces TLS v1.2 cryptography protocols. • **TLS1.3**. Enforces TLS v1.3 cryptography protocols.
minTlsVersionServer	String	Minimum TLS protocol version to use for server connections (such as the web server). This can be one of the following values. • **TLS1.2**. Enforces TLS v1.2 cryptography protocols. • **TLS1.3**. Enforces TLS v1.3 cryptography protocols.
nistMode	String	Cryptographic mode of Lenovo XClarity Administrator and all managed chassis. This can be one of the following values. • **nistcomp**. NIST compatibility mode. • **nist800-131a**. NIST800-131A strict compatibility mode. When this option is selected, you must also select `tls1.2` for the **minTlsVersionClient** and **minTlsVersionServer** attributes.
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": {
      "cipherSuite": "tls1.2"
      "minTlsVersionClient": "tls1.2",
      "minTlsVersionOsDeploy": "tls1.2",
      "minTlsVersionServer": "tls1.2",
      "nistMode": "nist800-131a"
   },
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
```

```
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```

PUT /cryptoSettings

Use this method to modify the current cryptographic settings on Lenovo XClarity Administrator.

To modify the current cryptographic setting for managed devices, use PUT /nodes/cryptoSettings.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/cryptoSettings`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
applyToMgmtServer	Optional	Boolean	Indicates whether to apply the specified settings to the XClarity Administrator management server. This can be one of the following values. • **true**. (default) Applies specified settings to the management server. • **false**. Does not apply settings to the management server.
cipherSuite	Optional	String	**Attention:** This attribute will be deprecated in a future release. Minimum cipher suite version to use for server connections. This can be one of the following values. • **tls1.2**. TLS v1.2 or v1.3 cipher suite is required for both servers and clients. Specify `tls1.2` for the **minTlsVersionClient** and **minTlsVersionServer** attributes instead. • **tls1.2-flexcat**. TLS v1.2 compliance with exceptions for deploying operating systems from the XClarity Administrator. Specify `tls1.2` for the **minTlsVersionClient**, **minTlsVersionServer**, **minTlsVersionOsDeploy** attributes instead.
minTlsVersionClient	Optional	String	Minimum TLS protocol version to use for client connections to other servers (such as the LDAP client). This can be one of the following values. • **TLS1.2**. Enforces TLS v1.2 cryptography protocols. • **TLS1.3**. Enforces TLS v1.3 cryptography protocols.
minTlsVersionOsDeploy	Optional	String	Minimum TLS protocol version to for the XClarity Administrator operating-system deployment server. This can be one of the following values. • **TLS1.2**. Enforces TLS v1.2 cryptography protocols. • **TLS1.3**. Enforces TLS v1.3 cryptography protocols.

Attributes	Required / Optional	Type	Description
minTlsVersionServer	Optional	String	Minimum TLS protocol version to use for server connections (such as the web server). This can be one of the following values. • **TLS1.2**. Enforces TLS v1.2 cryptography protocols. • **TLS1.3**. Enforces TLS v1.3 cryptography protocols.
nistMode	Optional	String	Cryptographic mode of the Lenovo XClarity Administrator and all managed chassis. This can be one of the following values. • **nistcomp**. NIST compatibility mode. • **nist800-131a**. NIST800-131A strict compatibility mode. When this option is selected, you must also select `tls1.2` for the **minTlsVersionClient** and **minTlsVersionServer** attributes.
returnJobInfo	Optional	Boolean	Indicates whether job information is to be returned as a result of changing the cryptographic settings. This can be one of the following values. • **true**. Returns job information in the response body and header if a job is created. • **false**. Does not return job information. This is the default setting.

The following example applies the specified TLS and NIST settings to the management server and all managed devices.

```
{
   "applyToManagedDevices": true,
   "applyToMgmtServer": true,
   "minTlsVersionClient": "tls1.2",
   "minTlsVersionOsDeploy": "tls1.2",
   "minTlsVersionServer": "tls1.2",
   "nistMode": "nist800-131a",
   "returnJobInfo": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
201	Created	One or more new resources were successfully created.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages

Attributes	Type	Description
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned when `"returnJobInfo": true` was specified and a job was created and successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

The following example is returned when `returnJobInfo="false"` was specified and a job was created but failed.

```
{
    "result": "failure",
    "messages": [{
        "explanation": "The provided minimum SSL/TLS protocol level does not match one
                        of the expected string values. The requested operation was not
                        performed.",
        "id": "FQXHMSE0501J",
        "recovery": {
            "text": "Correct the value and try the operation again.",
            "URL": ""
        },
        "text": "The provided minimum SSL/TLS protocol level is not valid."
    }]
}
```

/encapsulationSettings

Use this REST API to retrieve information about or modify Lenovo XClarity Administrator's global encapsulation setting.

The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.

Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see Recovering chassis management with a CMM after a management server failure and Recovering rack or tower server management after a management server failure.

HTTP methods

GET, PUT

GET /encapsulationSettings

Use this method to return information about the global encapsulation setting that is used during device management.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/encapsulationSettings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
encapsulationEnabled	Boolean	Indicates whether encapsulation is enabled during device management. This can be one of the following values. • **true**. Encapsulation is enabled. When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator. **Important:** For additional considerations, see /encapsulationSettings. • **false**. Encapsulation is disabled.The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

The following example is returned if the request is successful.

```
{
   "encapsulationEnabled": true
}
```

PUT /encapsulationSettings

Use this method to change the global encapsulation setting during the device management process.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/encapsulationSettings`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
encapsulationEnabled	Required	Boolean	Indicates whether encapsulation is enabled during device management. This can be one of the following values. • **true**. Encapsulation is enabled. When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator. **Important:** For additional considerations, see /encapsulationSettings. • **false**. Encapsulation is disabled.The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

The following example enables encapsulation.

```
{
   "encapsulationEnabled":true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/endpoint/signingCertificate/*{id}*/*{resource}*

Use this REST API to retrieve a signed certificate from the chassis, rack server, or tower server containing the specified device and replace the certificate that is currently in the Lenovo XClarity Administrator trust store.

HTTP methods

GET, PUT

GET /endpoint/signingCertificate/*{uuid}*/*{resource}*

Use this method to return information about the signed Certificate Authority (CA) root certificate for a specific resource type, in PEM format.

Note: This method is not support on ThinkServer and System x M4 servers.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/endpoint/signingCertificate/{uuid}/{resource}`

where:

- *{uuid}* specifies the UUID of the target device.
- *{resource}* can be one of the following values:
  - **updatedCIMCertificate**. This resource type applies only to rack or tower server UUIDs.
  - **updatedLDAPCertificate**. This resource type applies only to rack or tower server UUIDs.
  - **updatedSigningCertificate**. This resource type applies only to chassis, storage device, and switch UUIDs.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	
CertificateOwnerUUID	String	UUID of the certificate owner.
CurrentCertificatePEM	String	PEM representation of the certificate.
CurrentCertificateText	Array	
CertIssuer	String	Certificate user (for example, `"L=Austin,ST=TX,C=US,O=Generated by Lenovo Firmware, CN=CA for A4AFBBC4-7702-3204-9A45-C6F315D66236\\, 15-03-10 10:49:01"`)
CertKeyFields	Array	

Attributes	Type	Description
CertKeyFieldName	String	Identification of a component of the certificate key (for example, "Modulus" or "Exponent")
CertKeyFieldValue	String	Corresponds to the Key Field Name
CertPublicKeyAlgorithm	String	Public key algorithm (for example, "RSA")
CertPublicKeyLength	String	Length in bytes of the public key (for example, 2048)
CertSerialNumber	String	Certificate serial number
CertSignature	String	Digital signature of the device's signing certificate
CertSignatureAlgorithm	String	Algorithm used when signing the certificate (for example, "SHA1withRSA")
CertSubject	String	Contains the certificate subject (for example, "L=Austin,ST=TX,C=US,O=Generated by Lenovo Firmware, CN=CA for A4AFBBC4-7702-3204-9A45-C6F315D66236\\, 15-03-10 10:49:01")
CertValidNotBefore	String	Date before which the certificate is not valid. The timestamp is returned in ISO 8601 format (for example, "1970-01-01T00:00:00Z")
CertValidNotAfter	String	Date after which the certificate is not valid. The timestamp is returned in ISO 8601 format (for example, "2048-12-31T23:59:59Z")
CertX509Version	String	Version of the X.509 certificate standard (for example, 3)
TrustedCertificateText		
CertIssuer	String	Certificate user (for example, "L=Austin,ST=TX,C=US,O=Generated by Lenovo Firmware, CN=CA for A4AFBBC4-7702-3204-9A45-C6F315D66236\\, 15-03-10 10:49:01")
CertKeyFields	Array of objects	
CertKeyFieldName	String	Identification of a component of the certificate key (for example, "Modulus" or "Exponent")
CertKeyFieldValue	String	Corresponds to the Key Field Name
CertPublicKeyAlgorithm	String	Identifies the public key algorithm (for example, "RSA")
CertPublicKeyLength	String	Length in bytes of the public key (for example, 2048)
CertSerialNumber	String	Certificate serial number.
CertSignature	String	Digital signature of the device's signing certificate.
CertSignatureAlgorithm	String	Algorithm used when signing the certificate (for example, "SHA1withRSA")
CertSubject	String	Contains the certificate subject (for example, "2048-12-"L=Austin,ST=TX,C=US,O=Generated by Lenovo Firmware, CN=CA for A4AFBBC4-7702-3204-9A45-C6F315D66236\\, 15-03-10 10:49:01")
CertValidNotAfter	String	Date after which the certificate is not valid. The timestamp is returned in ISO 8601 format (for example, "2048-12-31T23:59:59Z").
CertValidNotBefore	String	Date before which the certificate is not valid. The timestamp is returned in ISO 8601 format (for example, "1970-01-01T00:00:00Z").
CertX509Version	String	Version of the X.509 certificate standard (for example, 3)

Attributes	Type	Description
result	String	Results of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.


```
{
   "response": {
      "CertificateOwnerUUID": "A4AFBBC4770232049A45C6F315D66236",
      "CurrentCertificatePem": "-----BEGIN CERTIFICATE-----\n
                        MIID8jCCAtqgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBmzFHMEUGA1UEAxM+QOEg\n
                        Zm9yIEEOQUZCQkM0LTc3MDItMzIwNC05QTQ1LUM2RjMxNUQ2NjIzNiwgMTUtMDIt\n
                        MTAgMTcMDk6MTAxJTAjBgNVBAoTHEdlbmVyYXRlZCBieSBMZW5vdm8gRmlybXdh\n
                        cmUxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJUWDEPMA0GA1UEBxMGQXVzdGluMB4X\n
                        DTcwMDEwMTAwMDAwMFoXDTQ4MTIzMTIzNTk1OVowgZsxRzBFBgNVBAMTPkNBIGZv\n
                        ciBBNEFGQkJDNC03NzAyLTMyMDQtOUE0NS1DNkYzMTVENjYyMzYsIDE1LTAyLTEw\n
                        IDE3OjA5OjEwMSUwIwYDVQQKExxHZW5lcmF0ZWQgYnkgTGVub3ZvIEZpcm13YXJl\n
                        MQswCQYDVQQGEwJVUzELMAkGA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjCCASIw\n
                        DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANa2OjDQESDz3IDaoyaTUxAmnKx1\n
                        ADhDFdL4md892U6WQLMWoeVHC/K3dUUS+Q/G/wk1gvXG9QRTUE5GAF/3yLVKL5xv\n
                        nmYmSLN7vR/By4tOZiOq3AlR71Us+NjXe8PpTud7piqtW4+2Q/mGOvvf7MtiOmQA\n
                        rjp3wSoOOZOJMgSIMCcme3POrETbbsGys/ENHBjBBxa1KZlAHzAMGkG7hY+eBOyZ\n
                        o9MdD8BW9ga9IaweiURhDJb8r5A3Bvk2+FQYeREYSeWrjrFZyHnkXtbZsMF8QnfB\n
                        7uCXUXv4xrQ2LnKOL7U98eOd8WBIfO46WpiwKPvJCALlqNXtCc2Qh//CPY8CAwEA\n
                        AaM/MDOwDAYDVR0TBAUwAwEB/zAOBgNVHQ8BAf8EBAMCAbYwHQYDVR0lBBYwFAYI\n
                        KwYBBQUHAwIGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQArAyb4oWH2ygxK\n
                        ZIk7+SNl8L7LO61T1nOrNmgYEL8rGmZQJyKqnZVz1PtTGIcnsOgugXrKU+UB1ZDK\n
                        FduNHg4T4GIpR4IthAincZAixXazkFJwf3izsTPYcyYBjyC1m9SWEsPEIVHCioAC\n
                        YLV2ckxYHpv6HndTRK8uIao/CAUZred03YjW78BS4aO3f+O6+63v3K35lOfSXNt+\n
                        OWkmHOqqpBDT8TbLGDNLOZMs6OOqzwT5iCULtjjasYVk+AX7UMrTlRJRVHAiJwkN\n
                        tvZtDVgeg7F+8wT1NziFEMdhmVWGusNzjn/NGIwqoUSklAj1opEY8DTVvVJleR8E\n
                        eerb7LRI\n
                        -----END CERTIFICATE-----\n",
      "CurrentCertificateText": {
         "CertIssuer": "L=Austin,ST=TX,C=US,O=Generated by Lenovo Firmware,
                        CN=CA for A4AFBBC4-7702-3204-9A45-C6F315D66236\\, 15-02-10 17:09:10",
         "CertKeyFields": [{
            "CertKeyFieldName": "Modulus",
            "CertKeyFieldValue": "27104856897092263881628924657409035726545809941480837091928188678853405444417985986087775622351553535692043985133
                                  92024783593731147448241547411588154638629834577297727770388973897666167175289605092484867693746340062771068275620645572823322887354006527067252255527400651309932019824218416562919492201349316259567512286728473767793866008851377802141442441605002795169526007063068766681728732385223578462830844738026917324598297824258592366029256422959119815275331225961686001031287285305384777872067366985694577207 8
```

```
                                67416061965757858311569128868977439622562886980390125950 4
                                37442881245320318676675403751368767519128446 87"
    },
    {
       "CertKeyFieldName": "Exponent",
       "CertKeyFieldValue": "65537"
    }],
    "CertPublicKeyAlgorithm": "RSA",
    "CertPublicKeyLength": "2048",
    "CertSerialNumber": "1",
    "CertSignature": "5429801536728126484921788109674957340505786174190498826058819020747
                  477023982943174484974227818967198422564210053481999472828071796438 3
                  234620572590939358804529426165540252979528812353282217731369472729 4
                  850557683042756326689212384986845403916180895258209960660147085322 5
                  855740620006305322392566222406747569860027168197317620007264184386 3
                  969853797578685192260892846328527251922750450803055439874001565806 7
                  607624552456704554389531591114720410215782517323580079169961303182 6
                  626713673177295546367958135678199050161296989633119290602515598715 1
                  525379430928089280382098698815246241062745108299747051560305999310 3
                  8218100454472",
    "CertSignatureAlgorithm": "SHA256withRSA",
    "CertSubject": "L=Austin,ST=TX,C=US,O=Generated by Lenovo Firmware,
                CN=CA for A4AFBBC4-77O2-32O4-9A45-C6F315D66236\\, 15-O2-1O 17:O9:1O",
    "CertValidNotAfter": "2O48-12-31T23:59:59Z",
    "CertValidNotBefore": "197O-O1-O1TOO:OO:OOZ",
    "CertX5O9Version": "3"
},
"TrustedCertificateText": {
    "CertIssuer": "L=Austin,ST=TX,C=US,O=Generated by Lenovo Firmware,
                CN=CA for A4AFBBC4-77O2-32O4-9A45-C6F315D66236\\, 15-O2-1O 17:O9:1O",
    "CertKeyFields": [{
       "CertKeyFieldName": "Modulus",
       "CertKeyFieldValue": "271048568970922638816289246574090357265458099414808370919
                         428188678853405444417985986087775622351553553569204398513
                         392024783593731147448241547411588154638629834577297727770
                         388973897666167175289605092484867693746340062771068275620
                         645572823322887354006527067252255527400651309932019824218
                         416562919492201349316259567512286728473767793866008851377
                         802141442441605002795169526007063068766681728732385223578
                         462830844738026917324598297824258592366029256422959119815
                         275331225961686001031287285305384777872067366985694577207 8
                         674160619657578583115691288689774396225628869803901259504 3
                         744288124532031867667540375136876751912844687"
    },
    {
       "CertKeyFieldName": "Exponent",
       "CertKeyFieldValue": "65537"
    }],
    "CertPublicKeyAlgorithm": "RSA",
    "CertPublicKeyLength": "2048",
    "CertSerialNumber": "1",
    "CertSignature": "5429801536728126484921788109674957340505786174190498826058819020747
                  477023982943174484974227818967198422564210053481999472828071796438 3
                  234620572590939358804529426165540252979528812353282217731369472729 4
                  850557683042756326689212384986845403916180895258209960660147085322 5
                  855740620006305322392566222406747569860027168197317620007264184386 3
                  969853797578685192260892846328527251922750450803055439874001565806 7
                  607624552456704554389531591114720410215782517323580079169961303182 6
                  626713673177295546367958135678199050161296989633119290602515598715 1
                  525379430928089280382098698815246241062745108299747051560305999310 3
                  8218100454472"
```

```
         "CertSignatureAlgorithm": "SHA256withRSA",
         "CertSubject": "L=Austin,ST=TX,C=US,O=Generated by Lenovo Firmware,
                     CN=CA for A4AFBBC4-7702-3204-9A45-C6F315D66236\\, 15-02-10 17:09:10",
         "CertValidNotAfter": "2048-12-31T23:59:59Z",
         "CertValidNotBefore": "1970-01-01T00:00:00Z",
         "CertX509Version": "3",
      }
   },
   "result": "success",
   "messages": [{
      "explanation": "The currently trusted certificate for the device matches the certificate
                  currently in use by the device. The untrusted connection is due to another
                  cause of certificate validation failure.",
      "id": "FQXHMSE0120I",
      "recovery": {
         "text": "Connect to the device and verify that the certificate in use is not expired
                and that the address the management server is using to connect to the device
                is present in the certificate. Ensure that the public key algorithm and
                signature algorithms in use in the certificate comply with the cryptography
                settings on the management server. If these actions do not resolve the issue,
                regenerate the devices certificate (selecting algorithms that comply with the
                cryptography settings on the management server) and try the operation again to
                resolve the untrusted connection. If the problem persists, collect service data
                and contact Support.",
         "URL": ""
      },
      "text": "The request to resolve the untrusted connection was not successful."
   }]
}
```


PUT /endpoint/signingCertificate/*{uuid}*/*{resource}*

Use this method to upload a Certificate Authority (CA) root certificate to the Lenovo XClarity Administrator trust store for a specific UUID.

Note: This method is not support on ThinkServer and System x M4 servers.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/endpoint/signingCertificate/{uuid}/{resource}`

where:

- *{uuid}* specifies the UUID of the target device.
- *{resource}* can be one of the following values.
  - **updatedCIMCertificate**. This resource type applies only to rack or tower server UUIDs.
  - **updatedLDAPCertificate**. This resource type applies only to rack or tower server UUIDs.
  - **updatedSigningCertificate**. This resource type applies only to chassis, storage device, and switch UUIDs.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
newCertificatePem	Required	String	PEM representation of the certificate to be uploaded into the XClarity Administrator trust store

The following example uploads a Certificate Authority (CA) root certificate.

```
{
    "NewCertificatePem": "-----BEGIN CERTIFICATE-----\n
                          MIID8jCCAtqgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmzFHMEUGA1UEAxM+QOEg\n
                          Zm9yIEEOQUZCQkMOLTc3MDItMzIwNCO5QTQ1LUM2RjMxNUQ2NjIzNiwgMTUtMDMt\n
                          MTAgMTA6NDk6MDExJTAjBgNVBAoTHEdlbmVyY XRlZCBieSBMZW5vdm8gRmlybXdh\n
                          ncmUxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJUWDEPMA0GA1UEBxMGQXVzdGluMB4X\n
                          DTcwMDEw MTAwMDAwMFoXDTQ4MTIzMTIzNTk1OVowgZsxRzBFBgNVBAMTPkNBIGZv\n
                          ciBBNEFGQkJDNCO3NzAyLTMyMDQtOUE0NS1DNkYzMTVEN jYyMzYsIDE1LTAzLTEw\n
                          IDEwOjQ5OjAxMSUwIwYDVQQKExxHZW5lcmFOZWQgYnkgTGVub3ZvIEZpcm13YXJln\n
                          MQswCQYDVQQGEwJVUzELM AkGA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjCCASIw\n
                          DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL1v1bO6QEoT4YWcD9fpjvWSZ uju\n
                          9HVspD45QBJo5rd8Pmpt+iaGyyPASTOa25TBQ8gSXADYkv7uRpKJ6b1fJhXsEeOC\n
                          4YXS3eTr4Ada9OfFqutzdbjygsxtyE4A5LijCu32wlSrXC KuQWCKTw35ItqkEc3n\n
                          DSqOwc9weRbsKzvDG2OoR+2NViwi9Wo7/fyYSQm+o5dIFbZenV4Jt5l3+wPiIYFnq\n
                          8TqFJeCRdZYvAFRnNs9FN2d7On 7AYtVZcL2CvFfnRhWfSpSWKABbwb5qcDRZ/D7\n
                          xis9c5MpqgX+Ca/3TUGVAO5VQatHXr2bR/odneSaViNyITxCgVfcNOH2xOECAwEA\n
                          AaM/M DOwDAYDVR0TBAUwAwEB/zAOBgNVHQ8BAf8EBAMCAbYwHQYDVR0lBBYwFAYI\n
                          KwYBBQUHAwIGCCsGAQUFBwMBMA0GCSqGSIb3DQEBB QUAA4IBAQBt56ech5RFnTTi\n
                          Hv7vG898TllKAFt7WDS5WA2I64x7SrWzWQcS1AuGrTvfRpDXKpdNjsZffmI+j9Oln\n
                          MbNBtQVWxxqfH/TVT+M+W PNVtBtkh1c3tLe9N55QxtBJtxgTJzwCI23JxS2DC34o\n
                          eAkbPYNq6B+wWaXectPj1dbQJvzOyVIPLMoyYmv7dR5bt05wQo83GoL1eYkofUls\n
                          rFXO z91rYF3QSIsovFp/KTTxR4/o2+aVHKl4K8J7bdDLQF5JrxB8tgxnlnOPt6U/\n
                          zIWy4uL5/WDZvlMzfTz7g/wPm4mz3amoOp2iUaUBG7azxciWtUg28dhGqwC/ejc/\n
                          ryhtZu+O\n
                          -----END CERTIFICATE-----\n"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

If the request is not successful, the response body includes the following attributes.

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request failed.

```
{
    "result": "failure",
    "messages": [{
        "explanation": "The operation to resolve the untrusted connection could not complete
                        because a resource associated with that device was not found.",
        "id": "FQXHMSE0119J",
        "recovery": {
            "text": "Ensure that the device is under management and attempt the operation
                     again. If the problem persists, collect service data and contact Support.",
            "URL": ""
        },
        "text": "The request to resolve the untrusted connection was not successful."
    }]
}
```

/identityManagementSystems

Use this REST API to return a list of all configured identity-management systems.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

HTTP methods

GET

GET /identityManagementSystems

Use this method to return a list of all configured identity-management systems.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/identityManagementSystems
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

The response body is an array of objects. Each object that contains information about each identity-management system.

Parameters	Type	Description
host	String	Hostname of the identity-management systems
name	String	Type of identity-management system
paths	Array of objects	Information about each path to the identity-management system
id	String	Path ID
appId	String	Application ID
safe	String	Safe
folder	String	Folder
port	String	Port for the identity-management system

The following example is returned if the request is successful.

```
[{
   "host": "cyberarkHostname",
   "name": "CyberArk",
   "paths": [{
      "id": "2",
      "appId": "LXCC",
      "safe": "safe_1",
      "folder": "folder_11"
   }, {
      "id": "4",
      "appId": "LXCC",
      "safe": "safe_2",
      "folder": ""
   }],
```

```
   "port": "1234"
}]
```

/identityManagementSystems/cyberark

Use this REST API to return information about or create the CyberArk identity-management system configuration.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

HTTP methods

GET, POST

GET /identityManagementSystems/cyberark

Use this method to return information about the CyberArk identity-management system configuration.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/identityManagementSystems/cyberark`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Parameters	Type	Description
host	String	IP address or hostname of the identity-management systems
name	String	Type of identity-management system
paths	Array of objects	Information about each path to the identity-management system
id	String	Path ID
appId	String	Application ID

Parameters	Type	Description
safe	String	Safe
folder	String	Folder
port	String	Port for the identity-management system

The following example is returned if the request is successful.

```
{
   "host": "cyberarkHostname",
   "name": "CyberArk",
   "paths": [{
      "id": "2",
      "appId": "LXCC",
      "safe": "safe_1",
      "folder": "folder_1"
   }, {
      "id": "4",
      "appId": "LXCC",
      "safe": "safe_2",
      "folder": ""
   }],
   "port": "1234"
}
```

POST /identityManagementSystems/cyberark

Use this method to create the CyberArk identity-management system configuration.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/identityManagementSystems/cyberark`

Query parameters

None

Request body

Parameter	Re-quired / Optional	Type	Description
host	Required	String	Hostname of the CyberArk server
port	Required	String	Port of the CyberArk server

The following example creates a CyberArk configuration.

```
{
   "host": "cyberarkHostname",
   "port": 12344
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

PUT /identityManagementSystems/cyberark

Use this method to modify the CyberArk identity-management system configuration.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/identityManagementSystems/cyberark`

Query parameters

None

Request body

Parameter	Re-quired / Optional	Type	Description
host	Required	String	Hostname of the CyberArk server
port	Required	String	Port of the CyberArk server

The following example creates a CyberArk configuration.

```
{
   "host": "cyberarkHostname",
   "port": 12344
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/identityManagementSystems/cyberark/paths

Use this REST API to return information about, modify, or delete a specific CyberArk path that is defined in Lenovo XClarity Administrator. A CyberArk path is made up of an application ID, safe, and optional folder that identify the location of onboarded user accounts in CyberArk.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

HTTP methods

GET, POST

GET /identityManagementSystems/cyberark/paths

Use this method to return a list of all CyberArk paths that are defined in Lenovo XClarity Administrator. A CyberArk path is made up of an application ID, safe, and optional folder that identify the location of onboarded user accounts in CyberArk.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/identityManagementSystems/cyberark/paths`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

The response body is an array of objects. Each object that contains information about each path to the identity-management system.

Parameters	Type	Description
id	String	Path ID
appId	String	Application ID
folder	String	Folder
safe	String	Safe

The following example is returned if the request is successful.

```
[{
   "id": "2",
   "appId": "LXCC",
   "safe": "safe_1",
   "folder": "folder_1",
}, {
   "id": "4",
   "appId": "LXCC",
   "safe": "safe_2",
   "folder": ""
}]
```

POST /identityManagementSystems/cyberark/paths

Use this method to create CyberArk path in Lenovo XClarity Administrator.

You can create at most one CyberArk identity-management system.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/identityManagementSystems/cyberark/paths`

Query parameters

None

Request body

Parameter	Re-quired / Optional	Type	Description
appId	Required	String	Application ID
safe	Required	String	Safe
folder	Required	String	Folder

The following example creates a CyberArk identity.

```
{
   "appId": "appid",
   "safe": "safe_1",
   "folder": "folder_1"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/identityManagementSystems/cyberark/paths/*{id}*

Use this REST API to return a list of all CyberArk paths that are defined in Lenovo XClarity Administrator, or to create a path.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

HTTP methods

GET, PUT, DELETE

GET /identityManagementSystems/cyberark/paths/*{id}*

Use this method to return information about a specific CyberArk path that is defined in Lenovo XClarity Administrator.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/identityManagementSystems/cyberark/paths/{id}`

where *{id}* is the ID of the CyberArk path. To obtain the path ID, use GET /identityManagementSystems/cyberark/paths.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Parameters	Type	Description
id	String	Path ID
appId	String	Application ID
safe	String	Safe
folder	String	Folder

The following example is returned if the request is successful.

```
{
   "id": "2",
   "appId": "LXCC",
   "safe": "safe_1",
   "folder": "folder_1",
}
```

PUT /identityManagementSystems/cyberark/paths/*{id}*

Use this method to modify a specific CyberArk path that is defined in Lenovo XClarity Administrator.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/identityManagementSystems/cyberark/paths/{id}`

where *{id}* is the ID of the CyberArk path. To obtain the path ID, use GET /identityManagementSystems/cyberark/paths.

Query parameters

None

Request body

Parameter	Re-quired / Optional	Type	Description
appId	Required	String	Application ID
safe	Required	String	Safe
folder	Required	String	Folder

The following example modifies a CyberArk identity.

```
{
   "appId": "appid",
   "safe": "safe_1",
   "folder": "folder_1"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /identityManagementSystems/cyberark/paths/*{id}*

Use this method to delete a specific CyberArk path that is defined in Lenovo XClarity Administrator.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/identityManagementSystems/cyberark/paths/{id}`

where *{id}* is the ID of the CyberArk path. To obtain the path ID, use GET /identityManagementSystems/cyberark/paths.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/ldapClientSettings

Use this REST API to retrieve or modify client settings when an external LDAP server is used for authentication.

HTTP methods

GET, PUT

GET /ldapClientSettings

Use this method to return information about the client settings when an external LDAP server is used for authentication.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/ldapClientSettings
```

Query parameters

Parameters	Required / Optional	Description
default=*{Boolean}*	Optional	Indicates whether default LDAP client settings are returned. This can be one of the following values. • **true**. Default settings are returned. • **false**. (default) Current values are returned.

The following example returns the default LDAP client settings.

```
GET https://192.0.2.0/ldapClientSettings?default=true
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Information about each user account
bindingMethod	String	Method that is used to bind XClarity Administrator to the external authentication server. This can be one of the following values. • **configured_credentials**: Uses the credentials specified in the **clientDn** and **clientPw** attributes to bind to the specified LDAP authentication server. • **login_credentials**: Uses the login credentials of the authenticating user to bind to the specified LDAP authentication server. The credentials specified in the existing **clientDn** and **clientPw** attributes are used to perform an initial test connection to the authentication server, but these values are not saved.
clientDn	String	Distinguished name of the client
clientPw	Boolean	Indicates if a client password is stored currently. This can be one of the following values. • **true**. There is currently a stored client password. • **false**. There is not currently a stored client password.
domainName	String	Domain name used by DNS to locate LDAP servers
forestName	String	Forest name used by DNS to locate LDAP servers
groupFilters	String	Groups search filters to customize the authentication process when configuring XClarity Administrator with an external LDAP server For information about search filter syntax, see How to write LDAP search filters. For search filter examples, see Examples of Common ldapsearches
groupNameAttribute	String	Attribute name that is used to identify the group name that is configured by the LDAP server The default is **uid**.
groupSearchAttribName	String	Attribute name that is used to identify the groups to which a user belongs The default is **memberOf**.
rootDn	String	Root distinguished name with the topmost entry in your LDAP directory tree
searchLimit	Integer	Maximum number of in-search results that can be retrieved in an LDAP search operation using user and group filters This can be a value from **0** – **5000**. The default value is **0**, which means that the operation does not time out.
serverAddress	Array of objects	Information about the server address
address	String	IP address for the server
port	Integer	Port number of the server connection

Attributes	Type	Description
serverSelectionMethod	String	Specifies how LDAP servers are to be selected. This can be one of the following values. • **preconfigured**. The IP addresses or hostnames will be used for external authentication servers. • **dns**. The domain name and optional forest name will be used to locate the domain controller (DC) and global catalog (GC) servers dynamically.
sslEnabled	Boolean	Indicates if SSL is enabled. This can be one of the following values. • **true**. SSL is enabled. • **false**. SSL is not enabled.
timeout	Integer	Amount of time, in seconds, to complete an LDAP search operation before timing out This can be a value from **0** – **300** (5 minutes). The default value is **0.**
userAuthenticationMethod	String	Type of user authentication. This can be one of the following values. • **local**. Authentication is performed locally. • **ldap**. Authentication is performed by an external LDAP server. • **ldap_local**. Authentication is performed by an external LDAP server first. If that fails, authentication is performed locally. • **local_ldap**. Authentication is performed locally first. If that fails, authentication is performed by an external LDAP server.
userFilters	String	Users search filters to customize the authentication process when configuring XClarity Administrator with an external LDAP server For information about search filter syntax, see How to write LDAP search filters. For search filter examples, see Examples of Common ldapsearches
userSearchAttribName	String	Attribute name that is used to identify the user IDs on the LDAP server When the binding method is set to **Configured Credentials**, the initial bind to the LDAP server is followed by a search request that retrieves specific information about the user, including the user's DN, login permissions, and group membership. This search request must specify the attribute name that represents the user IDs on that server. The default is **cn**.

Attributes	Type	Description
useServersAsGlobalCatalogs	Boolean	Indicates whether to treat domain controllers as global catalogs. This can be one of the following values. • **true**. (default) XClarity Administrator attempts to connect to the standard global-catalog port (3268 or 3269) on each known domain-controller address. If XClarity Administrator can bind to the port, the domain-controller server is treated as a global catalog, and XClarity Administrator uses the global catalog to locate additional user accounts during the authentication process. When a user account is located in the global catalog, XClarity Administrator connects to the domain-controller server that controls the domain in which the user exists to authenticate the user and obtain any domain local groups. XClarity Administrator can locate domain controllers that are not listed in the DNS as long as they are listed in the global catalog. • **false.** XClarity Administrator does not attempt to connect to the global catalog port on each domain-controller address unless the user explicitly specified the server's global-catalog port as one of the preconfigured servers in the **serverAddress** attribute.For example, if you set **serverSelectMethod** to `preconfigured`, **serverAddress** to `192.0.2.0` on port `389`, and **useServersAsGlobalCatalogs** to `false`, XClarity Administrator does not automatically attempt to connect to port 3268 on that server to determine whether it can function as a global catalog. However, if you specify two pre-configured servers in **serverAddress**, both with the same IP address `192.0.2.0` but different ports `389` and `3268`, XClarity Administrator connects to the second server as a global-catalog server because you explicitly requested XClarity Administrator to attempt to connect to that port. Setting **useServersAsGlobalCatalogs** to `true` allows you to specify the server only once.
result	String	Request results. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": {
      "bindingMethod": "configured_credentials",
      "clientDn": "",
      "clientPw": false,
      "domainName": "",
      "forestName": "",
```

```
      "groupFilter": "",
      "groupNameAttribute": "cn",
      "groupSearchAttribName": "memberOf",
      "rootDn": "",
        "serverAddress": [{
            "address": "1.1.1.1",
            "port": 1
        },
        {
            "address": "2.2.2.2",
            "port": 2
        },
        {
            "address": "3.3.3.3",
            "port": 3
        },
        {
            "address": "4.4.4.4",
            "port": 4
        }],
      "searchFilter": "",
      "searchSizeLimit": 0,
      "serverSelectionMethod": "preconfigured",
      "sslEnabled": true,
      "timeoutLimit": 0,
      "userAuthenticationMethod": "local",
      "userSearchAttribName": "cn"
   "useServersAsGlobalCatalogs" : true
   },
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```


PUT /ldapClientSettings

Use this method to modify the client settings when an external LDAP server is used for authentication..

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/ldapClientSettings`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
bindingMethod	Required	String	Method that is used to bind XClarity Administrator to the external authentication server. This can be one of the following values. • **configured_credentials**: Uses the credentials specified in the **clientDn** and **clientPw** attributes to bind to the specified LDAP authentication server. • **login_credentials**: Uses the login credentials of the authenticating user to bind to the specified LDAP authentication server. The credentials specified in the existing **clientDn** and **clientPw** attributes are used to perform an initial test connection to the authentication server, but these values are not saved.
clientDn	Required if **userAuthenticationMethod** is set to **ldap**.	String	Distinguished name of the client
clientPw	Required if **userAuthenticationMethod** is set to **ldap**.	String	Client password value **Note:** This attribute is required when **userAuthenticationMethod** is set to "ldap."
domainName	Required if **serverSelectMethod** is set to **dns**	String	Domain name used by DNS to locate LDAP servers
forestName	Optional	String	Forest name used by DNS to locate LDAP servers
groupFilters	Optional	String	Groups search filters to customize the authentication process when configuring XClarity Administrator with an external LDAP server For information about search filter syntax, see How to write LDAP search filters. For search filter examples, see Examples of Common ldapsearches
groupNameAttribute	Optional	String	Attribute name that is used to identify the group name that is configured by the LDAP server The default is **uid**.
groupSearchAttribName	Optional	String	Attribute name that is used to identify the groups to which a user belongs If this attribute is not specified, the default is **memberOf**.
rootDn	Optional	String	Root distinguished name with the topmost entry in your LDAP directory tree
searchLimit	Optional	Integer	Maximum number of in-search results that can be retrieved in an LDAP search operation using user and group filters This can be a value from **0** – **5000**. The default value is **0**, which means that the operation does not time out.

Attributes	Required / Optional	Type	Description
serverAddress	Required if **serverSelectMethod** is set to **preconfigured**.	Array of objects	Array of up to four LDAP server addresses and ports
port	Required for specified entries	Integer	Port number of the server connection
address	Required for specified entries	String	IP address for the server
serverSelectMethod	Required if **userAuthenticationMethod** is set to **ldap**.	String	Specifies how LDAP servers are to be selected. This can be one of the following values. • **preconfigured**. The IP addresses or hostnames will be used for external authentication servers. • **dns**. The domain name and optional forest name will be used to locate the domain controller (DC) and global catalog (GC) servers dynamically. **Note:** This attribute is required when **userAuthenticationMethod** is set to "ldap."
sslEnabled	Required	Boolean	Indicates if SSL is enabled. This can be one of the following values. • **true**. SSL is enabled. • **false**. SSL is not enabled.
timeout	Optional	Integer	Amount of time, in seconds, to complete an LDAP search operation before timing out This can be a value from **0** – **300** (5 minutes). The default value is **0.**
userAuthenticationMethod	Required	String	Type of user authentication. This can be one of the following values. • **local**. Authentication is performed locally. • **ldap**. Authentication is performed by an external LDAP server. • **ldap_local**. Authentication is performed by an external LDAP server first. If that fails, authentication is performed locally. • **local_ldap**. Authentication is performed locally first. If that fails, authentication is performed by an external LDAP server.
userFilters	Optional	String	Users search filters to customize the authentication process when configuring XClarity Administrator with an external LDAP server For information about search filter syntax, see How to write LDAP search filters. For search filter examples, see Examples of Common ldapsearches

Attributes	Required / Optional	Type	Description
userSearchAttribName	Optional	String	Attribute name that is used to identify the user IDs on the LDAP server When the binding method is set to **Configured Credentials**, the initial bind to the LDAP server is followed by a search request that retrieves specific information about the user, including the user's DN, login permissions, and group membership. This search request must specify the attribute name that represents the user IDs on that server. If this attribute is not specified, the default is **cn**.
useServersAsGlobalCata-logs	Optional	Boolean	Indicates whether to treat domain controllers as global catalogs. This can be one of the following values. • **true**. (default) XClarity Administrator attempts to connect to the standard global-catalog port (3268 or 3269) on each known domain-controller address. If XClarity Administrator can bind to the port, the domain-controller server is treated as a global catalog, and XClarity Administrator uses the global catalog to locate additional user accounts during the authentication process. When a user account is located in the global catalog, XClarity Administrator connects to the domain-controller server that controls the domain in which the user exists to authenticate the user and obtain any domain local groups. XClarity Administrator can locate domain controllers that are not listed in the DNS as long as they are listed in the global catalog. • **false.** XClarity Administrator does not attempt to connect to the global catalog port on each domain-controller address unless the user explicitly specified the server's global-catalog port as one of the preconfigured servers in the **serverAddress** attribute.For example, if you set **serverSelectMethod** to `preconfigured`, **serverAddress** to `192.0.2.0` on port `389`, and **useServersAsGlobalCatalogs** to `false`, XClarity Administrator does not automatically attempt to connect to port 3268 on that server to determine whether it can function as a global catalog. However, if you specify two pre-configured servers in **serverAddress**, both with the same IP address `192.0.2.0` but different ports `389` and `3268`, XClarity Administrator connects to the second server as a global-catalog server because

Attributes	Required / Optional	Type	Description
			you explicitly requested XClarity Administrator to attempt to connect to that port. Setting **useServersAsGlobalCatalogs** to `true` allows you to specify the server only once.

The following example modifies the client LDAP settings.

```
{
   "bindingMethod": "configured_credentials",
   "clientDn": "userid",
   "clientPw": "PasswOrd",
   "domainName": "lenovo.com",
   "forestName": "forestName",
   "groupNameAttribute": "cn",
   "groupSearchAttribName": "memberOf",
   "rootDn": "rootDn",
   "serverAddress": [{
      "port": 1,
      "address": "1.1.1.1"
   },
   {
      "port": 2,
      "address": "2.2.2.2"
   },
   {
      "port": 3,
      "address": "3.3.3.3"
   },
   {
      "port": 4,
      "address": "4.4.4.4"
   }],
   "serverSelectionMethod": "dns",
   "sslEnabled": true,
   "userAuthenticationMethod": "ldap",
   "userSearchAttribName": "cn"
   "useServersAsGlobalCatalogs" : true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request failed.

```
{
   "result": "failure",
   "messages": [{
      "id": "FQXHMSE0611J",
      "explanation": "The request to change the LDAP configuration could not complete for an unknown
                  reason.",
      "recovery": {
         "text": "Specify valid parameters on the request and try the request again. If the problem
                persists, contact Support.",
         "URL": ""
      },
      "text": "The request to change the LDAP configuration could not be completed successfully."
   }]
}
```

/mutualAuthCertificates

Use this REST API to return the list of all TLS mutual-authentication certificates or regenerate a TLS mutual-authentication certificate.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

HTTP methods

GET, POST

GET /mutualAuthCertificates

Use this method to return the list of all TLS mutual-authentication certificates.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/mutualAuthCertificates`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

When the request is successful, the mutual-authentication certificate file, in PEM format, is returned. If the request fails, standard message attributes are returned (see Status messages).

Parameters	Type	Description
serverTypeName	String	Server type name. This can be the following value. • **CyberArk**
serverTypeId	String	Server type key. This can be the following value. • **cyberark**
certificate	String	Certificate, in PEM format

The following example is returned if the request is successful.


```
[{
   "serverType": "cyberark",
   "certificate": "-----BEGIN CERTIFICATE-----
                   MIIFRjCCBC6gAwIBAgIVAOYU3FiQqz7RQ+KehCLhan3h+le4MA0GCSqGSIb3DQEB
                   CwUAMHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3JOaCBDYXJvbGluYTEQMA4G
                   A1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5IFNlcnZlciBGaXJt
                   d2FyZTEJMAcGA1UECxMAMQ0wCwYDVQQDEwRMWENBMCAXDTcwMDEwMTA1MDAwMFoY
                   DzIwNzAwMTAxMDQ1OTU5WjCBkDELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRo
                   IENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdoMQ8wDQYDVQQKEwZMZW5vdm8xDDAK
                   BgNVBAsTA0VCRzE3MDUGA1UEAxMuR2VuZXJhdGVkIGJ5IExlbm92byBTeXN0ZW0g
                   TWFuYWdlbWVudCBTb2ZOd2FyZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
                   ggEBAIHSk5uFESdIg2jz3p2EuMtT2bLXPOQLG4wzhKzp4es3HMne7sXfhZ3kYYoU
                   DjTtA8tV2t1z8lQdol3pVeJdA4rb2gO8s6kgtR/F+GgJbSGQUlTWuLNXT3zwAsCO
                   kipJBoZO1r3oYCJdUkgCvCOVMFDIyILyhSejsXXny5aFacl7OVJhATk7fEkEy3HH
                   4PdcB7UvJpaLwAUyMJtKr3ZST2K71BPMTNCraOyK42qiR6tUBhxuGraiuk6niMUn
                   XUPf81kCLmXVI96G3/YcMT9+4orooaXmFCtXz3g3ZJ9nZxzntgH2BcpQgnIGQ1Gm
                   NUw9HK3bOrLI7xNJuOkTCSA6Yt8CAwEAAaOCAakwggGlMAwGA1UdEwEB/wQCMAAw
                   gbYGA1UdIwSBrjCBq4AUbhZrZRZDulpKYG3OgI2t1Bn8AFmhfaR7MHkxCzAJBgNV
                   BAYTAlVTMRcwFQYDVQQIEw5Ob3JOaCBDYXJvbGluYTEQMA4GA1UEBxMHUmFsZWln
                   aDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5IFNlcnZlciBGaXJtd2FyZTEJMAcGA1UE
```

```
CxMAMQOwCwYDVQQDEwRMWENBghRWKEwW81vplOg538WZJ7uxayc2PzAdBgNVHQ4E
FgQUogeZxr9VEeeU5T8ELvS8lAW7MdOwgbwGA1UdEQSBtDCBsYcQ/oAAAAAAAAAK
ACf//sOOg4IeZmU4MDowOjA6MDphMDA6MjdmZjpmZWNkOmU4MyUyhwQK8Ynggg4x
MC4yNDEuMTM3LjIyNIcQAAAAAAAAAAAAAAAAAAAAAYIJbG9jYWxob3NOhwR/AAAB
gglsb2NhbGhvc3SCCWxvY2FsaG9zdIIuR2VuZXJhdGVkIGJ5IExlbm92byBTeXNO
ZWOgTWFuYWdlbWVudCBTb2ZOd2FyZTANBgkqhkiG9wOBAQsFAAOCAQEArHLB5QR2
Hn+RWIGfA4uYrIgD2tJvtkbE9uVXF/8s8HvNQ+fGIFZEdnuqjIXcxBAUq9xwapvj
PbDRgjzca/tl3xxvPQ9XW9jt9RdPAcn+TbxzlhnPTOydqoYy+Rfd2sGL1GgOn7GR
nxrlR+JWVGd7f3j8lPK3jO5JKThpUW+PrECZwbM9wgJ4wNF6xmHqLOiCWznqhtUd
ytp7aYmGuj4h53hyJeqzlBXQA1Kd5AhB2/3cpbO2lgB4av+stGHn2WzPER5jbRF/
q5Up7/5UhA2wSQaOVap4109XQqXQL8p5VxpPDlumhothguqgN4yOfVxF4pGytOqX
W+IcyiYy15ufNA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID1TCCAr2gAwIBAgIUVihMFvNb6ZdIOd/FmSe7sWsnNj8wDQYJKoZIhvcNAQEL
BQAweTELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYD
VQQHEwdSYWxlaWdoMSUwIwYDVQQKExxHZW5lcmF0ZWQgYnkgU2VydmVyIEZpcm13
YXJlMQkwBwYDVQQLEwAxDTALBgNVBAMTBExYQOEwIBcNNzAwMTAxMDUwMDAwWhgP
MjA3MDAxMDEwNDU5NTlaMHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBD
YXJvbGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5
IFNlcnZlciBGaXJtd2FyZTEJMAcGA1UECxMAMQOwCwYDVQQDEwRMWENBMIIBIjAN
BgkqhkiG9wOBAQEFAAOCAQ8AMIIBCgKCAQEAuFx2YjVCCAKa2Sp5QpxdmCS8R8GI
l/92LyK37HySwKgaTSm9nxkQt2paZUg+NzMqOAbOmTwmVOT8/eGbtWFmWyqeFGr4
5m+MC3KhxOjrhOzQyRzrbmIOprgW1LSbDwRRon5k4efXhcvfmrNGoXHkGysMLOCZ
+bRk9XCjm+EFjwaW28pTHE8XfdMJD1zxy467vJQ9AOVNSh7YYflKw1jV73xMYiV9
tNbAADFCUT5RHicXxgF8huyKcJCHppiH9z6DqEOtgOZfeXqQJHmW5udweVmt646s
HEGNrCqmntAQcASIzDVfgYKm1dQn+mQAH5FJ/jyjnqjhP7AFIoneXOLYkwIDAQAB
o1MwUTAPBgNVHRMBAf8EBTADAQH/MBOGA1UdDgQWBBRuFmtlFkO6WkpgbfSAja3U
GfwAWTAfBgNVHSMEGDAWgBRuFmtlFkO6WkpgbfSAja3UGfwAWTANBgkqhkiG9wOB
AQsFAAOCAQEAHa/w2SNQkSpAtoEnHZpDpZrThpNeeQxPMX2+Us2QxOa4Wr8WditB
9sK89inebkRSZxBTsZNKf4w1XT2TlND5mY88K4rQ15YZdLSJvaKr9QmKSbmBKWeT
dcOX5HLaB8evP4EoOC32BXvklx+SnNtZHupcXo8JfmC38Hxftpn8ZfiAfiYr4jZI
iIom6Zupxoc7ZuyAWOovp4V5jKmglWDM4xXRTDsYcHEOpnGOry+MlPEAszDexYd8
HNdO2BliTsytll6RsSoJ6B9gu49OOcSRYpp543azUDStsoJ8a/8CfyeGMje6aREg
tOumP61rQlEYyUmEcEr/eDZt8pjXiR/txw==
-----END CERTIFICATE-----
```

POST /mutualAuthCertificates

Use this method to regenerate a TLS mutual-authentication certificate.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/mutualAuthCertificates`

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
serverTypeId	Required	String	Server type key. This can be the following value. • **cyberark**

The following example regenerates a TLS mutual-authentication certificate.

```
{
   "serverType": "cyberark"
}
```

Response codes

Code	Description	Comments
201	Created	One or more new resources were successfully created.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The standard message attributes are returned (see Status messages).

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "The existing certificate has been replaced by the new certificate",
        "id": "FQXHMSE0134I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request to generate mutual-authentication certificate was successful.",
    }]
}
```

/mutualAuthCertificates/cyberark/*{type}*

Use this REST API to download the mutual-authentication certificate for CyberArk, in PEM or DER format.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

HTTP methods

GET

GET /mutualAuthCertificates/cyberark/*{type}*

Use this method to download the mutual-authentication certificate for CyberArk, in PEM or DER format.

Note: This API requires Lenovo XClarity Administrator v3.2.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/mutualAuthCertificates/cyberark/{type}`

where *{type}* is the format type. You can specify **der** (for DEM format) or **pem** (for PEM format).

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

When the request is successful, a response body is not returned. If the request fails, standard message attributes are returned (see Status messages).

/mutualAuthCertificates/cyberark/details

Use this REST API to return information about the mutual-authentication certificate for CyberArk.

HTTP methods

GET

GET /mutualAuthCertificates/cyberark/details

Use this method to return information about the mutual-authentication certificate for CyberArk.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/mutualAuthCertificates/cyberark/details`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	Information about the certificate
certificate	String	Certificate, in PEM format
issuerDn	String	LDAP Distinguished Name of the issuer (for example, `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`).
notAfter	String	Timestamp when the certificate is no longer valid. The timestamp is returned in ISO 8601 format (for example, `2014-02-05T15:54:13Z`).
notBefore	String	Timestamp when the certificate becomes valid. The timestamp is returned in ISO 8601 format (for example, `2014-02-05T15:54:13Z`).
serialNumber	String	Serial number of the certificate
signatureAlgorithm	String	Algorithm used to sign the certificate (for example, `"MD5withRSA","SHA256withRSA"`).
status	String	Certificate status. This can be one of the following values. • **internal**. The server certificate was signed by an internal Certificate Authority. • **external**. The server certificate was signed by an external Certificate Authority.
subjectDn	String	LDAP Distinguished Name of the subject (for example, `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`).
{message_attributes}	*varies*	Status messages (see Status messages).

The following example is returned if the request is successful.

```
{
   "response": [{
      "certificate": "-----BEGIN CERTIFICATE-----\r\n
                     MIIF2jCCBMKgAwIBAgIVAJgbWgQ/HUsaEEkFEdueK2lEONxqMA0GCSqGSIb3DQEB\r\n
                     CwUAMHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3JOaCBDYXJvbGluYTEQMA4G\r\n
                     A1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5IFNlcnZlciBGaXJt\r\n
                     d2FyZTEJMAcGA1UECxMAMQ0wCwYDVQQDEwRMWENBMCAXDTcwMDEwMTA2MDAwMFoY\r\n
                     DzIwNzAwMTAxMDU1OTU5WjB5MQswCQYDVQQGEwJVUzEXMBUGA1UECBMOTm9ydGgg\r\n
                     Q2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxJTAjBgNVBAoTHEdlbmVyYXRlZCBi\r\n
                     eSBTZXJ2ZXIgRmlybXdhcmUxCTAHBgNVBAsTADENMAsGA1UEAxMETFhDQTCCASIw\r\n
                     DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIRVJvuGU11o9Do/bjQvTbWaSXS9\r\n
                     tFPhg/JyZP5q9RYlCfgRveh1nArAAO7t2XZMLC2l5Cv6kmbQUPsTVQLs2JetmnLS\r\n
                     IpUwOuIwgV448OIl5jF7x4Wx4sDvPSTy9DnbeLUGOPV5zkwNLv8wVGe7eTTWGG2i\r\n
                     SGozfBCuwDc2MO6WJPhDiZhBf+CU/d27P3oIDxNUa6NJkfI3CI6sivpTfpT8oHdB\r\n
```

```
                        P4PIdKJ4VGmhO72bHCOvFaOm4C/eip5h5rskJmw5DHeiujp7nq9o+qOQYLST8mNU\r\n
                        IGuQ+12+s/4JYz2hZAFOtRmPbnmD8YSVPVKP67jYYsQziBn7jNtBS7oOOeUCAwEA\r\n
                        AaOCAlUwggJRMAwGA1UdEwEB/wQCMAAwgbYGA1UdIwSBrjCBq4AUeTimSPAWXgpz\r\n
                        6+pN33JKZ3zks2KhfaR7MHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3JOaCBD\r\n
                        YXJvbGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5\r\n
                        IFNlcnZlciBGaXJtd2FyZTEJMAcGA1UECxMAMQOwCwYDVQQDEwRMWENBghQX6Oe/\r\n
                        U7Ai3C78CGAhNptbHBF49TAdBgNVHQ4EFgQU/lKzmh6UpXDOdSTFmZk6Z9VRSPYw\r\n
                        ggFnBgNVHREEggFeMIIBWocEfwAAAYIJMTI3LjAuMC4xhxAAAAAAAAAAAAAAAAAA\r\n
                        AAABgg8wOjA6MDowOjA6MDowOjGHEP6AAAAAAAAAAOAAAAAAAACCFmZlODA6MDow\r\n
                        OjA6ZTA6MDowOjAlMTCHEP6AAAAAAAAAKePrsll+T/+CIWZlODA6MDowOjA6Mjll\r\n
                        MzplYmIyOjU5N2U6NGZmZiUxMocECipk3oIaRFJBSO5FUlVELThMRjBOLmxlbm92\r\n
                        by5jb22HEP6AAAAAAAAA4VspLzmOURiCGkRSQUtORVJVRCO4TEYwTi5sZW5vdm8u\r\n
                        Y29thxD+gAAAAAAAAFXfh6O5j+bqgiFmZTgwOjA6MDowOjU1ZGY6ODdhZDozOThm\r\n
                        OmU2ZWElMTaHEP6AAAAAAAAAAABe/goqZN6CHWZlODA6MDowOjA6MDo1ZWZlOmEy\r\n
                        YTo2NGRlJTE3gglsb2NhbGhvc3SCBExYQOEwDQYJKoZIhvcNAQELBQADggEBAJRj\r\n
                        k88tQx4IitOQ7HpmyjOE9W4ilvVTGZ9Zk56gN2lPWY/m2TL1RLbiid/cWpy6RnNd\r\n
                        PGbO1whRmwTpq5Ihec6wdONLXZFlS5GaOqMu+opzXnwvuGBn1y/jQjnpIV+TcKQL\r\n
                        9LAvzmPoMYd8BqF/sfR1rdmgyGeTzG/yUEaChXGOTLkbkT+9gYFN/gPDy4hAv2i9\r\n
                        zLQnCXsqH5ZIDRAf42P8uHZ6hBkgra/vXdh+rB9mgIJZV2ijgjoYl6bIGw+9zL3L\r\n
                        t2Jfh2u4MCpQs47FVZ2Fds3YaprHf5SVamUspTIOdsNzFU1F/xa2NRaWzu3T5+mj\r\n
                        JOHNoKWv4KcJXzyXuLo=\r\n
                        -----END CERTIFICATE-----\r\n",
        "is   suerDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
        "notAfter": "2070-01-01T05:59:59Z",
        "notBefore": "1970-01-01T06:00:00Z",
        "serialNumber": "981b5a043f1d4b1a10490511db9e2b694438dc6a",
        "signatureAlgorithm": "SHA256withRSA",
        "status": "internal",
        "subjectDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US"
    }],
    "result": "success",
    "messages": [{
        "id": "FQXHMSE0001I",
        "text": "The request completed successfully."
        "explanation": "",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
    }]
}
```


/privileges

Use this REST API to retrieve information about all user privileges.

HTTP methods

GET

GET /privileges

Use this method to return information about all user privileges.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/privileges`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Information about each user privilege
category	Object	Category to which the privilege belongs
description	String	Category description
id	String	Category ID
description	String	Privilege description
id	String	Privilege ID
managementModulePermis-sion	Long	(Management-module permissions only) LDAP permission bits (bitstrings) that are associated with the privilege. For information about the LDAP permission bits for each management module, see the online documentation. • Configuring LDAP in the CMM and CMM2 online documentation • Configuring LDAP in the IMM and IMM2 online documentation • Configuring LDAP in the XCC online documentation
name	String	Privilege name
result	String	Result of the request . This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event

Attributes	Type	Description
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.


```
{
   "response": [{
      "category": {
         "description": "Default",
         "id": "502"
      },
      "description": "Access All Resources",
      "id": "65",
      "name": "lxc-access-all-resources"
   },
   ...,
   {
      "category": {
         "description": "Task Management",
         "id": "521"
      },
      "description": "Run jobs",
      "id": "455",
      "name": "lxc-tasks-run-jobs"
   }],
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```


/privileges/*{id}*

Use this REST API to retrieve information about a specific user privilege.

HTTP methods

GET

GET /privileges/*{ID}*

Use this method to return information about a specific privilege.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/privileges/{ID}`

where *{id}* is the ID of the privilege to be retrieved. To obtain the privilege IDs, use GET /privileges.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Information about each privilege
category	Object	Category to which the privilege belongs
description	String	Category description
id	String	Category ID
description	String	Privilege description
id	String	Privilege ID
managementModulePermis-sion	Long	(Management-module permissions only) LDAP permission bits (bitstrings) that are associated with the privilege. For information about the LDAP permission bits for each management module, see the online documentation. • Configuring LDAP in the CMM and CMM2 online documentation • Configuring LDAP in the IMM and IMM2 online documentation • Configuring LDAP in the XCC online documentation
name	String	Privilege name
result	String	Result of the request . This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event

Attributes	Type	Description
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "result": "success",
   "response": {
      "category": {
         "description": "Task Management",
         "id": "521"
      },
      "description": "Run jobs",
      "id": "455",
      "name": "lxc-tasks-run-jobs"
   },
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```

/privilegeCategories

Use this REST API to retrieve information about all privilege categories.

HTTP methods

GET

GET /privilegeCategories

Use this method to return information about all privilege categories.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/privilegeCategories`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Information about each privilege category
description	String	Category description
id	String	Category ID
privileges	Array of objects	Information about the privileges that are assigned to the category
description	String	Privilege description
id	String	Privilege ID
name	String	Privilege name
result	String	Result of the request . This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": [{
      "description": "Default",
      "id": 502,
      "privileges": [{
         "description": "Administrator All",
         "id": "224",
         "name": "lxc-admin-all"
      },
      ...,
      {
         "description": "Hardware Admin All",
```

```
            "id": "164",
            "name": "lxc-hw-admin-all"
        }]
    },
    ...,
    {
        "description": "Security",
        "id": 504,
        "privileges": [{
            "description": "Regenerate server certificate",
            "id": "128",
            "name": "lxc-sec-regenerate-server-certificate"
        },
        ...,
        {
            "description": "Upload server certificate",
            "id": "127",
            "name": "lxc-sec-upload-server-certificate"
        }]
    }],
    "result": "success",
    "messages": [{
        "id": "FQXHMSE0001I",
        "text": "The request completed successfully.",
        "recovery": {
            "text": "Information only. No action is required.",
            "URL": ""
        },
        "explanation": ""
    }]
}
```

/privilegeCategories/*{id}*

Use this REST API to retrieve information about a specific privilege category.

HTTP methods

GET

GET /privilegeCategories/*{ID}*

Use this method to return information about a specific privilege category.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/privilegeCategories/{ID}`

where *{id}* is the ID of the category to be retrieved. To obtain the category IDs, use GET /privilegeCategories.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	Information about each privilege category
description	String	Category description
id	String	Category ID
privileges	Array of objects	Information about the privileges that are assigned to the category
description	String	Privilege description
id	String	Privilege ID
name	String	Privilege name
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.


```
{
   "response": {
      "description": "Security",
      "id": 504,
      "privileges": [{
         "description": "Regenerate server certificate",
         "id": "128",
         "name": "lxc-sec-regenerate-server-certificate"
      },
      ...,
      {
         "description": "Upload server certificate",
         "id": "127",
         "name": "lxc-sec-upload-server-certificate"
      }]
   },
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```


/resourceAccessControl

Use this REST API to retrieve and modify the access-control settings.

HTTP methods

GET, PUT

GET /resourceAccessControl

Use this method to return the current access-control settings.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/resourceAccessControl`

Query parameters

None

Request body

None

Response codes

Code	Description
200	OK
500	Internal server error

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
response	Object	
defaultRoleGroups	Array of strings	List of role groups that are authorized by default to view and manage all devices when the devices are initially managed. After a device is managed by Lenovo XClarity Administrator, you can change the authorized role groups for that device. (see PUT /chassis/*{uuid}*, PUT /nodes/*{uuid}*, PUT /storage/*{uuid}*, and PUT /storage/*{uuid}*).
publicAccess	Boolean	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups .
resourceAccessControlEnabled	String	Indicates whether access control is enabled. This can be one of the following values: • **true**. Access control is enabled • **false**. Access control is disabled
messages	Array	Information about one or more messages.
explanation	String	Additional information to clarify the reason for the message.
id	String	The message identifier of a returned message.
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event.
URL	String	Link to the help system for more information, if available.
text	String	Message text associated with the message identifier.

Response example

```
{
   "result": "success",
   "response": {
      "defaultRoleGroups": ["lxc-hw-admin","lxc-os-admin"]
      "publicAccess": false,
      "resourceAccessControlEnabled": true,
   },
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
```

```
      },
      "explanation": ""
   }]
}
```

PUT /resourceAccessControl

Use this method to modify the current access-control settings.

Note: Only users with **lxc-supervisor** or **lxc-security-admin** authority can modify the access-control settings.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/resourceAccessControl`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
defaultRoleGroups	Optional	Array of strings	List of role groups that are authorized by default to view and manage all devices when the devices are initially managed. After a device is managed by Lenovo XClarity Administrator, you can change the authorized role groups for that device. (see PUT /chassis/*{uuid}*, PUT /nodes/*{uuid}*, PUT /storage/*{uuid}*, and PUT /storage/*{uuid}*).
publicAccess	Optional	Boolean	Indicates whether the resource can be accessed by all role groups. This can be one of the following values. • **true**. The resource is can be access by all role group. • **false**. The resource is restricted to specific role groups .
resourceAccessControlEnabled	Optional	Boolean	Indicates whether access control is enabled. This can be one of the following values. • **true**. Access control is enabled • **false**. Access control is disabled

The following example disables access control.

```
{
   "resourceAccessControlEnabled": false
}
```

The following example enables access control and sets the default role groups for all devices.

```
{
   "resourceAccessControlEnabled": true,
   "defaultRoleGroups": ["lxc-hw-admin","lxc-os-admin"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/roles

Use this REST API to retrieve information about all user roles and to create a custom role.

HTTP methods

GET, POST

GET /roles

Use GET to retrieve information about all custom and predefined roles.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/roles`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	Each array element represents a user role
description	String	Role description
id	Integer	Role ID
name	String	Name of the role. To obtain a list of all predefined and custom role names, use the GET /roles method. For information about the predefined and reserved roles, see Creating a custom role in the Lenovo XClarity Administrator online documentation.
privileges	Array of strings	List of URIs that identify the IDs of privileges that are associated with the role (for example, /privileges/3). To obtain a list of all privileges, use the GET /privileges method.
reserved	Boolean	Indicates if the role is reserved and cannot be used to create new role groups or assigned to new users. This can be one of the following values. • **true**. The user role is reserved for use by the XClarity Administrator. • **false**. The user role is not reserved.
result	String	Result of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": [{
      "description": "Operator",
      "id": "702",
      "name": "lxc-operator",
      "privileges": ["/privileges/266","/privileges/203","/privileges/204","/privileges/205",
                     "/privileges/208","/privileges/210","/privileges/213","/privileges/217",
                     "/privileges/220","/privileges/222","/privileges/223","/privileges/160",
                     "/privileges/224","/privileges/225","/privileges/226","/privileges/227",
                     "/privileges/229","/privileges/234","/privileges/235","/privileges/363",
                     "/privileges/236","/privileges/364","/privileges/365","/privileges/110",
                     "/privileges/366","/privileges/111","/privileges/367","/privileges/368",
                     "/privileges/113","/privileges/369","/privileges/371","/privileges/117",
                     "/privileges/118"],
      "reserved": false
   },
   ...,
   {
      "description": "lxc-sysrdr",
```

```
      "id": "714",
      "name": "lxc-sysrdr",
      "privileges": ["/privileges/109"],
      "reserved": true
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```


POST /roles

Use this method to create a custom user role.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/roles`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
description	Required	String	Role description
existingRole	Optional	String	ID of the existing role on which to base the new role. All privileges in this existing role are added to the new role. To obtain the role ID, use the GET /roles method.
name	Required	String	Name of the role. To obtain the names of predefined and custom roles, use the GET /roles method.
privileges	Required	Array of string	List of URIs that identify the IDs of privileges that are associated with the role (for example, /privileges/3) To obtain a list of all privilege IDs, use the GET /privileges method.
reserved	Required	String	Indicates if the role is reserved and cannot be used to create new role groups or assigned to new users. This can be one of the following values. • **true**. The user role is reserved. • **false**. The user role is not reserved.

The following example create a custom role.


```
{
   "description": "A role that allows a user to…",
   "existingRole": "1007",
```

```
   "name": "lxc-admin",
   "privileges": ["/privileges/3","/privileges/5"],
   "reserved": false
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "response": {},
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```

/roles/*{id}*

Use this REST API to retrieve information about a specific user role, modify an existing custom role, or delete a role.

HTTP methods

GET, PUT, DELETE

GET /roles/*{id}*

Use this method to return information about a specific user role.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/roles/{id}`

where *{id}* is the ID of the role to be retrieved. To obtain the role IDs, use GET /roles.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
response		Array of objects	Each array element represents a user role
	description	String	Role description
	id	Integer	Role ID
	name	String	Name of the role. To obtain a list of all predefined and custom role names, use the GET /roles method. For information about the predefined and reserved roles, see Creating a custom role in the Lenovo XClarity Administrator online documentation.
	privileges	Array of strings	List of URIs that identify the IDs of privileges that are associated with the role (for example, /privileges/3). To obtain a list of all privileges, use the GET /privileges method.

Attributes	Type	Description
reserved	Boolean	Indicates if the role is reserved and cannot be used to create new role groups or assigned to new users. This can be one of the following values. • **true**. The user role is reserved for use by the XClarity Administrator. • **false**. The user role is not reserved.
result	String	Result of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "result": "success",
   "response": [{
      "description": "xClarity administrator",
      "id": "706",
      "name": "lxc-admin",
      "privileges": ["/privileges/195","/privileges/132","/privileges/140","/privileges/145",
                     "/privileges/149","/privileges/153","/privileges/155","/privileges/157",
                     "/privileges/160","/privileges/161","/privileges/225","/privileges/226",
                     "/privileges/163","/privileges/227","/privileges/167","/privileges/169",
                     "/privileges/175","/privileges/177","/privileges/179","/privileges/374",
                     "/privileges/183","/privileges/186","/privileges/124","/privileges/127"],
      "reserved": false
   }],
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```

PUT /roles/*{id}*

Use this method to modify an existing custom role. You *cannot* modify a predefined or reserved role

Authentication

Authentication with username and password is required.

Request URL

```
PUT https://{management_server_IP}/roles/{id}
```

where *{id}* is the ID of the role to be retrieved. To obtain the role IDs, use GET /roles.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
description	Optional	String	Role description
id	Required	String	Role ID
existingRole	Optional	String	ID of the existing role on which to base the target role. All privileges in this existing role are added to the target role. To obtain the role ID, use the GET /roles method.
name	Required	String	Name of the role. To obtain a list of all predefined and custom role names, use the GET /roles method. For information about the predefined and reserved roles, see Creating a custom role in the Lenovo XClarity Administrator online documentation.
privileges	Required	Array of strings	List of URIs that identify the IDs of privileges that are associated with the role (for example, /privileges/3). To obtain a list of all privileges, use the GET /privileges method.
reserved	Optional	Boolean	Indicates if the role is reserved and cannot be used to create new role groups or assigned to new users. This can be one of the following values. • **true**. The user role is reserved. • **false**. (default) The user role is not reserved.

The following example modifies a custom role.

```
{
   "description": "A role that allows a user to…",
   "id": "1102",
   "existingRole": "1002",
   "name": "lxc-admin",
   "privileges": ["/privileges/3", "/privileges/5"],
   "reserved": false
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Result of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```

/roleGroups

Use this REST API to retrieve information about all role groups or create a new role group.

HTTP methods

GET, POST

GET /roleGroups

Use this method to return information about all role groups.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/roleGroups`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Each array element represents a role group
description	String	Description for the role group
id	String	ID for the role group
name	String	Name of the role group
reserved	Boolean	Indicates if the role group is reserved and cannot be modified. This can be one of the following values. • **true**. The role group is reserved. • **false**. The role group is not reserved.
roles	Array of strings	List of the roles that are included in the role group. To obtain a list of all predefined and custom role names, use the GET /roles method. For information about the predefined and reserved roles, see Creating a custom role in the Lenovo XClarity Administrator online documentation.
users	Array of strings	List of user IDs that are a members of the role group
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Object	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "result": "success",
   "response": [{
      "description": "Operating System Administrator Group",
      "id": "10ad2fce-4003-46ae-a097-24d786efdada",
      "name": "LXC-OS-ADMIN",
```

```
    "reserved": false,
    "roles": ["lxc-os-admin"],
    "users": []
  },
  {
    "description": "Reserved SYSMGR group",
    "id": "21651293-69db-43f0-8d16-e10bc0173419",
    "name": "LXC-SYSMGR",
    "reserved": true,
    "roles": ["lxc-sysmgr"],
    "users": ["SYSMGR_K5YIQSFY"]
  },
  {
    "description": "Management Server Administrator Group",
    "id": "9e18eb00-df77-4032-886e-d77ebf5ba996",
    "name": "LXC-ADMIN",
    "reserved": false,
    "roles": ["lxc-admin"],
    "users": []
  },
  {
    "reserved": false,
    "description": "Firmware Administrator Group",
    "name": "LXC-FW-ADMIN",
    "id": "48c5134b-51b1-4ebc-b3ac-3f8ebd71029e",
    "roles": ["lxc-fw-admin"],
    "users": []
  },
  {
    "description": "Managed Server and Flex Chassis Administrator Group",
    "id": "1b029de2-302b-4d15-9804-ba680c1a5c21",
    "name": "LXC-HW-ADMIN",
    "reserved": false,
    "roles": ["lxc-hw-admin"],
    "users": []
  },
  {
    "description": "Server and Flex Chassis Discovery and Manage Group",
    "id": "eb6bff01-8858-4738-976d-92f4da15fff8",
    "name": "LXC-HW-MANAGER",
    "reserved": false,
    "roles": ["lxc-hw-manager"],
    "users": []
  },
  {
    "description": "Operator group",
    "id": "be79098d-707e-4338-b9d3-fd658c154ec5",
    "name": "LXC-OPERATOR",
    "reserved": false,
    "roles": ["lxc-operator"],
    "users": []
  },
  {
    "description": "Local User Recovery Group",
    "id": "cc3ec604-e5dc-42c8-8649-1673c9240a3b",
    "name": "LXC-RECOVERY",
    "reserved": false,
    "roles": ["lxc-recovery"],
    "users": []
  },
  {
```

```
      "description": "Security Administrator Group",
      "id": "3667eb91-5101-4fce-9957-3482510f4b47",
      "name": "LXC-SECURITY-ADMIN",
      "reserved": false,
      "roles": ["lxc-security-admin"],
      "users": []
   },
   {
      "description": "service administrator Group",
      "id": "33516e73-992c-4c14-a531-4db9e52bbd62",
      "name": "LXC-SERVICE-ADMIN",
      "reserved": false,
      "roles": ["lxc-service-admin"],
      "users": []
   },
   {
      "description": "Supervisor group",
      "id": "ea967b76-f604-4759-a7f6-8a303ee3de58",
      "name": "LXC-SUPERVISOR",
      "reserved": false,
      "roles": ["lxc-supervisor"],
      "users": ["ADMIN"]
   },
   {
      "description": "Reserved SYSRDR group",
      "id": "42c85103-a6a6-4664-9840-66ae86b83e06",
      "name": "LXC-SYSRDR",
      "reserved": true,
      "roles": ["lxc-sysrdr"],
      "users": ["SYSRDR_NUDCMYXX"]
   }],
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```


POST /roleGroups

Use this method to create a new role group.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/roleGroups`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
description	Optional	String	Description of the role group
name	Required	String	Name of the role group
roles	Required	Array of strings	List of the roles that are included in the role group. To obtain a list of all predefined and custom role names, use the GET /roles method. For information about the predefined and reserved roles, see Creating a custom role in the Lenovo XClarity Administrator online documentation.
users	Optional	Array of strings	List of user IDs that are a members of the role group

Request example

```
{
   "name": "test-group",
   "description": "description",
   "roles": ["lxc-hw-admin", "lxc-fw-admin"],
   "users": ["USER1", "USER2", "USER3"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
result		String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages		Array of objects	Information about one or more messages
	id	String	Message identifier of a returned message
	text	String	Message text associated with the message identifier
	explanation	String	Additional information to clarify the reason for the message
	recovery	Array of objects	Recovery information

Attributes	Type	Description
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

/roleGroups/*{id}*

Use this REST API to modify properties for that role group.

HTTP methods

PUT

PUT /roleGroups/*{id}*

Use this method to modify a specific role group.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/roleGroups/{id}`

where *{id}* is the ID of the role group. To obtain role group ID, use GET /roleGroups.

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
description	Optional	String	Description of the role group
name	Optional	String	Name of the role group

Attributes	Re-quired / Optional	Type	Description
roles	Required	Array of strings	List of the roles that are included in the role group. To obtain a list of all predefined and custom role names, use the GET /roles method. For information about the predefined and reserved roles, see Creating a custom role in the Lenovo XClarity Administrator online documentation.
users	Optional	Array of strings	List of user IDs that are a members of the role group

The following example modifies a specific role group.

```
{
   "name": "test-group",
   "description": "description",
   "roles": ["lxc-hw-admin", "lxc-fw-admin"],
   "users": ["USER1", "USER2", "USER3"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
```

```
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```


/roleGroups/*{name}*

Use this REST API to retrieve information about a specific role group or delete a role group.

HTTP methods

GET

GET /roleGroups/*{name}*

Use this method to return information about a specific role group.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/roleGroups/{name}`

where <*name}* is the name of the role group. To obtain role group name, use GET /roleGroups.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	Each array element represents a role group
description	String	Description for the role group
id	String	System-assigned identifier for the role group
name	String	Name of the role group

Attributes	Type	Description
reserved	Boolean	Indicates if the role group is reserved and cannot be modified. This can be one of the following values. • **true**. The role group is reserved. • **false**. The role group is not reserved.
roles	Array of strings	List of the roles that are included in the role group. To obtain a list of all predefined and custom role names, use the GET /roles method. For information about the predefined and reserved roles, see Creating a custom role in the Lenovo XClarity Administrator online documentation.
users	Array	List of all user IDs that are members of the role group
result	String	Result of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": {
      "description": "Operator group",
      "id": "896726ab-6b96-4d50-8678-e97a9059a784",
      "name": "LXC-OPERATOR",
      "reserved": false,
      "roles": ["lxc-operator"],
      "users": []
   },
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```

DELETE /roleGroups/*{name}*

Use this method to modify a specific role group.

Notes:
- You cannot delete role groups that have members (users).
- You cannot delete the reserved role groups **lxc-sysrdr** and **lxc-sysmgr**.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/roleGroups/{name}`

where <*name}* is the name of the role group. To obtain role group name, use GET /roleGroups.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
```

```
    }]
}
```

/ssoSettings

Use this REST API to retrieve and modify client settings when an external SAML 2.0 identity provider is used for authentication.

HTTP methods

GET, PUT

GET /ssoSettings

Use this method to return information about the client settings when an external SAML 2.0 identity provider is used for authentication.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/ssoSettings`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
samlEnabled	Boolean	Indicates whether an SAML identity provider is used for authentication. This can be one of the following values. • **true**. SAML identity provider is used. • **false**. An SAML identity provider is not used.
spMetadataAttributes	Object	Information about the SAML service provider metadata.
entityId	String	The service provider base URL as the unique identifier of the service provider.
signMetadata	Boolean	Indicates whether the generated metadata is digitally signed. This can be one of the following values. • **true**. Metadata must be signed. • **false**. Metadata can be unsigned.

Attributes	Type	Description
signingAlgorithm	String	The algorithm that is used to create digital signature on the metadata object. This can be the following value: • **sha1**
signAuthenticationRequests	Boolean	Indicates whether authentication requests are signed. This can be one of the following values. • **true**. Authentication requests are signed. • **false**. Authentication requests are not signed.
requireSignedAuthenticationResponse	Boolean	Indicates whether authentication responses are signed. This can be one of the following values. • **true**. Authentication responses are signed. • **false**. Authentication responses are not signed.
requireSignedArtifactResolution	Boolean	Indicates whether the signing of artifact resolution requests sent to the remote identity providers is enabled. This can be one of the following values: • **true**. Signing of artifact resolutions is enabled. • **false**. Signing of artifact resolutions is disabled.
spMetadata	String	SAML service provider metadata that was generated by Lenovo XClarity Administrator.
idpMetadata	String	SAML identity provider metadata that was retrieved from ADFS.

The following example is returned if the request is successful.

```
{
   "samlEnabled":true,
   "spMetadataParameters":{
      "entityId":"10.243.2.124",
      "signMetadata":true,
      "signingAlgorithm":"sha1",
      "signAuthenticationRequests":true,
      "requireSignedAuthenticationResponse":true,
      "requireSignedArtifactResolution":true
   },
   "spMetadata":"SP metadata xml ",
   "idpMetadata":"IDP metadata xml"
}
```

PUT /ssoSettings

Use this method to modify the client settings when an external SAML 2.0 identity provider is used for authentication. The identity provider must be Microsoft Active Directory Federated Services (AD FS) and must reside on a server that is connected to the management network.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/ssoSettings`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
samlEnabled	Optional	Boolean	Indicates whether an SAML identity provider is used for authentication. This can be one of the following values. • **true**. SAML identity provider is used. • **false**. An SAML identity provider is not used.
spMetadataAttributes	Optional	Object	Information about the SAML service provider metadata.
entityId	Required	String	The service provider base URL as the unique identifier of the service provider.
signMetadata	Required	Boolean	Indicates whether the generated metadata is digitally signed. This can be one of the following values. • **true**. Metadata must be signed. • **false**. Metadata can be unsigned.
signingAlgorithm	Required	String	The algorithm that is used to create digital signature on the metadata object. This can be the following value: • **sha1**
signAuthenticationRequests	Required	Boolean	Indicates whether authentication requests are signed. This can be one of the following values. • **true**. Authentication requests are signed. • **false**. Authentication requests are not signed.
requireSignedAuthenticationResponse	Required	Boolean	Indicates whether authentication responses are signed. This can be one of the following values. • **true**. Authentication responses are signed. • **false**. Authentication responses are not signed.
requireSignedArtifactResolution	Required	Boolean	Indicates whether the signing of artifact resolution requests sent to the remote identity providers is enabled. This can be one of the following values: • **true**. Signing of artifact resolutions is enabled. • **false**. Signing of artifact resolutions is disabled.
idpMetadata	Optional	String	SAML identity provider metadata that was retrieved from ADFS.

The following example modifies an external SAML 2.0 identity provider client.

```
{
    "samlEnabled":true,
    "spMetadataParameters":{
        "entityId":"10.243.2.124",
        "signMetadata":true,
```

```
        "signingAlgorithm":"sha1",
        "signAuthenticationRequests":true,
        "requireSignedAuthenticationResponse":true,
        "requireSignedArtifactResolution":true
    },
    "idpMetadata":"IDP metadata xml"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "failure",
    "messages": [{
        "explanation": "The request to change the SAML  configuration could not complete for an unknown
                        reason.",
        "id": "FQXHMSE0611J",
        "recovery": {
            "text": "Specify valid parameters on the request and try the request again. If the problem
                     persists, contact Support.",
            "URL": ""
        },
        "text": "The request to change the SAML  configuration could not be completed successfully."
```

```
    }]
}
```

/serverCertificate

Use this REST API to generate a self-signed certificate and download a certificate.

HTTP methods

GET, PUT

GET /serverCertificate

Use this method to download the server certificate in PEM format.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/serverCertificate`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information

Attributes		Type	Description
	text	String	User actions that can be taken to recover from the event
	URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
-----BEGIN CERTIFICATE-----
MIIFRjCCBC6gAwIBAgIVAOYU3FiQqz7RQ+KehCLhan3h+le4MA0GCSqGSIb3DQEB
CwUAMHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4G
A1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5IFNlcnZlciBGaXJt
d2FyZTEjMAcGA1UECxMAMQ0wCwYDVQQDEwRMWENBMCAXDTcwMDEwMTA1MDAwMFoY
DzIwNzAwMTAxMDQ1OTU5WjCBkDELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRo
IENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdoMQ8wDQYDVQQKEwZMZW5vdm8xDDAK
BgNVBAsTA0VCRzE3MDUGA1UEAxMuR2VuZXJhdGVkIGJ5IExlbm92byBTeXN0ZWOg
TWFuYWdlbWVudCBTb2Z0d2FyZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAIHSk5uFESdIg2jz3p2EuMtT2bLXPOQLG4wzhKzp4es3HMne7sXfhZ3kYYoU
DjTtA8tV2t1z8lQdol3pVeJdA4rb2gO8s6kgtR/F+GgJbSGQUlTWuLNXT3zwAsCO
kipJBoZO1r3oYCJdUkgCvCOVMFDIyILyhSejsXXny5aFacl7OVJhATk7fEkEy3HH
4PdcB7UvJpaLwAUyMJtKr3ZST2K71BPMTNCraOyK42qiR6tUBhxuGraiuk6niMUn
XUPf81kCLmXVI96G3/YcMT9+4orooaXmFCtXz3g3ZJ9nZxzntgH2BcpQgnIGQ1Gm
NUw9HK3bOrLI7xNJuOkTCSA6Yt8CAwEAAaOCAakwggGlMAwGA1UdEwEB/wQCMAAw
gbYGA1UdIwSBrjCBq4AUbhZrZRZDulpKYG3OgI2t1Bn8AFmhfaR7MHkxCzAJBgNV
BAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBxMHUmFsZWln
aDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5IFNlcnZlciBGaXJtd2FyZTEJMAcGA1UE
CxMAMQ0wCwYDVQQDEwRMWENBghRWKEwW81vplOg538WZJ7uxaygc2PzAdBgNVHQ4E
FgQUogeZxr9VEeeU5T8ELvS8lAW7MdOwgbwGA1UdEQSBtDCBsYcQ/oAAAAAAAAAK
ACf//sOOg4IeZmU4MDowOjA6MDphMDA6MjdmZjpmZWNkOmU4MyUyhwQK8Ynggg4x
MC4yNDEuMTM3LjIyNIcQAAAAAAAAAAAAAAAAAAAAAYIJbG9jYWxob3NOhwR/AAAB
gglsb2NhbGhvc3SCCWxvY2FsaG9zdIIuR2VuZXJhdGVkIGJ5IExlbm92byBTeXNO
ZWOgTWFuYWdlbWVudCBTb2ZOd2FyZTANBgkqhkiG9w0BAQsFAAOCAQEArHLB5QR2
Hn+RWIGfA4uYrIgD2tJvtkbE9uVXF/8s8HvNQ+fGIFZEdnuqjIXcxBAUq9xwapvj
PbDRgjzca/tl3xxvPQ9XW9jt9RdPAcn+TbxzlhnPTOydqoYy+Rfd2sGL1GgOn7GR
nxrlR+JWVGd7f3j8lPK3jO5JKThpUW+PrECZwbM9wgJ4wNF6xmHqLOiCWznqhtUd
ytp7aYmGuj4h53hyJeqzlBXQA1Kd5AhB2/3cpbO2lgB4av+stGHn2WzPER5jbRF/
q5Up7/5UhA2wSQaOVap41O9XQqXQL8p5VxpPDlumhothguqgN4yOfVxF4pGytOqX
W+IcyiYy15ufNA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID1TCCAr2gAwIBAgIUVihMFvNb6ZdIOd/FmSe7sWsnNj8wDQYJKoZIhvcNAQEL
BQAweTELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYD
VQQHEwdSYWxlaWdoMSUwIwYDVQQKExxHZW5lcmF0ZWQgYnkgU2VydmVyIEZpcm13
YXJlMQkwBwYDVQQLEwAxDTALBgNVBAMTBExYQ0EwIBcNNzAwMTAxMDUwMDAwWhgP
MjA3MDAxMDEwNDU5NTlaMHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBD
YXJvbGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5
IFNlcnZlciBGaXJtd2FyZTEJMAcGA1UECxMAMQ0wCwYDVQQDEwRMWENBMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuFx2YjVCCAKa2Sp5QpxdmCS8R8GI
l/92LyK37HySwKgaTSm9nxkQt2paZUg+NzMqOAbOmTwmVOT8/eGbtWFmWyqeFGr4
5m+MC3KhxOjrhOzQyRzrbmIOprgW1LSbDwRRon5k4efXhcvfmrNGoXHkGysMLOCZ
+bRk9XCjm+EFjwaW28pTHE8XfdMJD1zxy467vJQ9AOVNSh7YYflKw1jV73xMYiV9
tNbAADFCUT5RHicXxgF8huyKcJCHppiH9z6DqEOtgOZfeXqQJHmW5udweVmt646s
HEGNrCqmntAQcASIzDVfgYKm1dQn+mQAH5FJ/jyjnqjhP7AFIoneXOLYkwIDAQAB
o1MwUTAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRuFmtlFkO6WkpgbfSAja3U
GfwAWTAfBgNVHSMEGDAWgBRuFmtlFkO6WkpgbfSAja3UGfwAWTANBgkqhkiG9w0B
AQsFAAOCAQEAHa/w2SNQkSpAtoEnHZpDpZrThpNeeQxPMX2+Us2QxOa4Wr8WditB
9sK89inebkRSZxBTsZNKf4w1XT2TlND5mY88K4rQ15YZdLSJvaKr9QmKSbmBKWeT
dcOX5HLaB8evP4EoOC32BXvklx+SnNtZHupcXo8JfmC38Hxftpn8ZfiAfiYr4jZI
iIom6Zupxoc7ZuyAWOovp4V5jKmglWDM4xXRTDsYcHEOpnGOry+MlPEAszDexYd8
HNdO2BliTsytll6RsSoJ6B9gu49OOcSRYpp543azUDStsoJ8a/8CfyeGMje6aREg
tOumP61rQlEYyUmEcEr/eDZt8pjXiR/txw==
-----END CERTIFICATE-----
```

PUT /serverCertificate

Use this method to generate a self-signed server certificate.

Important: You are disconnected from XClarity Administrator for a short period of time during this request.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/serverCertificate`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
CommonName	Required	String	The name of the certificate owner. Typically, this is the fully-qualified domain name (FQDN) or IP address of the server that is using the certificate (for example, `www.domainname.com` or `10.15.23.99`). The length of this value cannot exceed 63 characters. The default is xHMC.
Country	Required	String	The two-letter ISO 3166 code for the country or region of origin associated with the certificate organization (for example, `US for the United States`). The default is US.
Organization	Required	String	The organization (company) that will own the certificate. Typically, this is the legal incorporate name of a company. It should include any suffixes, such as Ltd., Inc., or Corp (for example, `ACME International Ltd.`). The length of this value cannot exceed 60 characters. The default is generated by the server firmware.
OrganizationUnit	Required	String	The organizational unit that will own the certificate (for example, `ABC Division`). The length of this value cannot exceed 60 characters. The default is None.
StateLocality	Required	String	Full name of the locality (city) to be associated with the certificate (for example, `San Jose`). The length of the value cannot exceed 50 characters. The default is Raleigh.
StateProvince	Required	String	Full name of the state or province to be associated with the certificate (for example, `California` or `New Brunswick`). The length of this value cannot exceed 60 characters. The default is North Carolina.

Attributes	Re-quired / Optional	Type	Description
notBefore	Optional	String	The UTC date and time before which the created certificate is not valid. Specify the date and time in ISO 8601 format `YYYY-MM-DDTHH:MM:SSZ` (for example, 2017-01-25T18:00:00Z or 2017-01-25T12:00:00-0600). If not specified, the value that is used for the certificate generation is the most recently specified *notBefore* date. If the date has never been specified, the default is 1970-01-01T00:00:00Z.
notAfter	Optional	String	The UTC date and time after which the created certificate is not valid. Specify the date and time in ISO 8601 format`YYYY-MM-DDTHH:MM:SSZ` (for example, 2017-01-25T18:00:00Z or 2017-01-25T12:00:00-0600). If not specified, the value that is used for the certificate generation is the most recently specified *notAfter* date. If the date has never been specified, the default 2069-12-31T23:59:59Z.

The following example generates a self-signed server certificate.

```
{
   "CommonName": "LXCA",
   "Country": "US",
   "Organization": "Generated by Server Firmware",
   "OrganizationUnit": "Organization unit",
   "StateLocality": "Raleigh",
   "StateProvince": "North Carolina",
   "notBefore": "2017-06-01T12:30:00Z",
   "notAfter": "2018-06-01T12:30:00Z"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

/serverCertificate/tmp

Use this REST API to upload a new signed certificate to Lenovo XClarity Administrator and creates a job to send the new certificate to all managed devices.

HTTP methods

POST

POST /serverCertificate/tmp

Use this method to uploads a new signed server certificate to Lenovo XClarity Administrator and provisions the new certificate to all managed devices.

When a self-signed certificate is generated and, a job is created to provision the new certificate to all managed devices. Use the GET /serverCertificate/jobs/*{job_id}* method to retrieve the job status and additional job details. If a job was not successfully started, refer to the response code and response body for details.

Note: If the CA chain that you are importing has the same certificate as a CA certificate that is already installed, the CA certificate is not sent to all management devices and no job is created.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/serverCertificate/tmp`

Query parameters

None

Request body

Parameters	Required / Optional	Type	Description
action	Optional	String	Action to take. This can be one of the following values. • **import**. Imports the new certificate. This is the default value. • **resume**. Resumes installation.
{server_certificate}	Required	String	Server certificate in PEM forma The certificate to be uploaded must have been created from the certificate signing request using the GET /certificateSigningRequest or downloaded from the XClarity Administrator user interface.

Request example

```
----------------------------269032580128512  Content-Disposition
: form-data; name="uploadedfile"; filename="cert_chain.pem"  Cont
ent-Type: application/octet-stream   -----BEGIN CERTIFICATE-----
MIIF8TCCA9mgAwIBAgIJAPCc8OvvkTPlMA0GCSqGSIb3DQEBBQUAMIGOMQswCQYD
VQQGEwJVUzESMBAGA1UECAwJTWlubmVzb3RhMRIwEAYDVQQHDAlSb2NoZXN0ZXIx
EzARBgNVBAoMCnhITUMgTWFrZXIxCzAJBgNVBAsMAklTMRAwDgYDVQQDDAdUZXN0
IENBMSMwIQYJKoZIhvcNAQkBFhRwa2lhZG1pbkBleGFtcGxlLmNvbTAeFw0xNTAz
MDIyMDEwMDNaFw0yNTAyMjcyMDEwMDNaMIGOMQswCQYDVQQGEwJVUzESMBAGA1UE
CAwJTWlubmVzb3RhMRIwEAYDVQQHDAlSb2NoZXN0ZXIxEzARBgNVBAoMCnhITUMg
TWFrZXIxCzAJBgNVBAsMAklTMRAwDgYDVQQDDAdUZXN0IENBMSMwIQYJKoZIhvcN
AQkBFhRwa2lhZG1pbkBleGFtcGxlLmNvbTCCAiIwDQYJKoZIhvcNAQEBBQADggIP
ADCCAgoCggIBAMjv1twlYnr2r4lcXOMtIhHRmCjx5x9IPsm8ymaO28MgwHRaxDUE
Peu2NuCJobHg1kcLyIHNPZriWXY2D4tZsYstGLNPCxLYGkJgBwGSW3KDnr4//OxF
/ftXt6kXi/Sb7ErFAuw7zKmCORlOioU15LM1Vt4oKVJkTlOEOvKs4tlY8gB/vfaJ
wLOizJn7f/LQDccE/KBHN+6jtUgTNUDOMZprLMojdc+QLe2P2nW3NamdJh9Hc64t

... certificate contents here ...

N/vYEzL5ll9ODUcvIfZkOESgMoZOHwKUndizfFuplSR2iXlIdUAoqZ1LAgMBAAGj
UDBOMB0GA1UdDgQWBBS7M179cu/wanOCqJMM7+6eM18AozAfBgNVHSMEGDAWgBS7
M179cu/wanOCqJMM7+6eM18AozAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUA
A4ICAQCyDeLKYJeK85amA36yiO8pOWC+EgKhA7MhzAij+/yoprofLQO1+ovSuOHQ
jpjh7s67OlIZC6+4Oo7sntk1fjQHoSpoE2B3/dmXMtxkRDTp1Z2kJaaOoV1dmEkM
23l8M1vZONTy9vb4STxFUBxQ9wEKA7aNKBHnUnwZu3HOeQ6lzOOf7ZRlGANIT2mR
NsxIPVcjXZcqsK5s1l+CSEOhjAPBsBnhSYYPDC8Z+OjtztljwuIcODO8tgr3NZZ/
4NRMCugAZLQU1CcdQKwgQA5OYIQM1yFzFl6U61PNOQefWE3tb/Ov7tFmMf7EAQbU
wkjsQUrlQakAFJUJ9Sosb1Q/p8VoMY5f52coEI/AzV8cO5t59NHHPInOgF/S9l1v
vBCO4J+lPyVxVdKnwS2EpIWRSMgwbb1Iz1pTyexBBVi3NzC5R1oaZKHsLGmbC1Hh
B5HHZcEBOzUQtJjnEVeLTAGCQiPQzMv8OxI+dWRgIdutKZoIB5xMCXhFyXCgGUPj
```

```
SkGjoFJL46mqE5u+qqdv1a6lKy+KDBkQg4J4hyjGOf4Y/YPkoszVy9jRaeImE5Bi
R56ttIkp4K5yCCJVNT8Wou8b8hYh1qYUGLs+jOixs5rtbbGAVCntjOhbFEiC5obL
1l8DIOHqZiX6XnRTwIjOZq+JJYMdc1ikM+j/C5oN5TVb7cHlFA==  -----END CE
RTIFICATE-----  -----BEGIN CERTIFICATE-----  MIIF4zCCA8ugAwIBAgICE
AAwDQYJKoZIhvcNAQEFBQAwgY4xCzAJBgNVBAYTAlVT  MRIwEAYDVQQIDAlNaW5u
ZXNvdGExEjAQBgNVBAcMCVJvY2hlc3RlcjETMBEGA1UE  CgwKeEhNQyBNYWtlcjE
LMAkGA1UECwwCSVMxEDAOBgNVBAMMB1Rlc3QgQOExIzAh  BgkqhkiG9w0BCQEWFH
BraWFkbWluQGV4YW1wbGUuY29tMB4XDTEwMDEwMTEyMDAw  MFoXDTI1MDIyNzIwM
TQyMVowgYcxCzAJBgNVBAYTAlVTMRIwEAYDVQQIDAlNaW5u  ZXNvdGExEzARBgNV
BAoMCnhITUMgTWFrZXIxCzAJBgNVBAsMAklTMROwGwYDVQQD  DBRUZXNOIEludGV
ybWVkaWFOZSBDQTEjMCEGCSqGSIb3DQEJARYUcGtpYWRtaW5A  ZXhhbXBsZS5jb2
OwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDBHJXF  IJWrcN3O7O5yS
NOfpkW7psgYddhn5vJzsyqMBTDR9gO7oIeI+YLkD2Za414Bl8mO  zxEizsOl8YiY
dASh5UF2zsiKt1o9FkNprdqTfAjEbq/gNDOe8ju6c/DTE2KFsuI3  8U2xSSuarAn
+QGHq186pXPwY7r3MkY6adiiOOYylbr2a7qzEfCmQavh3FpsUJ4+x
 QqJUXsfrcEd5sQwYXP/uyAvucONlz/1nmomoVC+YSaVX7tfzLlaZ4jZe2kamNRAf
 W1elXOohVa8j6SqS53IHuUXIgb+DQyqoIXb9DdceyQcOwdObAUOcRCuKA7Jj+e1P
 cgUnlxMapOlUQ9pRJjn9enPIauO1IjREFvKxfr3hajHLg26q4uoS2dJJhlTDGEnb
 C1lZf+/FBOkFk+vdjXDdq/5Kl4RrKOaX5uQhHVb6sYBafhjQ/QIpSAyUrFcANInE
 AOzn9GpBSgcacJYI4k86BYjEkgKoALqoTShLRk2Go3rpIIpOYpVP81saT1xOuCAX

 ...certificate contents here ...

 vdLkS4Bw+vmMYbR6MSA9HqToDcOl2TbAjttGImlg7K7HFHybIp4QnofrdYJ7fbwV
 bmoKLOQL6OwXOefqp7r6eKIP+uYNVEYr4gXvYUn+PPqZaViRTrhIuWUQydQApeI7
 RAaypfTGvUy8f3ezpR8+JHr+Yp4AbQeLmqJU7LgCI6fbGdVK8fwlYNsOYbCmyrcq
 EKMlRjc15pBp7ZGm/zxErn9c+CK6c+s=  -----END CERTIFICATE----- -----
BEGIN CERTIFICATE-----  MIIFyDCCA7CgAwIBAgICEAIwDQYJKoZIhvcNAQEFB
QAwgYcxCzAJBgNVBAYTAlVT  MRIwEAYDVQQIDAlNaW5uZXNvdGExEzARBgNVBAoM
CnhITUMgTWFrZXIxCzAJBgNV  BAsMAklTMROwGwYDVQQDDBRUZXNOIEludGVybWV
kaWFOZSBDQTEjMCEGCSqGSIb3  DQEJARYUcGtpYWRtaW5AZXhhbXBsZS5jb2OwHh
cNMTAwMTAxMTIwMDAwWhcNMjUw  MjI3MjEwMzI1WjB5MQswCQYDVQQGEwJVUzESM
BAGA1UECBMJTWlubmVzb3RhMRIw  EAYDVQQHEwlSb2NoZXNOZXIxJTAjBgNVBAoT
HEdlbmVyYXRlZCBieSBTZXJ2ZXIg  RmlybXdhcmUxCzAJBgNVBAsTAk9VMQ4wDAY
DVQQDEwVMWENBMjCCASIwDQYJKoZI  hvcNAQEBBQADggEPADCCAQoCggEBALoiw8
KeONj2+8xNrXlUs1CK5h7uAksVf1d4  +34UqdVOVeM89NjG6I4g9s8+c46ugRxXC
AnsLDWAdHqNcMz+VAc7Avn68BqwWkMF  mzboe7sgbOBK5ALEBruH+sashz84m/DX
NDCqXSg8FndU45z9OpRsTAHCSC9i4DtO  AMo6vgB3Mq9O/IyfrZcd+IhPZIhOTwO
brPssNXHJOINRwLQ7orUOaeoi3hggkobX  LmPm6pmMqVFeSvpaGKVOXPSANvE68D
f3SZv9U9aAzg6jlehwn+CqzYmXkoIHWRIh  SOjvsV2SqAjVTHJJqZwOqFbS9BSQL
/hNT98ad/AFdUOkI7VgNCsCAwEAAaOCAUkw  ggFFMAkGA1UdEwQCMAAwEQYJYIZI
AYb4QgEBBAQDAgZAMAsGA1UdDwQEAwIF4DAw  BglghkgBhvhCAQOEIxYhT3BlblN
TTCBHZW5lcmF0ZWQgUOFOIENlcnRpZmljYXRl  MBOGA1UdDgQWBBRYUEiNjENDqU
5FNClJxYOjK+6jqzAfBgNVHSMEGDAWgBRWpDFJ  Hnw3CSSeR1O2WOAlepPskzCBp
QYDVRORBIGdMIGahxD+gAAAAAAAAAoAJ//+njAT  gh9mZTgwOjA6MDowOmEwMDoy
N2ZmOmZlOWU6MzAxMyUyhwQK8Yn6giBpcDEwLTIO  MSOxMzctMjUwLmxhYnMubGV
ub3ZvLmNvbYcQAAAAAAAAAAAAAAAAAAAAAYIJbG9j  YWxob3NOhwR/AAABgglsb2
NhbGhvc3SCCWxvY2FsaG9zdIIETFhDQTANBgkqhkiG  9w0BAQUFAAOCAgEAcm34H
7jhHFNqduuStMOY5FTkSFpJ1EdUDs5FEYh93PHNofCa  OIPb45ANeKq1KxmE4KTZ
lTrqiHKNcomEcwht2JlFfrqCq5oS4UoTOPtt278ScVHr  BTS1QTIKdLa/A2t5R89
WVVSIqRfPfjuRbrCMVTYBKSzQkv8LwIOF7C+Rq94IhQT2  jGJKilTg1qrFgOJxp7
sZSaYauhbUsedh6p3QZVl12NqJq/RezUOhQr4bAmnzJfv6  5UO2bU5i85HQFBokq
3sx8lkNeWgnPWWARrRDDdfTErrirpEBCodwMSbcE25Jo2Kw  HyJYZy/S7GnnNvVP
aGabPhE2ztIubKo5lYPEgvxJldEmbxZ5u8LN3rcSjeOtvM7u  Gb/xYPiyH89ptHR
G+XnwK1fxapCeiIjQbK9exvXIOsXFJulIKIrPpch/+QHjZK7H  AQjVUVfV5vM+62
2U1tdwmj7PlAyYXjBpZYTOwhnNT1RUFypy5VOZr2/D/1rCrgCy  uNodqiPkeQzfk
5xE8Sxq1Zkw/I6c9O5g222g3lY3Lr88u9+8Q5f1NlQpqc5wDaiw  qoX92ToEHWdz
+z7V6NhlXlhASOPmBWPPmQg+yOoeYmKlOw71AEk1R6dYSzZoxr9b  5H4ITTC3kQZ
Qn4vR9+QWvVzQSMZ7xubiSo3DrahV81pYWXcSsYVJ+3C53vM=  ---
--END CERTIFICATE-----  ------------------------------269032580128
512--
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	Response content. This attribute is provided only if the CA that is specified in the certification chain is new and **returnJobInfo="true"** is specified in the request.
jobPath	String	A URI in the form /serverCertificate/jobs/*{job_id}* (for example, `/serverCertificate/jobs/383`) that represents the job that is monitored by the management server. You can use GET /serverCertificate/jobs/*{job_id}* to determine the status of the job. If a job was not successfully started, refer to the response code and response body for details. This is the same URI that is included in the response header. If no job was created, this attribute is empty.
result	String	The results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages.
explanation	String	Additional information to clarify the reason for the message.
id	String	The message identifier of a returned message.
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event.
URL	String	Link to the help system for more information, if available.
text	String	Message text associated with the message identifier.

The following example is returned if the request is successful.

```
{
    "response": {
        "jobPath": "/serverCertificate/jobs/383"
    },
    "result": "success",
    "messages": [{
        "explanation": "The existing server certificate has been replaced by the new certificate",
        "id": "FQXHMSE0134I",
        "recovery": {
            "text": "Information only; no action is required.",
```

```
            "URL": ""
        },
        "text": "The request to upload new server certificate was successful.",
    }]
}
```


/serverCertificate/details

Use this REST API to retrieve detailed information about the server certificate.

HTTP methods

GET

GET /serverCertificate/details

Use this method to returnd detailed information about the server certificate. The certificate is returned in PEM format.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/serverCertificate/details`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	Information about each certificate
certificate	String	Certificate, in PEM format
issuerDn	String	LDAP Distinguished Name of the issuer (for example, `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`).
notAfter	String	Timestamp when the certificate is no longer valid. The timestamp is returned in ISO 8601 format (for example, `2014-02-05T15:54:13Z`).
notBefore	String	Timestamp when the certificate becomes valid. The timestamp is returned in ISO 8601 format (for example, `2014-02-05T15:54:13Z`).

Attributes		Type	Description
	serialNumber	String	Serial number of the certificate
	signatureAlgorithm	String	Algorithm used to sign the certificate (for example, "MD5withRSA","SHA256withRSA").
	status	String	Certificate status. This can be one of the following values. • **internal**. The server certificate was signed by an internal Certificate Authority. • **external**. The server certificate was signed by an external Certificate Authority.
	subjectDn	String	LDAP Distinguished Name of the subject (for example, "CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU").
{message_attributes}		*varies*	Status messages (see Status messages).

The following example is returned if the request is successful.


```
{
   "response": [{
      "certificate": "-----BEGIN CERTIFICATE-----\r\n
                     MIIF2jCCBMKgAwIBAgIVAJgbWgQ/HUsaEEkFEdueK2lEONxqMA0GCSqGSIb3DQEB\r\n
                     CwUAMHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3JOaCBDYXJvbGluYTEQMA4G\r\n
                     A1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5IFNlcnZlciBGaXJt\r\n
                     d2FyZTEJMAcGA1UECxMAMQ0wCwYDVQQDEwRMWENBMCAXDTcwMDEwMTA2MDAwMFoY\r\n
                     DzIwNzAwMTAxMDU1OTU5WjB5MQswCQYDVQQGEwJVUzEXMBUGA1UECBMOTm9ydGgg\r\n
                     Q2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxJTAjBgNVBAoTHEdlbmVyYXRlZCBi\r\n
                     eSBTZXJ2ZXIgRmlybXdhcmUxCTAHBgNVBAsTADENMAsGA1UEAxMETFhDQTCCASIw\r\n
                     DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIRVJvuGU11o9Do/bjQvTbWaSXS9\r\n
                     tFPhg/JyZP5q9RYlCfgRveh1nArAAO7t2XZMLC2l5Cv6kmbQUPsTVQLs2JetmnLS\r\n
                     IpUwOuIwgV448OIl5jF7x4Wx4sDvPSTy9DnbeLUGOPV5zkwNLv8wVGe7eTTWGG2i\r\n
                     SGozfBCuwDc2MO6WJPhDiZhBf+CU/d27P3oIDxNUa6NJkfI3CI6sivpTfpT8oHdB\r\n
                     P4PIdKJ4VGmhO72bHCOvFaOm4C/eip5h5rskJmw5DHeiujp7nq9o+qOQYLST8mNU\r\n
                     IGuQ+12+s/4JYz2hZAFOtRmPbnmD8YSVPVKP67jYYsQziBn7jNtBS7oOOeUCAwEA\r\n
                     AaOCAlUwggJRMAwGA1UdEwEB/wQCMAAwgbYGA1UdIwSBrjCBq4AUeTimSPAWXgpz\r\n
                     6+pN33JKZ3zks2KhfaR7MHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3JOaCBD\r\n
                     YXJvbGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5\r\n
                     IFNlcnZlciBGaXJtd2FyZTEJMAcGA1UECxMAMQ0wCwYDVQQDEwRMWENBghQX6Oe/\r\n
                     U7Ai3C78CGAhNptbHBF49TAdBgNVHQ4EFgQU/lKzmh6UpXDOdSTFmZk6Z9VRSPYw\r\n
                     ggFnBgNVHREEggFeMIIBWocEfwAAAYIJMTI3LjAuMC4xhxAAAAAAAAAAAAAAAAAA\r\n
                     AAABgg8wOjA6MDowOjA6MDowOjGHEP6AAAAAAAAAAOAAAAAAAACCFmZlODA6MDow\r\n
                     OjA6ZTA6MDowOjAlMTCHEP6AAAAAAAAAKePrsll+T/+CIWZlODA6MDowOjA6Mjll\r\n
                     MzplYmIyOjU5N2U6NGZmZiUxMocECipk3oIaRFJBSO5FUlVELThMRjBOLmxlbm92\r\n
                     by5jb22HEP6AAAAAAAAA4VspLzmOURiCGkRSQUtORVJVRCO4TEYwTi5sZW5vdm8u\r\n
                     Y29thxD+gAAAAAAAAFXfh6O5j+bqgiFmZTgwOjA6MDowOjU1ZGY6ODdhZDozOThm\r\n
                     OmU2ZWElMTaHEP6AAAAAAAAAABe/goqZN6CHWZlODA6MDowOjA6MDo1ZWZlOmEy\r\n
                     YTo2NGRlJTE3gglsb2NhbGhvc3SCBExYQOEwDQYJKoZIhvcNAQELBQADggEBAJRj\r\n
                     k88tQx4IitOQ7HpmyjOE9W4ilvVTGZ9Zk56gN2lPWY/m2TL1RLbiid/cWpy6RnNd\r\n
                     PGbO1whRmwTpq5Ihec6wdONLXZFlS5GaOqMu+opzXnwvuGBn1y/jQjnpIV+TcKQL\r\n
                     9LAvzmPoMYd8BqF/sfR1rdmgyGeTzG/yUEaChXGOTLkbkT+9gYFN/gPDy4hAv2i9\r\n
                     zLQnCXsqH5ZIDRAf42P8uHZ6hBkgra/vXdh+rB9mgIJZV2ijgjoYl6bIGw+9zL3L\r\n
                     t2Jfh2u4MCpQs47FVZ2Fds3YaprHf5SVamUspTIOdsNzFU1F/xa2NRaWzu3T5+mj\r\n
                     JOHNoKWv4KcJXzyXuLo=\r\n
                     -----END CERTIFICATE-----\r\n",
      "is   suerDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
      "notAfter": "2070-01-01T05:59:59Z",
      "notBefore": "1970-01-01T06:00:00Z",
      "serialNumber": "981b5a043f1d4b1a10490511db9e2b694438dc6a",
      "signatureAlgorithm": "SHA256withRSA",
      "status": "internal",
```

```
        "subjectDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US"
    }],
    "result": "success",
    "messages": [{
       "id": "FQXHMSE0001I",
       "text": "The request completed successfully."
       "explanation": "",
       "recovery": {
          "text": "Information only; no action is required.",
          "URL": ""
       },
    }]
}
```


/serverCertificate/jobs

Use this REST API to retrieve information about all known jobs for provisioning signed server certificates to managed devices.

HTTP methods

GET

GET /serverCertificate/jobs

Use this method to return information about all known jobs for provisioning signed server certificates to all managed devices.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/serverCertificate/jobs`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Response content
progress	Double	Percentage complete of the job. This can be one of the following values. • **0**. Created • **50**. In progress. • **100**. Complete.

Attributes	Type	Description
result	Array	Information about the job results. There is one entry for each managed device on which cryptographic settings are being changed.
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageID	String	Message ID for the set of job tasks
messageAttributes	String	UUID that is associated with the job
progress	Long	Percentage complete of the job. This value can be `0 -100`
result	String	Result of the request. This can be one of the following values. • **SUCCESS**
resultShortDescription	String	Short description of the result
resultLongDescription	String	Long description of the result
status	Object	Information about the current status of the job
description	Array	
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageDisplay	String	Translated label that corresponds to the message ID or to the pre-translated backup string if no message ID is specified
messageID	String	Message ID for the set of job tasks
messageTime	String	Time when this message was generated
percentage	Long	Percentage complete of the job

Attributes	Type	Description
state		State of the job. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
substatus	Array	Information about each step in the overall task. There is one entry for each step.
completed	Boolean	Indicates whether the step completed. This can be one of the following values. • **true**. The step has completed. • **false**. The task has not completed.
id	String	Short name of the step
longDescription	String	Long message description
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageID	String	Message ID for the task
progress	String	Progress of the task
shortDescription	String	Short message description
started	Boolean	Indicates if the management step has started. This can be one of the following values. • **true**. The step has started. • **false**. The step has not started.
status	Object	
percentage	Integer	Percentage complete of the task

Attributes	Type	Description
state	String	State of the task. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
userAction	String	Any user action that is required
taskid	Integer	Name of the job **Note:** This job ID might not be the same as the job ID that is returned by the POST /serverCertificate/tmp method.
taskName	String	Name of the job
time_spent	Long	Duration of the task in milliseconds
uuid	String	UUID of the device for which this job is running
status	String	Current status of the overall task. This can be one of the following values. • **CREATED** • **INCOMPLETE** • **DONE**
title	String	Job title. This is always “Managed System Cryptography Settings.”
result	String	Result of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message

Attributes	Type	Description
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

/serverCertificate/jobs/*{job_id}*

Use this REST API to retrieve information about a specific job for provisioning a signed server certificate to managed devices.

HTTP methods

GET

GET /serverCertificate/jobs/*{job_id}*

Use the PUT method to retrieve information about a specific job for provisioning a signed server certificates to all managed devices.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/serverCertificate/jobs/{job_id}`

where *{job_id}* is the job ID that was returned by the POST /serverCertificate/tmp method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Response content
progress	Double	Percentage complete of the job. This can be one of the following values. • **0**. Created • **50**. In progress. • **100**. Complete.
result	Array	Information about the job results. There is one entry for each managed device on which cryptographic settings are being changed.

Attributes	Type	Description
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageID	String	Message ID for the set of job tasks
messageAttributes	String	UUID that is associated with the job
progress	Long	Percentage complete of the job. This value can be `0 -100`
result	String	Result of the request. This can be one of the following values. • **SUCCESS**
resultShortDescription	String	Short description of the result
resultLongDescription	String	Long description of the result
status	Object	Information about the current status of the job
description	Array	
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageDisplay	String	Translated label that corresponds to the message ID or to the pre-translated backup string if no message ID is specified
messageID	String	Message ID for the set of job tasks
messageTime	String	Time when this message was generated
percentage	Long	Percentage complete of the job
state		State of the job. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**

Attributes	Type	Description
substatus	Array	Information about each step in the overall task. There is one entry for each step.
completed	Boolean	Indicates whether the step completed. This can be one of the following values. • **true**. The step has completed. • **false**. The task has not completed.
id	String	Short name of the step
longDescription	String	Long message description
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageID	String	Message ID for the task
progress	String	Progress of the task
shortDescription	String	Short message description
started	Boolean	Indicates if the management step has started. This can be one of the following values. • **true**. The step has started. • **false**. The step has not started.
status	Object	
percentage	Integer	Percentage complete of the task
state	String	State of the task. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
userAction	String	Any user action that is required

Attributes	Type	Description
taskid	Integer	Name of the job **Note:** This job ID might not be the same as the job ID that is returned by the POST /serverCertificate/tmp method.
taskName	String	Name of the job
time_spent	Long	Duration of the task in milliseconds
uuid	String	UUID of the device for which this job is running
status	String	Current status of the overall task. This can be one of the following values. • **CREATED** • **INCOMPLETE** • **DONE**
title	String	Job title. This is always “Managed System Cryptography Settings.”
result	String	Result of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

/service/country

Use this REST API to return or modify the country in which XClarity Administrator is located. This country used to download Storage DM firmware.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

HTTP methods

GET, PUT

GET /service/country

Use this method to return the country in which XClarity Administrator is located. This country used to download Storage DM firmware.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://<management_server_IP>/service/country
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

Parameters	Type	Description
country	String	Two-letter ISO 3166 code for the country or region To obtains the code, use GET /utils/countries

The following example is returned if the request is successful.

```
{
   "country": "CN"
}
```

PUT /service/country

Use this method to modify the country in which XClarity Administrator is located. This country used to download Storage DM firmware.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://<management_server_IP>/service/country`

Query parameters

None

Request body

Parameter	Re-quired / Optional	Type	Description
country	Required	String	Two-letter ISO 3166 code for the country or region To obtains the code, use GET /utils/countries.

The following examples set the country code.

```
{
   "country": "US"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Response body

None

/sessions

Use this REST API to retrieve information about all active user sessions, or log in or out of Lenovo XClarity Administrator.

HTTP methods

GET, POST, DELETE

GET /sessions

Use this method to return information about current sessions with Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/sessions`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
response		Array of objects	Information about each user session
	Address	Boolean	IP address of the server from which the user is connected
	authenticationServer	String	IP address of the authentication server
	created	String	Date and time when the user logged in and the session was started
	id	String	Session ID

Attributes	Type	Description
idleFor	String	Amount of time, in seconds, that the session has not had activity
isOwnSession	Boolean	This can be one of the following values. • **true** • **false**
lastAccessed	String	Date and time when the user performed the last action
UserId	String	User ID
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	The message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.


```
{
   "result": "success",
   "response": [{
      "Address": "10.38.99.166",
      "authenticationServer": "127.0.0.1",
      "created": "2019-01-25T16:27:07Z",
      "id": "1vze81e09gmmk1tctgb9of8y39",
      "idleFor": "0",
      "isOwnSession": true,
      "lastAccessed": "2019-01-25T16:27:16Z",
      "UserId": "ADMIN",
   },
   {
      "Address": "10.38.111.145",
      "authenticationServer": "127.0.0.1",
      "created": "2016-05-04T20:02:44Z",
      "id": "1xarpu7b3ksk23hj89jxo9y12",
      "idleFor": "50",
      "isOwnSession": true,
      "lastAccessed": "2016-05-07T20:02:52Z",
      "UserId": "JOE"
  }],
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      },
      "explanation": ""
   }]
}
```

POST /sessions

Use this method to create a new session with (log in to) Lenovo XClarity Administrator.

Important: When running automated scripts, if you want the session to respect the inactivity timeout, add the **X-NOT-USER-INPUT** field with a value of **checkSession** to the request header of each request. Adding this header implies that the session times out based on the inactivity timeout value. If the session times out, the session is not renewed, although active requests for uploading and downloading data are not canceled.

Authentication

Authentication is not required.

Request URL

`POST https://{management_server_IP}/sessions`

Query parameters

None

Request body

Parameters	Required / Optional	Type	Description
password	Required	String	Password for the user account.
UserId	Required	String	User name for the account to be used to log in to Lenovo XClarity Administrator.

The following example creates a new session.

```
{
   "password": "passwOrd",
   "UserId": "test"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	Information about each session.
pwChangeRequired	Boolean	Indicates whether the password must be changed the next time this user ID is used to log in to Lenovo XClarity Administrator. This can be one of the following values. • **true**. The password must be changed. • **false**. The password is not required to be changed.
session	Object	Information about the user session

Attributes	Type	Description
Address	String	IP address of the server from which the user is connected
authenticationServer	String	IP address of the authentication server
created	String	Date and time when the user logged in and the session was started
csrf	String	Cross-Site Request Forgery token for the session
id	String	Session ID
idleFor	String	Amount of time, in seconds, that the session has not had activity
inactivityTimeout	String	Amount time of inactivity, in seconds, after which the session is closed and the user is logged out
lastAccessed	String	Date and time when the user performed the last action
UserId	String	User ID
result	String	Results of the request. This can be one of the following values • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	The message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.


```
{
    "response": {
      "pwChangeRequired": false,
      "session": {
         "Address": "10.41.44.187",
         "authenticationServer": "127.0.0.1",
         "created": "2019-01-25T15:56:44Z",
         "csrf": "jbrnbSKznHM4ppOUMTDm-A5JcNNf46AXVNvX98lsRIvGc3Ryav3uTJUmTSP7-gPYacBtIrsEwjEs1IhSxU7_djeE3r_6--PKoa6_5Ois-
         "id": "19lee2nO5Oduf1Osew3a6l49gs",
         "idleFor": "0",
         "inactivityTimeout": "1440",
         "lastAccessed": "2019-01-25T15:56:44Z",
         "UserId": "USERID"
      }
    },
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
```

```
    }]
}
```

DELETE /sessions

Use this method to disconnect the current user session from Lenovo XClarity Administrator (log off).

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/sessions`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
```

```
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

/sessions/*{uuid}*

Use this REST API to disconnect (log off) another active user session from Lenovo XClarity Administrator.

HTTP methods

DELETE

DELETE /sessions/*{uuid}*

Use this method to disconnect (log off) another active user session from Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/sessions/{uuid}`

where *{uuid}* is the ID of the user to be logged off. To obtain the user ID, use the GET /sessions method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages

Attributes			Type	Description
	id		String	Message identifier of a returned message
	text		String	Message text associated with the message identifier
	explanation		String	Additional information to clarify the reason for the message
	recovery		Array of objects	Recovery information
		text	String	User actions that can be taken to recover from the event
		URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

/signingCertificate

Use this REST API to retrieve information about or regenerate the Certificate Authority (CA) root (signing) certificate that is currently in the Lenovo XClarity Administrator trust store in Lenovo XClarity Administrator and creates a job to send the certificate to all managed devices.

HTTP methods

GET, PUT

GET /signingCertificate

Use this method to return the current Certificate Authority (CA) root certificate in PEM format.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/signingCertificate`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.


```
-----BEGIN CERTIFICATE-----
MIID1TCCAr2gAwIBAgIUVihMFvNb6ZdIOd/FmSe7sWsnNj8wDQYJKoZIhvcNAQEL
BQAweTELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYD
VQQHEwdSYWxlaWdoMSUwIwYDVQQKExxHZW5lcmFOZWQgYnkgU2VydmVyIEZpcm13
YXJlMQkwBwYDVQQLEwAxDTALBgNVBAMTBExYQOEwIBcNNzAwMTAxMDUwMDAwWhgP
MjA3MDAxMDEwNDU5NTlaMHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3JOaCBD
YXJvbGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5
IFNlcnZlciBGaXJtd2FyZTEJMAcGA1UECxMAMQOwCwYDVQQDEwRMWENBMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuFx2YjVCCAKa2Sp5QpxdmCS8R8GI
l/92LyK37HySwKgaTSm9nxkQt2paZUg+NzMqOAbOmTwmVOT8/eGbtWFmWyqeFGr4
5m+MC3KhxOjrhOzQyRzrbmIOprgW1LSbDwRRon5k4efXhcvfmrNGoXHkGysMLOCZ
+bRk9XCjm+EFjwaW28pTHE8XfdMJD1zxy467vJQ9AOVNSh7YYflKw1jV73xMYiV9
tNbAADFCUT5RHicXxgF8huyKcJCHppiH9z6DqEOtgOZfeXqQJHmW5udweVmt646s
HEGNrCqmntAQcASIzDVfgYKm1dQn+mQAH5FJ/jyjnqjhP7AFIoneXOLYkwIDAQAB
o1MwUTAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRuFmtlFkO6WkpgbfSAja3U
GfwAWTAfBgNVHSMEGDAWgBRuFmtlFkO6WkpgbfSAja3UGfwAWTANBgkqhkiG9w0B
AQsFAAOCAQEAHa/w2SNQkSpAtoEnHZpDpZrThpNeeQxPMX2+Us2QxOa4Wr8WditB
9sK89inebkRSZxBTsZNKf4w1XT2TlND5mY88K4rQ15YZdLSJvaKr9QmKSbmBKWeT
dcOX5HLaB8evP4EoOC32BXvklx+SnNtZHupcXo8JfmC38Hxftpn8ZfiAfiYr4jZI
iIom6Zupxoc7ZuyAWOovp4V5jKmglWDM4xXRTDsYcHEOpnGOry+MlPEAszDexYd8
HNdO2BliTsytll6RsSoJ6B9gu49OOcSRYpp543azUDStsoJ8a/8CfyeGMje6aREg
tOumP61rQlEYyUmEcEr/eDZt8pjXiR/txw==
-----END CERTIFICATE-----
```

PUT /signingCertificate

Use this method to generate a new Certificate Authority (CA) root certificate in Lenovo XClarity Administrator and creates a job to send the certificate to all managed devices.

When a new CA root certificate is generated and, a job is created to provision the new certificate to all managed devices. Use the GET /signingCertificate/jobs/*{job_id}* method to retrieve the job status and additional job details. If a job was not successfully started, refer to the response code and response body for details.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/signingCertificate`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	Response content This attribute is provided only if the CA that is specified in the certification chain is new and **returnJobInfo="true"** is specified in the request.
jobPath	String	URI in the form /serverCertificate/jobs/*{job_id}* (for example, `/serverCertificate/jobs/383`) that represents the job that is monitored by the management server. You can use GET /signingCertificate/jobs/*{job_id}* to determine the status of the job. If a job was not successfully started, refer to the response code and response body for details. This is the same URI that is included in the response header. If no job was created, this attribute is empty.
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.

Attributes	Type	Description
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Identifier of the returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
    "response": {
        "jobPath": "/signingCertificate/jobs/383"
    },
    "result": "success",
    "messages": [{
        "explanation": "The CA root certificate was regenerated.",
        "id": "FQXHMSE0132I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request to generate the CA root certificate was successful."
    }]
}
```

/signingCertificate/details

Use this REST API to retrieve detailed information about the Certificate Authority (CA) root (signing) certificate that is currently in the Lenovo XClarity Administrator trust store.

HTTP methods

GET

GET /signingCertificate/details

Use GET to retrieve detailed information about the current Certificate Authority (CA) root certificate in PEM format.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/signingCertificate/details`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	
certificate	String	Certificate in PEM format
issuerDn	String	LDAP Distinguished Name of the issuer, for example: `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`
notAfter	String	Date and time that the certificate is no longer valid The timestamp is returned in ISO 8601 format , for example: `2014-02-05T15:54:13Z`
notBefore	String	Date and time the certificate becomes valid. The timestamp is returned in ISO 8601 format, for example: `2014-02-05T15:54:13Z`
serialNumber	String	Serial number of the certificate
signatureAlgorithm	String	Algorithm used to signed the certificate, for example: `"MD5withRSA","SHA256withRSA"`
subjectDn	String	The LDAP Distinguished Name of the subject, for example: `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Information about one or more messages
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": {
      "certificate": "-----BEGIN CERTIFICATE-----\n
                MIID1TCCAr2gAwIBAgIUVihMFvNb6ZdIOd/FmSe7sWsnNj8wDQYJKoZIhvcNAQEL\n
                BQAweTELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYD\n
```

```
                    VQQHEwdSYWxlaWdoMSUwIwYDVQQKExxHZW5lcmF0ZWQgYnkgU2VydmVyIEZpcm13\n
                    YXJlMQkwBwYDVQQLEwAxDTALBgNVBAMTBExYQOEwIBcNNzAwMTAxMDUwMDAwWhgP\n
                    MjA3MDAxMDEwNDU5NTlaMHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBD\n
                    YXJvbGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5\n
                    IFNlcnZlciBGaXJtd2FyZTEJMAcGA1UECxMAMQOwCwYDVQQDEwRMWENBMIIBIjAN\n
                    BgkqhkiG9wOBAQEFAAOCAQ8AMIIBCgKCAQEAuFx2YjVCCAKa2Sp5QpxdmCS8R8GI\n
                    l/92LyK37HySwKgaTSm9nxkQt2paZUg+NzMqOAbOmTwmVOT8/eGbtWFmWyqeFGr4\n
                    5m+MC3KhxOjrhOzQyRzrbmIOprgW1LSbDwRRon5k4efXhcvfmrNGoXHkGysMLOCZ\n
                    +bRk9XCjm+EFjwaW28pTHE8XfdMJD1zxy467vJQ9AOVNSh7YYflKw1jV73xMYiV9\n
                    tNbAADFCUT5RHicXxgF8huyKcJCHppiH9z6DqEOtgOZfeXqQJHmW5udweVmt646s\n
                    HEGNrCqmntAQcASIzDVfgYKm1dQn+mQAH5FJ/jyjnqjhP7AFIoneXOLYkwIDAQAB\n
                    o1MwUTAPBgNVHRMBAf8EBTADAQH/MBOGA1UdDgQWBBRuFmtlFkO6WkpgbfSAja3U\n
                    GfwAWTAfBgNVHSMEGDAWgBRuFmtlFkO6WkpgbfSAja3UGfwAWTANBgkqhkiG9wOB\n
                    AQsFAAOCAQEAHa/w2SNQkSpAtoEnHZpDpZrThpNeeQxPMX2+Us2QxOa4Wr8WditB\n
                    9sK89inebkRSZxBTsZNKf4w1XT2TlND5mY88K4rQ15YZdLSJvaKr9QmKSbmBKWeT\n
                    dcOX5HLaB8evP4EoOC32BXvklx+SnNtZHupcXo8JfmC38Hxftpn8ZfiAfiYr4jZI\n
                    iIom6Zupxoc7ZuyAWOovp4V5jKmglWDM4xXRTDsYcHEOpnGOry+MlPEAszDexYd8\n
                    HNdO2BliTsytll6RsSoJ6B9gu49OOcSRYpp543azUDStsoJ8a/8CfyeGMje6aREg\n
                    tOumP61rQlEYyUmEcEr/eDZt8pjXiR/txw==\n
                    -----END CERTIFICATE-----\n",
      "issuerDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
      "notAfter": "2070-01-01T04:59:59Z",
      "notBefore": "1970-01-01T05:00:00Z",
      "serialNumber": "56284c16f35be9974839dfc59927bbb16b27363f",
      "signatureAlgorithm": "SHA256withRSA",
      "subjectDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US"
   },
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```


/signingCertificate/jobs

Use this REST API to retrieve information about all known jobs for provisioning signing certificates to managed devices.

HTTP methods

GET

GET /signingCertificate/jobs

Use this method to retrieve information about all known jobs for provisioning signing certificates to managed devices.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/signingCertificate/jobs`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Response content
progress	Double	Percentage complete of the job. This can be one of the following values. • **0**. Created • **50**. In progress. • **100**. Complete.
result	Array	Information about the job results. There is one entry for each managed device on which cryptographic settings are being changed.
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageID	String	Message ID for the set of job tasks
messageAttributes	String	UUID that is associated with the job
progress	Long	Percentage complete of the job. This value can be `0 -100`.
result	String	Result of the request. This can be one of the following values. • **SUCCESS**
resultShortDescription	String	Short description of the result
resultLongDescription	String	Long description of the result
status	Object	Information about the current status of the job
description	Array	
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageDisplay	String	Translated label that corresponds to the message ID or to the pre-translated backup string if no message ID is specified.
messageID	String	Message ID for the set of job tasks
messageTime	String	Time when this message was generated
percentage	Integer	Percentage complete of the job

Attributes	Type	Description
state	String	State of the job. is can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
substatus	Array	Information about each step in the overall task. There is one entry for each step.
completed	Boolean	Indicates whether the step is complete. This can be one of the following values. • **true**. The step is complete. • **false**. The task is not complete.
id	String	Short name of the step
longDescription	String	Long message description
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com. lenovo.lxca.security.base.bundle.tasks.messages.”
messageID	String	Message ID for the task
progress	String	Progress of the task
shortDescription	String	Short message description
started	Boolean	Indicates if the management step has started. This can be one of the following values. • **true**. The step has started. • **false**. The step has not started.
status	Object	
percentage	Long	Percentage complete of the tas.

Attributes	Type	Description
state	String	State of the task. The following values can be returned: • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
userAction	String	Any user action that is required
taskid	Integer	Job ID **Note:** This job ID might not be the same as the job ID that is returned by the PUT /signingCertificate method.
taskName	String	Job name
time_spent	Long	Duration of the task in milliseconds
uuid	String	UUID of the device for which this job is running
status	String	Current status of the overall task. This can be one of the following values: • **CREATED** • **INCOMPLETE** • **DONE**
title	String	Job title. This is always “Managed System Cryptography Settings.”
result	String	Results of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
id	String	Identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message

Attributes	Type	Description
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event.
URL	String	Link to the help system for more information, if available

/signingCertificate/jobs/*{job_id}*

Use this REST API to retrieve information about a specific job for provisioning a signing certificate to managed devices.

HTTP methods

GET

GET /signingCertificate/jobs/*{job_id}*

Use the PUT method to retrieve information about a specific job for provisioning a signing certificate to managed devices.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/signingCertificate/jobs/{job_id}`

where *{job_id}* is the job ID that was returned by the PUT /signingCertificate method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Response content
progress	Double	Percentage complete of the job. This can be one of the following values. • **0**. Created • **50**. In progress. • **100**. Complete.
result	Array	Information about the job results. There is one entry for each managed device on which cryptographic settings are being changed.

Attributes	Type	Description
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageID	String	Message ID for the set of job tasks
messageAttributes	String	UUID that is associated with the job
progress	Long	Percentage complete of the job. This value can be `0 -100`
result	String	Result of the request. This can be one of the following values. • **SUCCESS**
resultShortDescription	String	Short description of the result
resultLongDescription	String	Long description of the result
status	Object	Information about the current status of the job
description	Array	
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageDisplay	String	Translated label that corresponds to the message ID or to the pre-translated backup string if no message ID is specified
messageID	String	Message ID for the set of job tasks
messageTime	String	Time when this message was generated
percentage	Long	Percentage complete of the job
state		State of the job. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**

Attributes	Type	Description
substatus	Array	Information about each step in the overall task. There is one entry for each step.
completed	Boolean	Indicates whether the step completed. This can be one of the following values. • **true**. The step has completed. • **false**. The task has not completed.
id	String	Short name of the step
longDescription	String	Long message description
messageBundle	String	Location where messages.properties can be found if it is not located in the default task management bundle. This value is always “com.lenovo.lxca.security.base.bundle.tasks.messages.”
messageID	String	Message ID for the task
progress	String	Progress of the task
shortDescription	String	Short message description
started	Boolean	Indicates if the management step has started. This can be one of the following values. • **true**. The step has started. • **false**. The step has not started.
status	Object	
percentage	Integer	Percentage complete of the task
state	String	State of the task. This can be one of the following values. • **Aborted** • **Blocked** • **Cancelled** • **CancelledWithError** • **CancelledWithWarning** • **Cancelling** • **Complete** • **CompleteWithError** • **CompleteWithWarning** • **Expired** • **Initializing** • **Interrupted** • **InterruptedWithError** • **InterruptedWithWarning** • **Investigating** • **Pending** • **Resolved** • **Running** • **RunningWithError** • **RunningWithWarning** • **Skipped** • **Stopped** • **StoppedWithError** • **StoppedWithWarning** • **Unknown** • **Uploading** • **Validating** • **Waiting**
userAction	String	Any user action that is required

Attributes	Type	Description
taskid	Integer	Name of the job **Note:** This job ID might not be the same as the job ID that is returned by the POST /serverCertificate/tmp method.
taskName	String	Name of the job
time_spent	Long	Duration of the task in milliseconds
uuid	String	UUID of the device for which this job is running
status	String	Current status of the overall task. This can be one of the following values. • **CREATED** • **INCOMPLETE** • **DONE**
title	String	Job title. This is always “Managed System Cryptography Settings.”
result	String	Result of the request . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

/singleSignOn

Use this REST API to retrieve and modify the single sign-on setting.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

HTTP methods

GET, PUT

GET /singleSignOn

Use this method to returns the single sign-on setting.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://<management_server_IP>/singleSignOn
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
ssoEnabled	Boolean	Indicates whether single sign-on is enabled for managed devices. This can be one of the following values. • **true**. Sign-on is enabled. • **false**. Sign-on is disabled. **Note:** Single sign-on is disabled automatically when using the CyberArk identity-management system for authentication.

The following example is returned if the request is successful.

```
{
   "ssoEnabled": true
}
```

PUT /singleSignOn

Use this method to enable or disable single sign-on for managed devices.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/singleSignOn`

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
ssoEnabled	Required	Boolean	Indicates whether single sign-on is enabled for managed devices. This can be one of the following values. • **true**. Sign-on is enabled. • **false**. Sign-on is disabled. **Note:** Single sign-on is disabled automatically when using the CyberArk identity-management system for authentication.

The following example enables single sign-on for managed devices.

```
{
   "ssoEnabled": true
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/storedCredentials

Use this REST API to retrieve information about all stored credentials and to create a stored credential.

If you choose to manage devices using local authentication instead of Lenovo XClarity Administrator managed authentication, you must select a stored-credentials account during the management process. The stored credential can be a local user account on the device or a user account in Active Directory. For more information about stored credentials, see Managing stored credentials in the Lenovo XClarity Administrator online documentation.

Important: Lenovo XClarity Administrator does not validate the user name and password that you specify for the stored credential. It is your responsibility to ensure that specified information corresponds to an active user account on the local device or Active Directory (if the managed device is configured to use Active Directory for authentication).

Note: This API requires Lenovo XClarity Administrator v1.4.0 or later.

HTTP methods

GET, POST

GET /storedCredentials

Use this method to return information about all stored credentials.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/storedCredentials
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Information about each stored credential
description	String	Description of the stored credential
id	String	ID of the stored credential
userName	String	Name of the stored credential
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information

Attributes	Type	Description
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": [{
      "description": "For server A",
      "id": "100",
      "userName": "USERID"
   },
   {
      "description": "For server B",
      "id": "200",
      "userName": "USERID"
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "explanation": "",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      }
   }]
}
```

POST /storedCredentials

Use this method to create a stored credential.

Important: Lenovo XClarity Administrator does not validate the user name and password that you specify for the stored credential. It is your responsibility to ensure that specified information corresponds to an active user account on the local device or LDAP server (if the managed device is configured to use Microsoft Active Directory or OpenLDAP for authentication).

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/storedCredentials`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
description	Optional	String	Description of the stored-credential account Use this attribute to differentiate between accounts when users and stored credentials have the same name.
password	Required	String	Password for the stored-credential account
userName	Required	String	Name of the stored-credential account You must specify a user name for management, OS-management, and local user accounts. For other stored credential type, the user name is optional.

The following example creates a stored credential.

```
{
   "description": "CME44",
   "password: "passwr0d"
   "userName": "USERID"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
id	String	The stored credential ID.

The following example is returned if the request is successful.

```
{
   "id":"605"
}
```

/storedCredentials/*{id}*

Use this REST API to retrieve information about a specific stored credential, to modify properties for a stored credential, or to delete a stored credential account.

If you choose to manage devices using local authentication instead of Lenovo XClarity Administrator managed authentication, you must select a stored-credentials account during the management process. The stored credential can be a local user account on the device or a user account in Active Directory. For more

information about stored credentials, see Managing stored credentials in the Lenovo XClarity Administrator online documentation.

Important: Lenovo XClarity Administrator does not validate the user name and password that you specify for the stored credential. It is your responsibility to ensure that specified information corresponds to an active user account on the local device or Active Directory (if the managed device is configured to use Active Directory for authentication).

HTTP methods

GET, PUT, DELETE

GET /storedCredentials/*{id}*

Use this method to return information about a specific stored credential.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/storedCredentials/{id}`

where *{id}* is the ID of the stored credential. To obtain the stored credential ID, use GET /storedCredentials or POST /storedCredentials.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
401	Unauthorized	The user cannot be authenticated. Authentication has not been provided or has failed. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	Information about each stored credential
description	String	Description of the stored-credential
id	String	ID of the stored-credential
userName	String	Name of the stored-credential, if applicable
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful when an administrator specifies the **includePassowrd=true** query parameter.

```
{
   "response": {
      "description": "CME44",
      "id": "602",

      "userName": "USERID"
   },
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "explanation": "",
      "recovery": {
         "text": "Information only. No action is required.",
         "URL": ""
      }
   }]
}
```

PUT /storedCredentials/*{id}*

Use this method to modify the properties for a specific stored credential.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/storedCredentials/{id}`

where *{id}* is the ID of the stored credential. To obtain the stored credential ID, use GET /storedCredentials or POST /storedCredentials.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
description	Optional	String	Description of the stored credential Use this attribute to differentiate between accounts when users and stored credentials have the same name.
id	Required	String	Name of the stored credential to be modified
password	Required	String	Password for the stored credential
userName	Required	String	Name of the stored credential

The following example modifies a stored credential.

```
{
   "description": "CME44",
   "id": "603",
   "password: "passwr0d",
   "userName": "USERID"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages

Attributes	Type	Description
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "explanation": "The request to modify the storage account ID USER2 was successful.",
      "id": "FQXHMSE0260I",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request to modify the storage account ID USER2 completed successfully."
   }]
}
```

DELETE /storedCredentials/*{id}*

Use this method to remove a specific stored credential.

Note: You cannot delete a stored credential that is associated with one or more managed devices.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/storedCredentials/{id}`

where *{id}* is the ID of the stored credential. To obtain stored credential ID, use GET /storedCredentials.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/trustedCertificates

Use this REST API to retrieve information about all trusted certificates that are currently installed, or upload and install a new trusted certificate.

HTTP methods

GET, POST

GET /trustedCertificates

Use this method to return information for all trusted certificates that are currently installed.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/trustedCertificates`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
response		Array of objects	Information about each trusted certificate
	certificate	String	Certificate in PEM format
	id	String	Identifier used to identify this particular trusted certificate
	issuerDn	String	LDAP Distinguished Name of the issuer, for example: `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`

Attributes	Type	Description
notAfter	String	Date and time that the certificate is no longer valid. The timestamp is returned in ISO 8601 format, for example: `"2014-02-05T15:54:13Z"`
notBefore	String	Date and time the certificate becomes valid. The timestamp is returned in ISO 8601 format, for example: `2014-02-05T15:54:13Z`
serialNumber	String	Serial number of the certificate.
signatureAlgorithm	String	Algorithm used to signed the certificate, for example: `"MD5withRSA","SHA256withRSA"`
subjectDn	String	LDAP Distinguished Name of the subject, for example: `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`
result	String	Request results . This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	The message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.


```
{
   "response": [{
      "id": "mgmt_server",
      "issuerDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
      "notAfter": "2070-01-01T04:59:59Z",
      "notBefore": "1970-01-01T05:00:00Z",
      "serialNumber": "1155c78e5ad9f91dd90bb2cbc7b0620a0cebde73",
      "signatureAlgorithm": "SHA256withRSA",
      "subjectDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US"
   },
   ...,
   {
      "id": "c29379aa380e11e39df3000af7256714.2",
      "issuerDn": "OU=-,CN=betadraco02,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
      "notAfter": "2025-01-06T21:10:03Z",
      "notBefore": "2015-01-09T21:10:03Z",
      "serialNumber": "be55a603167bf15f",
      "signatureAlgorithm": "SHA256withECDSA",
      "subjectDn": "OU=-,CN=betadraco02,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US"
   }],
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
```

```
      },
      "text": "The request completed successfully."
   }]
}
```

POST /trustedCertificates

Use this method to upload and install a new trust certificate.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/trustedCertificates`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
certificate	Required	String	The server certificate in PEM format. The certificate to be uploaded must have been created from the certificate signing request using GET /certificateSigningRequest or downloaded from the Lenovo XClarity Administrator user interface.

The following example uploads and installs a new trust certificate.

```
{
    "certificate": "-----BEGIN CERTIFICATE-----\n
                    MIID8jCCAtqgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmzFHMEUGA1UEAxM+Q0Eg\n
                    Zm9yIEE0QUZCQkM0LTc3MDItMzIwNC05QTQ1LUM2RjMxNUQ2NjIzNiwgMTUtMDEt\n
                    MjAgMTQ6MDY6MDAxJTAjBgNVBAoTHEdlbmVyYXRlZCBieSBMZW5vdm8gRmlybXdh\n
                    cmUxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJUWDEPMA0GA1UEBxMGQXVzdGluMB4X\n
                    DTcwMDEwMTAwMDAwMFoXDTQ4MTIzMTIzNTk1OVowgZsxRzBFBgNVBAMTPkNBIGZv\n
                    ciBBNEFGQkJDNC03NzAyLTMyMDQtOUE0NS1DNkYzMTVENjYyMzYsIDE1LTAxLTIw\n
                    IDE0OjA2OjAwMSUwIwYDVQQKExxHZW5lcmF0ZWQgYnkgTGVub3ZvIEZpcm13YXJl\n
                    MQswCQYDVQQGEwJVUzELMAkGA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjCCASIw\n
                    DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOxO218Op9Zf93jYhOubiNeZK4Bl\n
                    Xj6p5AvMhBqr5drgs8coXKXgDcj1Z4UKxJgNh+HuacSmnpUQrk7rYFp7Mn8CqVQQ\n
                    fNa3sYy49bccdGlCuCnWpI1jvoLLbDn229UQw3hznLVOaGLYUPs61SHf1euOunLb\n
                    X+E9FsOeU7rEtiRaaXkDcmsAruV+POnSOxg9vA1Op4O9rg7OpIhVX99VRbc4RFeb\n
                    hHYDCTtjW48sYRoxB/vxuEjaO+QhBYcUu3B4l+uhZasxNmlfpQEDOgyNjjxTv1+T\n
                    +N9hXwSsx4BUraF/2aR9Hr3NPxelhNqFUsfKeKqgIZ+wnSswElRvoiClmJkCAwEA\n
                    AaM/MD0wDAYDVR0TBAUwAwEB/zAOBgNVHQ8BAf8EBAMCAbYwHQYDVR0lBBYwFAYI\n
                    KwYBBQUHAwIGCCsGAQUFBwMBMA0GCSqGSIb3DQEBBQUAA4IBAQANEmEsIXOkOj84\n
                    D9+KAcsqp86ozeWgWiKJzOHatZACLVEt5fNE8I+vvnHUucLNUNttQyFx2phw33sS\n
                    2nVHOnysOdr7bZnIlUhUxMLuuXXLU+2/HavVnVFzlv8tWiq3ARCgNHBQphbEhmpy\n
                    bdBmkySf1zz7ErslXy/CzHm2zUTrNitKdC1edIyt9Ph2/tJ8nEEMFN5hPyOt/nkZ\n
                    bHZmWfE54gDxOacCCDb4O+stxnihtD4AeDCJwNmbxhOtxLCAgsw7YeNw3rbvm4FP\n
                    sas6a2I/4edd/A7cfgWs2ADLpOPDBhuR6pJrdIMeADdD9JF1KolwdXnB7caKqTtH\n
                    eTUkKVnX\n
                    -----END CERTIFICATE-----\n"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

/trustedCertificates/*{id}*

Use this REST API to retrieve information about or delete a specific trusted certificate.

HTTP methods

GET, DELETE

GET /trustedCertificates/*{id}*

Use this method to download the PEM file for a specific trusted certificate.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/trustedCertificates/{id}`

where *{id}* is the trusted certificate ID. To obtain trusted certificate ID, use GET /trustedCertificates or GET /trustedCertificates/details.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
-----BEGIN CERTIFICATE-----
MIID7DCCAtSgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmDFHMEUGA1UEAxM+Q0Eg
Zm9yIEZGQjY1NzQwLThCRUItNDE2MS05NTA3LTA0QUIwRUQzQTgOQSwgMTUtMDUt
MDYgMTQ6MjU6NTIxIjAgBgNVBAoTGUdlbmVyYXRlZCBieSBJQk0gRmlybXdhcmUx
CzAJBgNVBAYTAlVTMQswCQYDVQQIEwJUWDEPMA0GA1UEBxMGQXVzdGluMB4XDTUw
```

```
MDEwMTAwMDEwMFoXDTQ4MTIzMTIzNTk1OVowgZgxRzBFBgNVBAMTPkNBIGZvciBG
RkI2NTc0MCO4QkVCLTQxNjEtOTUwNy0wNEFCMEVEMOE4NEEsIDE1LTA1LTA2IDEO
OjI1OjUyMSIwIAYDVQQKExlHZW5lcmFOZWQgYnkgSUJNIEZpcm13YXJlMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALtxWUCKlsukZHytbArcc9fttQNsMxroOLUi
hrNYJoYsu51ReNgIf4zTwsVrguRpeNzvFjgIsxx+WtyWL3Lz3yOvJuQ2D55VZAXz
B1oyO/P3FnfNZMmDgzVzcvTO3DPF2wtMYbgzG248gn/2i9/po/JSc9Y8txXNFmTg
zjZyv3dkjk1fHTDx+KXpP43F37Ey1OoHMuXMrb92KiXduPpy2Mf7W7R8U+Xe8O66
dKKyOmF7HMz+ODaRlnb+bxxiCKtZIW2l8JXkpxm9Jzvx5iVz+KRkxUtxPZ5h3pIz
SkkKsL1JzMEDwnj5tf+xiyHEweWuVuwtF8Aap1g4zd1gEBcWbhsCAwEAAaM/MDOw
DAYDVROTBAUwAwEB/zAOBgNVHQ8BAf8EBAMCAbYwHQYDVROlBBYwFAYIKwYBBQUH
AwIGCCsGAQUFBwMBMAOGCSqGSIb3DQEBBQUAA4IBAQCKlKz6Msl2QaFsKqTZu1aL
8JV3Ipa4Arjpey98Q5rO26jMkgcuEkpYX9RxoVp4hjjXFPBvoMoH/PoSf58Bwe+p
zFcvAWOqYeeGnBx9o29JeYK8VhwyL4bDM997t8sNbxr/5gajVpZHHRV2hFKxVmwl
AGOgN3jf7vZdPt5dp7aKIhdpOM2GKdZ6TJNEiOl2XXzsn39qlUoKNQ3Juyh13Jru
7JSFItVz8OSN9sWi7+V4hulcB8OehMTpapFAwKly3nndFOtAAOCdOxL3socMB5SO
sEop/nQvfrT2UKtcOQMPmYOGofvLoOr65gLlFjW4GWcZxWOOfkdVHv+E9ofHswbN
-----END CERTIFICATE-----
```

DELETE /trustedCertificates/*{id}*

Use this method to remove a specific trusted certificate.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/trustedCertificates/{id}`

where *{id}* is the trusted certificate ID. To obtain trusted certificate ID, use GET /trustedCertificates or GET /trustedCertificates/details.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

/trustedCertificates/details

Use this REST API to retrieve detailed information about all trusted certificates.

HTTP methods

GET

GET /trustedCertificates/details

Use this method to returnd detailed information about all trusted certificate. The certificate is returned in PEM format.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/trustedCertificates/details
```

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Information about each trusted certificate
certificate	String	Certificate in PEM format
id	String	Identifier used to identify this particular trusted certificate
issuerDn	String	LDAP Distinguished Name of the issuer, for example: `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`
notAfter	String	Date and time that the certificate is no longer valid. The timestamp is returned in ISO 8601 format, for example: `2014-02-05T15:54:13Z`
notBefore	String	Date and time the certificate becomes valid. The timestamp is returned in ISO 8601 format, for example: `2014-02-05T15:54:13Z`
serialNumber	String	Serial number of the certificate
signatureAlgorithm	String	Algorithm used to signed the certificate, for example: `"MD5withRSA","SHA256withRSA"`
subjectDn	String	LDAP Distinguished Name of the subject, for example: `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	The message identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
```

```
"response": [{
   "certificate": "-----BEGIN CERTIFICATE-----\n
                   MIID1TCCAr2gAwIBAgIUEVXHjlrZ+R3ZC7LLx7BiCgzr3nMwDQYJKoZIhvcNAQEL\n
                   BQAweTELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYD\n
                   VQQHEwdSYWxlaWdoMSUwIwYDVQQKExxHZW5lcmF0ZWQgYnkgU2VydmVyIEZpcm13\n
                   YXJlMQkwBwYDVQQLEwAxDTALBgNVBAMTBExYQ0EwIBcNNzAwMTAxMDUwMDAwWhgP\n
                   MjA3MDAxMDEwNDU5NTlaMHkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBD\n
                   YXJvbGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5\n
                   IFNlcnZlciBGaXJtd2FyZTEJMAcGA1UECxMAMQ0wCwYDVQQDEwRMWENBMIIBIjAN\n
                   BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp9FLowe87titCSbzlgMmjSOwRMBE\n
                   C4Vk+D7kwq/fdS/pTJT2vhfRb+OARrkflAu4qn8PTu/XpxCUkiGik/2ho2SW2Anj\n
                   ZdlLYLJj6DOgB+qC24P7U8yaG9OTSiwQ2+TEungcdAOa9RLBmHrEC5vw3oFxr61j\n
                   tcA+OSiYdne2tfgW7JMnrxmpLtf7UiL7b89A9nHuep6kw8EQLxAPOKZxRf/MsFtH\n
                   yN8nTNRdDuR7HUKRl+hahKYrcyX8kvPtnXbjPr1sqxCNfLjyEjOaPf4QBEOzVx1g\n
                   xagrfmSZscY7h1QZOWnTIhtxV4BiHRQVQStqLen+BUS/yBs7ltGxyP9nJwIDAQAB\n
                   o1MwUTAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRz/PlTGS/szZjR41wmCjrA\n
                   Lp1sezAfBgNVHSMEGDAWgBRz/PlTGS/szZjR41wmCjrALp1sezANBgkqhkiG9w0B\n
                   AQsFAAOCAQEAEuO9NFq5zVgH8UACYZxpnCazQoOUQrHWGPjX9SsgsvHWHn31lyke\n
                   wADIkPQePSqLO6fHVsK1CSx7hx8e9uBROzAHDehPe4GZCS3Z59U2Hv3WTdZjjIO6\n
                   gi2/UX+cn+/wNtYO3xzreDgeRkdn6iSNkvGjfFGpe/yaNmG3cRe5zDQhrCibM1Nx\n
                   b4xBOZfrRiuHHNO4Bo/4FwzkAOKMrFBKUK3LrGbmwEhhvZ12dYPSWEeG7CJ2EIDM\n
                   3Xfj4BApCek6/9lqjJId54YAFM1wXOgUZi71BG8NtAvL2GGr7t/OXaKsYly2aiBr\n
                   S7CzKMZE8+uaiTtB5K9j/bBOlykxnmBIlw==\n
                   -----END CERTIFICATE-----\n",
   "id": "mgmt_server",
   "issuerDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
   "notAfter": "2070-01-01T04:59:59Z",
   "notBefore": "1970-01-01T05:00:00Z",
   "serialNumber": "1155c78e5ad9f91dd90bb2cbc7b0620a0cebde73",
   "signatureAlgorithm": "SHA256withRSA",
   "subjectDn": "CN=LXCA,OU=,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US"
},
...,
{
   "certificate": "-----BEGIN CERTIFICATE-----\n
                   MIICMTCCAbcCCQC+VaYDFnvxXzAKBggqhkjOPQQDAjCBgTELMAkGA1UEBhMCVVMx\n
                   FzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdoMSUwIwYD\n
                   VQQKExxHZW5lcmF0ZWQgYnkgU2VydmVyIEZpcm13YXJlMRQwEgYDVQQDEwtiZXRh\n
                   ZHJhY28wMjEKMAgGA1UECxMBLTAeFw0xNTAxMDkyMTEwMDNaFw0yNTAxMDYyMTEw\n
                   MDNaMIGBMQswCQYDVQQGEwJVUzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAO\n
                   BgNVBAcTB1JhbGVpZ2gxJTAjBgNVBAoTHEdlbmVyYXRlZCBieSBTZXJ2ZXIgRmly\n
                   bXdhcmUxFDASBgNVBAMTC2JldGFkcmFjbzAyMQowCAYDVQQLEwEtMHYwEAYHKoZI\n
                   zj0CAQYFK4EEACIDYgAEcdUVUwFlYQFBcUw/YfYzlk5acgSFJsH7ugrb2YTrlb2m\n
                   PgBPxPLqJwZE8cQHS3OqbIbh4SFrLaaVejgQ4LLdBMUj2vpXA/2VsOHGwN/uP4cJ\n
                   XuppRtlij2hTpopCxmf1MAoGCCqGSM49BAMCA2gAMGUCMQDHD2BnCGOTfiqGoP+g\n
                   13RTuyvngr+OjuY5KeZwaOHOGy77YId//w8WLfobp18OpdICMEOqryDz1DSBwnn/\n
                   aCZChFTCz4WF8p+5MQ4WqaDq/5pVQhjbDI3Ra/yQgrvdgH6C3A==\n
                   -----END CERTIFICATE-----\n",
   "id": "c29379aa380e11e39df3000af7256714.2",
   "issuerDn": "OU=-,CN=betadraco02,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
   "notAfter": "2025-01-06T21:10:03Z",
   "notBefore": "2015-01-09T21:10:03Z",
   "serialNumber": "be55a603167bf15f",
   "signatureAlgorithm": "SHA256withECDSA",
   "subjectDn": "OU=-,CN=betadraco02,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
}],
"result": "success",
"messages": [{
   "id": "FQXHMSE0001I",
   "text": "The request completed successfully.",
   "explanation": "",
```

```
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      }
   }]
}
```

/trustedCertificates/details/*{id}*

Use this REST API to retrieve the detailed information about a specific trusted certificate.

HTTP methods

GET

GET /trustedCertificates/details/*{id}*

Use this method to return detailed information about a specific trusted certificate. The trusted certificate is in PEM format.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/trustedCertificates/details/{id}`

where *{id}* is the trusted certificate ID. To obtain trusted certificate ID, use GET /trustedCertificates or GET /trustedCertificates/details.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	Information about the trusted certificate
certificate	String	Certificate in PEM format
id	String	Identifier used to identify this particular trusted certificate
issuerDn	String	LDAP Distinguished Name of the issuer, for example: `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`
notAfter	String	Date and time that the certificate is no longer valid. The timestamp is returned in ISO 8601 format, for example: `2014-02-05T15:54:13Z`

Attributes	Type	Description
notBefore	String	Date and time the certificate becomes valid. The timestamp is returned in ISO 8601 format, for example: `2014-02-05T15:54:13Z`
serialNumber	String	Serial number of the certificate
signatureAlgorithm	String	Algorithm used to signed the certificate, for example: `"MD5withRSA","SHA256withRSA"`
subjectDn	String	LDAP Distinguished Name of the subject, for example: `"CN=demo server,OU=CS,O=Com Ltd.,ST=QLD,C=AU"`
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Identifier of a returned message
recovery	Array	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.


```
{
   "response": {
      "certificate": "-----BEGIN CERTIFICATE-----\n
                      MIICMTCCAbcCCQC+VaYDFnvxXzAKBggqhkjOPQQDAjCBgTELMAkGA1UEBhMCVVMx\n
                      FzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdoMSUwIwYD\n
                      VQQKExxHZW5lcmFOZWQgYnkgU2VydmVyIEZpcm13YXJlMRQwEgYDVQQDEwtiZXRh\n
                      ZHJhY28wMjEKMAgGA1UECxMBLTAeFw0xNTAxMDkyMTEwMDNaFw0yNTAxMDYyMTEw\n
                      MDNaMIGBMQswCQYDVQQGEwJVUzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAO\n
                      BgNVBAcTB1JhbGVpZ2gxJTAjBgNVBAoTHEdlbmVyYXRlZCBieSBTZXJ2ZXIgRmly\n
                      bXdhcmUxFDASBgNVBAMTC2JldGFkcmFjbzAyMQowCAYDVQQLEwEtMHYwEAYHKoZI\n
                      zj0CAQYFK4EEACIDYgAEcdUVUwFlYQFBcUw/YfYzlk5acgSFJsH7ugrb2YTrlb2m\n
                      PgBPxPLqJwZE8cQHS3OqbIbh4SFrLaaVejgQ4LLdBMUj2vpXA/2VsOHGwN/uP4cJ\n
                      XuppRtlij2hTpopCxmf1MAoGCCqGSM49BAMCA2gAMGUCMQDHD2BnCGOTfiqGoP+g\n
                      13RTuyvngr+OjuY5KeZwaOHOGy77YId//w8WLfobp18OpdICMEOqryDz1DSBwnn/\n
                      aCZChFTCz4WF8p+5MQ4WqaDq/5pVQhjbDI3Ra/yQgrvdgH6C3A==\n
                      -----END CERTIFICATE-----\n",
      "id": "c29379aa380e11e39df3000af7256714.2",
      "issuerDn": "OU=-,CN=betadraco02,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
      "notAfter": "2025-01-06T21:10:03Z",
      "notBefore": "2015-01-09T21:10:03Z",
      "serialNumber": "be55a603167bf15f",
      "signatureAlgorithm": "SHA256withECDSA",
      "subjectDn": "OU=-,CN=betadraco02,O=Generated by Server Firmware,L=Raleigh,ST=North Carolina,C=US",
   },
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "text": "The request completed successfully.",
      "explanation": "",
      "recovery": {
```

```
         "text": "Information only; no action is required.",
         "URL": ""
      }
   }
}
```

/utils/countries

Use this REST API to return a list of country and region codes.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

HTTP methods

GET

GET /utils/countries

Use this method to return a list of common country and region codes.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://<management_server_IP>/utils/countries`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

Parameters	Type	Description
id	String	County code ID
abbreviation	String	ISO 3166 code for the country or region
name	String	Country or region name

The following example is returned if the request is successful.

```
[
   {
      "id": "7",
      "abbreviation": "AO",
      "name": "ANGOLA"
   },
```

```
    {
        "id": "11",
        "abbreviation": "AR",
        "name": "ARGENTINA"
    },
    {
        "id": "12",
        "abbreviation": "AM",
        "name": "ARMENIA"
    },
    ...,
    {
        "id": "242",
        "abbreviation": "VI",
        "name": "VIRGIN ISLANDS, U.S."
    },
    {
        "id": "246",,
        "abbreviation": "ZM"
        "name": "ZAMBIA"
    },
    {
        "id": "247",
        "abbreviation": "ZW",
        "name": "ZIMBABWE"
    }
]
```

/userAccounts

Use this REST API to retrieve information about all user accounts or create a new user account. *User accounts* are used to log in and manage the Lenovo XClarity Administrator and all chassis and servers that are managed by the Lenovo XClarity Administrator.

HTTP methods

GET, POST

GET /userAccounts

Use GET to retrieve information about all user accounts.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/userAccounts`

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array of objects	Each array element represents a user account
activeSessions	Integer	Number of currently active sessions for the user account
createTimestamp	String	Date and time when the account was created. The timestamp is returned in ISO 8601 format (for example, `2014-02-05T15:54:13Z`).
description	String	Description for the user account
groups	Array of strings	The list of role groups to which the user account belongs
id	String	Hashed index uniquely identifying a user account
lastLoginTimestamp	String	Date and time when the account was last successfully logged in. The timestamp is returned in ISO 8601 format (for example, `2014-02-05T15:54:13Z`).
ldapDn	String	User's LDAP distinguished name (for example, `"cn=USERID,ou=Users,dc=ibmbase,dc=com"`).
loginAttempts	Integer	Number of times that the user has attempted to log in
loginCount	Integer	Number of times the user has successfully logged in
modifyTimestamp	String	Date and time when the account was last modified. The timestamp is returned in ISO 8601 format (for example, `2014-02-05T15:54:13Z`).
PasswordChangeFirstAccess	Boolean	Indicates if the user is required to change the password on the initial access. This can be one of the following values. • **true**. The password must be changed. • **false**. The password does not have to be changed.
pwdAge	Integer	Number of seconds that have elapsed since the password was last changed
pwExpirationWarning	Boolean	Indicates if a password expiration warning is to be displayed when a user logs in. This can be one of the following values. • **true**. The password warning is to be displayed. • **false**. The password has not expired.
pwExpired	Boolean	Indicates if the password has expired. This can be one of the following values. • **true**. The password has expired. • **false**. The password has not expired.
reserved	Boolean	Indicates whether the user account is reserved for use by the XClarity Administrator. This can be one of the following values. • **true**. The user account is reserved. • **false**. The user account is not reserved.

Attributes	Type	Description
state	String	User-account state. This can be one of the following values. • **Active**. The user account is in an active state. • **Inactive**. The user account is in an inactive state (disabled). • **Locked**. The user account is locked
supervisor	Boolean	Indicates whether the user is a supervisor. This can be one of the following values. • **true**. The user account is a supervisor. • **false**. The user account is not a supervisor.
timeBeforeExpirationInDays	Integer	Number of days remaining before a password expires
userName	String	Name of the user account
userPw	String	User password. This value is always “NA.”
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": [{
      "activeSessions": 0,
      "createTimestamp": "2015-09-04T11:58:38Z",
      "description": "System Manager",
      "groups": ["lxc-sysmgr"],
      "id": "e1500a5d-7d78-464f-9b00-76d6ff8c3bc4",
      "lastLoginTimestamp": "",
      "ldapDn": "cn=SYSMGR_AXKVXE2I,ou=Users,dc=ibmbase,dc=com",
      "loginAttempts": 1,
      "loginCount": 1,
      "modifyTimestamp": "2015-09-04T11:58:38Z",
      "PasswordChangeFirstAccess": false,
      "pwdAge": 635303,
      "pwExpirationWarning": false,
      "pwExpired": false,
      "reserved": true,
      "state": "Active",
      "supervisor": false,
      "timeBeforeExpirationInDays": 82,
      "userName": "SYSMGR_AXKVXE2I",
      "userPw": "NA"
   },
   ...,
```

```
   {
      "activeSessions": 0,
      "createTimestamp": "2015-07-20T17:02:26Z",
      "description": "alanhawk",
      "groups": ["lxc-supervisor"],
      "id": "75d5aa42-266d-4241-ad5b-61f260dea827",
      "lastLoginTimestamp": "",
      "ldapDn": "cn=ALANHAWK,ou=Users,dc=ibmbase,dc=com",
      "loginAttempts": 0
      "loginCount": 0,
      "modifyTimestamp": "2015-07-20T17:02:26Z",
      "PasswordChangeFirstAccess": false,
      "pwdAge": 4591474,
      "pwExpirationWarning": false,
      "pwExpired": false,
      "reserved": false,
      "state": "Active",
      "supervisor": true,
      "timeBeforeExpirationInDays": 36,
      "userName": "ALANHAWK",
      "userPw": "NA",
   }],
   "result": "success",
   "messages": [{
      "id": "FQXHMSE0001I",
      "explanation": "",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```


POST /userAccounts

Use this method to create a user account.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/userAccounts`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
userName	Required	String	User name
userPw	Required	String	Initial account password
description	Optional	String	Description for the user account

Attributes	Required / Optional	Type	Description
groups	Required	Array of strings	List of role groups to which this user account belongs. This can be one of the following values. • **LXC-SUPERVISOR**. Includes the **lxc-supervisor** role. • **LXC-ADMIN**. Includes the **lxca-admin** role. • **LXC-SECURITY-ADMIN**. Includes the **lxc-security-admin** role. • **LXC-HW-ADMIN**. Includes the **lxc-hw-admin** role. • **LXC-FW-ADMIN**. Includes the **lxc-fw-admin** role. • **LXC-OS-ADMIN**. Includes the **lxc-os-admin** role. • **LXC-SERVICE-ADMIN**. Includes the **lxc-service-admin** role. • **LXC-HW-MANAGER**. Includes the **lxc-hw-manager** role. • **LXC-OPERATOR**. Includes the **lxc-operator** role. • **LXC-RECOVERY**. Includes the **lxc-recovery** role.
PasswordChangeFirstAccess	Optional	Boolean	Indicates if the password must be changed when the user initially accesses the XClarity Administrator. This can be one of the following values. • **true**. The password must be changed. • **false**. The password does not have to be changed. If not specified, the default value is taken from the user account settings (see /userAccountSettings).

Request example

```
{
    "userPw": "passwOrd",
    "userName": "test2",
    "description": "test2 description",
    "groups": ["lxc-admin"],
    "PasswordChangeFirstAccess": true
}
```

Response codes

Code	Description	Comments
201	Created	One or more new resources were successfully created.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	Each array element represents a user account
activeSessions	Integer	Number of currently active sessions for the user account
createTimestamp	String	Date and time when the account was created. The timestamp is returned in ISO 8601 forma (for example, `2014-02-05T15:54:13Z`).
description	String	Description for the user account
fullName	String	Descriptive name of the user account (for example: First M Last)
groups	Array of strings	List of role groups to which the user account belongs
id	String	Hashed index uniquely identifying a user account
lastLoginTimestamp	String	Date and time when the account was last successfully logged in. he timestamp is returned in ISO 8601 format (for example, `2014-02-05T15:54:13Z`).
ldapDn	String	User's LDAP distinguished name (for example, `"cn=USERID,ou=Users,dc=ibmbase,dc=com"`).
loginAttempts	Integer	Number of times that the user has attempted to log in
loginCount	Integer	Number of times the user has successfully logged in
modifyTimestamp	String	Date and time when the account was last modified. The timestamp is returned in ISO 8601 format (for example, `2014-02-05T15:54:13Z`).
PasswordChangeFirstAccess	Boolean	Indicates if the user is required to change the password on the initial access. This can be one of the following values. • **true**. The password must be changed. • **false**. The password does not have to be changed.
pwdAge	Integer	Number of days that have elapsed since the password was last changed
pwExpirationWarning	Boolean	Indicates if a password expiration warning is to be displayed when a user logs in. This can be one of following values. • **true**. The password warning is to be displayed. • **false**. The password has not expired.
pwExpired	Boolean	Indicates if the password has expired. This can be one of the following values. • **true**. The password has expired. • **false**. The password has not expired.
reserved	Boolean	Indicates whether the user account is reserved for use by the XClarity Administrator. This can be one of the following values. • **true**. The user account is reserved. • **false**. The user account is not reserved.
state	String	User-account status. This can be one of the following values. • **Active**. The user account is in an active state. • **Inactive**. The user account is in an inactive state (disabled). • **Locked**. The user account is locked
timeBeforeExpirationInDays	Integer	Number of days remaining before a password expires
userName	String	Name of the user account
userPw	String	Internal use only

Attributes	Type	Description
result	String	Request results. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.


```
{
    "response": {
        "createTimestamp": "2015-01-05T22:28:28Z",
        "description": "test2 description",
        "groups": ["lxc-admin"],
        "id": "478e6564-066a-4714-b734-e0f5c3073fbf",
        "lastLoginTimestamp": "",
        "ldapDn": "cn=TEST2,ou=Users,dc=ibmbase,dc=com",
        "loginAttempts": 0,
        "loginCount": 0,
        "modifyTimestamp": "2015-01-05T22:28:28Z",
        "PasswordChangeFirstAccess": true,
        "pwdAge": 0,
        "pwExpirationWarning": false,
        "pwExpired": true,
        "state": "Active",
        "timeBeforeExpirationInDays": 90,
        "userName": "TEST2",
        "userPw": "NA"
    },
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```


/userAccounts/*{id}*

Use this REST API to retrieve information about, modify, or delete a specific user account. *User accounts* are used to log in and manage the Lenovo XClarity Administrator and all chassis and servers that are managed by the XClarity Administrator.

HTTP methods

GET, PUT, DELETE

GET /userAccounts/*{id}*

Use GET to retrieve information about a specific user account.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/userAccounts/{id}`

where *{id}* is the unique ID of the user to be retrieved. To obtain the user ID, use the GET /userAccounts method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	Each array element represents a user account
activeSessions	Integer	Number of currently active sessions for the user account
createTimestamp	String	Date and time when the account was created. The timestamp is returned in ISO 8601 format, for example: `2014-02-05T15:54:13Z`
description	String	Description for the user account
groups	Array of strings	List of role groups to which the user account belongs
id	String	Hashed index uniquely identifying a user account
lastLoginTimestamp	String	Date and time when the account was last successfully logged in. The timestamp is returned in ISO 8601 format. For example: `2014-02-05T15:54:13Z`
ldapDn	String	User's LDAP distinguished name, for example: `"cn=USERID,ou=Users,dc=ibmbase,dc=com"`
loginAttempts	Integer	Number of times that the user has attempted to log in

Attributes	Type	Description
loginCount	Integer	Number of times the user has successfully logged in
modifyTimestamp	String	Date and time when the account was last modified. The timestamp is returned in ISO 8601 format, for example: `2014-02-05T15:54:13Z`
PasswordChangeFirstAccess	Boolean	Indicates if the user is required to change the password on the initial access. This can be one of the following values. • **true**. The password must be changed. • **false**. The password does not have to be changed.
pwdAge	Integer	Number of days that have elapsed since the password was last changed
pwExpirationWarning	Boolean	Indicates if a password expiration warning is to be displayed when a user logs in. This can be one of the following values. • **true**. The password warning is to be displayed. • **false**. The password has not expired.
pwExpired	Boolean	Indicates if the password has expired. This can be one of the following values. • **true**. The password has expired. • **false**. The password has not expired.
reserved	Boolean	Indicates whether the user account is reserved for use by the XClarity Administrator. This can be one of the following values. • **true**. The user account is reserved. • **false**. The user account is not reserved.
state	String	User-account state. This can be one of the following values. • **Active**. The user account is in an active state. • **Inactive**. The user account is in an inactive state (disabled). • **Locked**. The user account is locked
supervisor	Boolean	Indicates whether the user is a supervisor. This can be one of the following values. • **true**. The user account is a supervisor. • **false**. The user account is not a supervisor.
timeBeforeExpirationInDays	Integer	Number of days remaining before a password expires
userName	String	Name of the user account
userPw	String	User password. This value is always “NA.”
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages.
explanation	String	Additional information to clarify the reason for the message
id	String	Message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.


```
{
   "response": {
      "activeSessions": 0,
      "createTimestamp": "2015-09-16T19:11:43Z",
      "description": "",
      "groups": ["lxc-supervisor"],
      "id": "a74ce309-9167-4320-b7d0-83fb70df8131",
      "lastLoginTimestamp": "",
      "ldapDn": "cn=ADMINSITRATOR,ou=Users,dc=ibmbase,dc=com",
      "loginAttempts": 0,
      "loginCount": 0,
      "modifyTimestamp": "2015-09-16T19:11:43Z",
      "PasswordChangeFirstAccess": false,
      "pwdAge": 69837,
      "pwExpirationWarning": false,
      "pwExpired": false,
      "reserved": false,
      "state": "Active",
      "supervisor": true,
      "timeBeforeExpirationInDays": 89,
      "userName": "ADMIN",
      "userPw": "NA"
   },
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```


PUT /userAccounts/*{id}*

Use this method to modify the properties for a specific user account.

Tip: To change the password for a specific user account, use PUT /userAccounts/passwordChange

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/userAccounts/{id}`

where *{id}* is the unique ID of the user to be modified. To obtain the user ID, use the GET /userAccounts method.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
description	Optional	String	Description for the user account.
groups	Optional	Array of strings	List of role groups to which this user account belongs To obtain the role groups, use GET /roles.
userName	Optional	String	User-account name. This value must match an existing user name. To obtain the user names, use GET /userAccounts.

The following example modifies a user account.

```
{
    "description": "new description",
    "groups": ["lxc-supervisor","lxc-admin"],
    "userName": "JOE"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body. • An account with the specified user name exists already. • A violation of the security policy occurred.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information

Attributes	Type	Description
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "explanation": "The request to modify the user ID JOE was successful.",
      "id": "FQXHMSE0260I",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request to modify the user ID JOE completed successfully."
   }]
}
```

DELETE /userAccounts/*{id}*

Use this method to remove a specific user account from Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/userAccounts/{id}`

where *{id}* is the unique ID of the user to be removed. To obtain the user ID, use the GET /userAccounts method.

Query parameters

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "result": "success",
    "messages": [{
        "id": "FQXHMSE0270I",
        "text": "The request to delete the user ID TEST2 completed successfully.",
        "explanation": "The request to delete the user ID TEST2 was successful.",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        }
    }]
}
```

/userAccounts/passwordChange

Use this REST API to change the password for a specific user account that is currently logged in to Lenovo XClarity Administrator.

HTTP methods

PUT

PUT /userAccounts/passwordChange

Use this method to change the password for the user account that is currently logged in to the Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/userAccounts/passwordChange`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
confirmPassword	Required	String	Confirmation of the new password
newPassword	Required	String	New password
password	Required	String	Current password for the user account that is currently logged in

The following example change the password for the logged in user account.

```
{
    "confirmPassword": "theNewPasswOrd",
    "newPassword": "theNewPasswOrd",
    "password": "currentPasswOrd"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Object	
authenticated	Boolean	Indicates if the current password was authenticated successfully. This can be one of the following values. • **true**. The password was authenticated. • **false**. The password was not authenticated.
changed	Boolean	Indicates if the current password was changed successfully. This can be one of the following values. • **true**. The password was changed successfully. • **false**. The password was not changed successfully.
result	String	The request results. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
text	String	Message text associated with the message identifier

Attributes			Type	Description
	explanation		String	Additional information to clarify the reason for the message
	id		String	The message identifier of a returned message
	recovery		Array of objects	Recovery information
		text	String	User actions that can be taken to recover from the event
		URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
    "response": {
        "changed": true,
        "authenticated": true
    },
    "result": "success",
    "messages": [{
        "explanation": "",
        "id": "FQXHMSE0001I",
        "recovery": {
            "text": "Information only; no action is required.",
            "URL": ""
        },
        "text": "The request completed successfully."
    }]
}
```

/userAccountSettings

Use this REST API to retrieve or modify the security settings for all user accounts.

HTTP methods

GET, PUT

GET /userAccountSettings

Use GET to retrieve the current or default security settings for the user accounts.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/userAccountSettings`

Query parameters

Parameters	Re-quired / Optional	Description
default=*{Boolean}*	Optional	Indicates whether to return the default account security settings. This can be one of the following values. • **true**. Returns the default account security settings • **false**. (default) Returns the current account security settings

The following example returns the default account security settings.

```
GET https://192.0.2.0/userAccountSettings?default=true
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
response	Array	Each array element represents a user account
InactivityTimeout	Integer	Amount of time, in minutes, that a user session that is established with the Lenovo XClarity Administrator can be inactive before the user is logged off
LockoutTime	Integer	Minimum amount of time, in minutes, that must pass before a user that was locked out can attempt to log back in again
MaxConcurrentSessions	Integer	Maximum number of active sessions for a specific user that is allowed at any given time.
MaximumLoginFailures	Integer	Maximum number of times that a user can attempt to log in with an incorrect password before the user account is locked out. The number specified for the lockout period after maximum login failures determines how long the user account is locked out. Accounts that are locked cannot be used to gain access to the system even if a valid password is provided.
MaximumPasswordExpiration	Integer	Amount of time, in days, that a user can use a password before it must be changed. Smaller values reduce the amount of time for attackers to guess passwords
MaximumPasswordLength	Integer	Maximum number of characters that can be used to specify a valid password
MinimumChangeTime	Integer	Minimum amount of time, in hours, that must elapse before a user can change a password again after it was previously changed. The value specified for this setting cannot exceed the value specified for the password expiration period.
MinimumDifferentChars	Integer	Minimum number of characters that must be changed between the current password and a new password when the password is changed
MinimumPasswordLength	Integer	Minimum number of characters that can be used to specify a valid password

Attributes	Type	Description
PasswordChangeFirstAccess	Boolean	Indicates whether a user is required to change the password when the user logs in to XClarity Administrator for the first time. This can be one of the following values. • **true**. The password must be changed on initial log in. • **false**. The password is not required to be changed on initial log in.
PasswordExpirationWarningPeriod	Long	Amount of time, in days, before the password expiration date that users begin to receive warnings about the impending expiration of the user password
PasswordHistoryDepth	Integer	Minimum number of times that a user must enter a unique password when changing the password before the user can start to reuse passwords
SimplePasswordRules	Boolean	Indicates whether simple password rules are in effect. This can be one of the following values. • **true**. Simple password rules are in effect. • **false**. Simple password rules are not in effect.
MinPasswordComplexityRules	Integer	Number of complexity rules that must be followed when creating a new password Rules are enforced starting with rule 1, and up to the number of rules specified. For example, if the password complexity is set to 4, then rules 1, 2, 3 and 4 must be followed. If the password complexity is set to 2, then rules 1 and 2 must be followed. This can be a value from **0 – 5**. The default is **4**. XClarity Administrator supports the following password complexity rules. • (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed). • (2) Must contain at least one number (0 - 9). • (3) Must contain at least *two* of the following characters. – Uppercase alphabetic characters (A – Z) – Lowercase alphabetic characters (a – z) – Special characters. Only these characters are supported ; @ _ ! ' $ & + • (4) Must not repeat or reverse the user name. • (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed). If set to **0**, passwords are not required to comply with any complexity rules.
result	String	Request results. This can be one of the following values. • **success**. The request completed successfully. • **failure**. The request failed. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages

Attributes	Type	Description
explanation	String	Additional information to clarify the reason for the message
id	String	The message identifier of a returned message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available
text	String	Message text associated with the message identifier

The following example is returned if the request is successful.

```
{
   "response": {
      "InactivityTimeout": 1440,
      "LockoutTime": 60,
      "MaxConcurrentSessions": 3,
      "MaximumLoginFailures": 20,
      "MaximumPasswordExpiration": 90,
      "MaximumPasswordLength": 20,
      "MinimumChangeTime": 24,
      "MinimumDifferentChars": 2,
      "MinimumPasswordLength": 8,
      "PasswordChangeFirstAccess": true,
      "PasswordExpirationWarningPeriod": 5,
      "PasswordHistoryDepth": 5,
      "SimplePasswordRules": false,
      "MinPasswordComplexityRules": 5
   },
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSE0001I",
      "recovery": {
         "text": "Information only; no action is required.",
         "URL": ""
      },
      "text": "The request completed successfully."
   }]
}
```

PUT /userAccountSettings

Use this method to modify the security settings for the user accounts.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/userAccountSettings`

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
InactivityTimeout	Required	Integer	Amount of time, in minutes, that a user session that is established with the Lenovo XClarity Administrator can be inactive before the user is logged off. If set to 0, the web session never expires. The default is 1 minute.
LockoutTime	Required	Integer	Minimum amount of time, in minutes, that must pass before a user that was locked out can attempt to log back in again. If set to 0, the account remains locked until an administrator explicitly unlocks it. A setting of 0 might make your system more exposed to serious denial of service attacks, where deliberate failed login attempts can leave accounts permanently locked. The default is 60 minutes.
MaxConcurrentSessions	Required	Integer	Maximum number of active sessions for a specific user that is allowed at any given time. If set to 0, the number of allowed active sessions for a specific user is unlimited. The default is 3 sessions.
MaximumLoginFailures	Required	Integer	Maximum number of times that a user can attempt to log in with an incorrect password before the user account is locked out. The number specified for the lockout period after maximum login failures determines how long the user account is locked out. Accounts that are locked cannot be used to gain access to the system even if a valid password is provided. If set to 0, accounts are never locked. The failed login counter is reset to zero after a successful login. The default is 20 occurrences.
MaximumPasswordExpiration	Required	Integer	Amount of time, in days, that a user can use a password before it must be changed. Smaller values reduce the amount of time for attackers to guess passwords. If set to 0, passwords never expire. The default is 90 days. **Note:** This value applies only when the user accounts are managed locally on the management server using the internal authentication server. They are not used when the external authentication server is used.

Attributes	Required / Optional	Type	Description
MaximumPasswordLength	Required	Integer	Maximum number of characters that can be used to specify a valid password The default is 20 characters. **Note:** This value must be equal to or greater than the **MinimumPasswordLength** and the **MinimumDifferentCharacters** values.
MinimumChangeTime	Required	Integer	Minimum amount of time, in hours, that must elapse before a user can change a password again after it was previously changed. The value specified for this setting cannot exceed the value specified for the password expiration period. If set to 0, users can change passwords immediately. The default is 24 hours.
MinimumDifferentChars	Required	Integer	Minimum number of characters that must be changed between the current password and a new password when the password is changed The default is 2 characters. **Note:** This value must not exceed the **MaximumPasswordLength** value.
MinimumPasswordLength	Required	Integer	Minimum number of characters that can be used to specify a valid password The default is 8 characters. **Note:** This value must not exceed the **MaximumPasswordLength** value.
PasswordChangeFirstAccess	Required	Boolean	Specify if a user is required to change the password when the user logs in to XClarity Administrator for the first time. This can be one of the following values. • **true**. The user must change the password on initial access. • **false**. The user is not required to change the password on initial access.
PasswordExpirationWarningPeriod	Required	Long	Amount of time, in days, before the password expiration date that users begin to receive warnings about the impending expiration of the user password If set to 0, users are never warned. The default is 5 days.
PasswordHistoryDepth	Required	Integer	Minimum number of times that a user must enter a unique password when changing the password before the user can start to reuse passwords If set to 0, users can reuse passwords immediately. The default is 5 occurrences.

Attributes	Re-quired / Optional	Type	Description
SimplePasswordRules	Required	Boolean	This value must be set to **false**.
MinPasswordComplexityRules	Required	Integer	Number of complexity rules that must be followed when creating a new password Rules are enforced starting with rule 1, and up to the number of rules specified. For example, if the password complexity is set to 4, then rules 1, 2, 3 and 4 must be followed. If the password complexity is set to 2, then rules 1 and 2 must be followed. This can be a value from **0 – 5**. The default is **4**. XClarity Administrator supports the following password complexity rules. • (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed). • (2) Must contain at least one number (0 - 9). • (3) Must contain at least *two* of the following characters. – Uppercase alphabetic characters (A – Z) – Lowercase alphabetic characters (a – z) – Special characters. Only these characters are supported ; @ _ ! ' $ & + • (4) Must not repeat or reverse the user name. • (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed). If set to **0**, passwords are not required to comply with any complexity rules.

The following example modifies user security settings.

```
{
   "InactivityTimeout": 1440,
   "LockoutTime": 60,
   "MaxConcurrentSessions": 3,
   "MaximumLoginFailures": 20,
   "MaximumPasswordExpiration": 90,
   "MaximumPasswordLength": 20,
   "MinimumChangeTime": 24,
   "MinimumDifferentChars": 2,
   "MinimumPasswordLength": 8,
   "PasswordChangeFirstAccess": false,
   "PasswordExpirationWarningPeriod": 5,
   "PasswordHistoryDepth": 5,
   "SimplePasswordRules": false,
   "MinPasswordComplexityRules": 5
}
```

Response codes

Code	Description	Comments
204	No Content	The request completed successfully, but no response content is returned.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

Chapter 14. Service and support

The following resources are available for performing service and support functions.

/bulletinService

Use this REST API to return a list of bulletins from the last 30 days or modify bulletins options.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

HTTP methods

GET, PUT

GET /bulletinService

Use this method to return a list of bulletins from the last 30 days.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/bulletinService`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
bulletins		Array of objects	Information about each bulletin
	id	String	Bulletin ID
	category	String	Bulletin category
	component	String	Component associated with this bulletin

Attributes		Type	Description
	date	Long	Date when the bulletin was published
	date_range	String	Period in which the bulletin is valid This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
	end_date	Long	End date Bulletins that were published on specified date or later are included in this response.
	link	String	URL to detailed information about the bulletin
	message	String	Bulletin message
	severity	String	Bulletin severity
	start_date	Long	Start date Bulletins that were published on specified date or earlier are included in this response.
enabled		Boolean	Indicates whether receiving bulletins is enabled. This can be one of the following values. • **true**. Receiving bulletins is enabled. • **false**. Receiving bulletins is disabled.

The following example is returned if the request is successful.

```
{
   "bulletins": [{
      "id": 1,
      "category": "Planned Outage",
      "component": "Call home",
      "date": 1611292020000,
      "date_range": "2021-07-23 - 2021-08-31",
      "end_date": 1630393200000,
      "link": "[https://datacentersupport.lenovo.com/us/en/products/solutions-and-software/]
               software/lenovo-xclarity/lxca/solutions/ht507888-how-to-upload-a-file-to-
               lenovo-data-center-support",
      "message": "There is a planned outage of the call home servers from 7/23 ??? 8/31.
               During this time, call home requests will fail. It is recommended that you
               check for alerts on your LXCA to see if any service tickets should be opened
                manually.",
      "severity": "Call home",
      "start_date": 1627023600000
   }],
   "enabled": true
}
```

PUT /bulletinService

Use this method to modify bulletins options.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/bulletinService`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
enabled	Required	String	Indicates whether receiving bulletins from Lenovo is enabled. This can be one of the following values. • **true**. Receiving bulletins is enabled. • **false**. Receiving bulletins is disabled.

The following example enables receiving bulletins.

```
{
   "enabled": "true"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/callhome/endPointsPMR

Use this REST API to retrieve or delete information about service tickets that were generated by Call Home.

HTTP methods

GET, DELETE

GET /callhome/endPointsPMR

Use this method to return information about all service tickets that were generated by Call Home.

For service tickets that were generated by a support service other than Call Home, use GET /service/tickets.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/callhome/endPointsPMR`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
componentID	String	Component ID of the service ticket
eventID	String	ID of the event that generated service ticket
id	String	ID of the service ticket
lastUpdate	String	Timestamp of the last update to the service ticket
sourceID	String	Source ID of the generated event
state	String	Current state of the service ticket. This can be one of the following values. • **Processing** • **Answered** • **Cancelled** • **Closed** • **Created** • **Error** • **Initialized** • **Rejected** • **Submitted** • **Unknown** • **Waiting**
type	String	Type of the service ticket. This can be one of the following values. • **Normal** • **Test**
uid	String	UID of the service ticket
uri	String	URL where the service ticket can be accessed from the Internet

The following example is returned if the request is successful.

```
[{
   "eventID": "FQXHMSS1045I",
   "componentID": "",
   "id": "1",
   "lastUpdate": "2015-03-03T12:56:37Z",
   "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
   "state": "Processing",
   "type": "Test",
   "uid": "USEODSBNWWS",
   "uri": "https://www.lenovo.com:443/services/projects/ecc/iepd/services/ProblemReport
          ?vSessionId=PS120150303112132790 42"
}]
```

DELETE /callhome/endPointsPMR

Use this method to delete one or more service tickets that were generated by Call Home.

For service tickets that were generated by a support service other than Call Home, use DELETE /service/tickets/*{record_id_list}*.

Authentication

Authentication with username and password is required.

Request URL

```
DELETE https://{management_server_IP}/callhome/endPointsPMR
```

Query parameters

Parameters	Required / Optional	Description
list=*{problem_record_UID>*	Required	UID of one or more service tickets to be deleted, separated by a comma To obtain a list of problem-record UIDs, use the GET /callhome/endPointsPMR method.

The following example deletes a list of service tickets.

```
GET https://192.0.2.0/events/callhome/endPointsPMR?list=USE0DSBNWWS,USE0DSBNXYZ
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier

Attributes			Type	Description
	explanation		String	Additional information to clarify the reason for the message
	recovery		Array of objects	Recovery information
		text	String	User actions that can be taken to recover from the event
		URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "explanation": "",
      "id": "FQXHMSS1064I",
      "recovery": {
         "text": "",
         "url": ""
      },
      "text": "The specified service tickets have successfully been deleted."
   }]
}
```

/callhome/endPointsPMR/*{record_id}*

Use this REST API to retrieve information about a specific service ticket that were generated by Call Home.

HTTP methods

GET

GET /callhome/endPointsPMR/*{record_uid}*

Use this method to return information about a specific service ticket that were generated by Call Home.

For service tickets that were generated by a support service other than Call Home, use GET /service/tickets/*{record_id}*.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/callhome/endPointsPMR/{record_uid}`

where *{record_uid}* is the UID of the service ticket to be retrieved. To obtain the service ticket UID, use the GET /callhome/endPointsPMR method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
componentID	String	Component ID of the service ticket
eventID	String	ID of the event that generated service ticket
id	String	ID of the service ticket
lastUpdate	String	Timestamp of the last update to the service ticket
sourceID	String	Source ID of the generated event
state	String	Current state of the service ticket. This can be one of the following values. • **Processing** • **Answered** • **Cancelled** • **Closed** • **Created** • **Error** • **Initialized** • **Rejected** • **Submitted** • **Unknown** • **Waiting**
type	String	Type of the service ticket. This can be one of the following values. • **Normal** • **Test**
uid	String	UID of the service ticket
uri	String	URL where the service ticket can be accessed from the Internet

The following example is returned if the request is successful.

```
[{
   "eventID": "FQXHMSS1045I",
   "componentID": "",
   "id": "1",
   "lastUpdate": "2015-03-03T12:56:37Z",
   "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
   "state": "Processing",
   "type": "Test",
   "uid": "USEODSBNWWS",
   "uri": "https://www.lenovo.com:443/services/projects/ecc/iepd/services/ProblemReport
          ?vSessionId=PS120150303112132790 42"
}]
```

/callhome/endPointsPMRStatus

Use this REST API to retrieve the current status for one or more service tickets that were generated by Call Home.

HTTP methods

GET

GET /callhome/endPointsPMRStatus

Use this method to return the current status for one or more service tickets that were generated by Call Home.

This method returns the job ID for the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job.

For service tickets that were generated by a support service other than Call Home, use GET /service/tickets/*{record_id}*.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/callhome/endPointsPMRStatus
```

Query parameters

Parameters	Required / Optional	Description
list=*{problem_record_id}*	Optional	List of IDs for service tickets to be retrieved, separated by a comma (for example `list="USEODSBNWWS","USEODSBNXYZ"`) If this query parameter is not specified, all PMRs are returned. To obtain a list of service-ticket UIDs, use the GET /callhome/endPointsPMR method.

The following example retrieves the current status for all Call Home service tickets.

```
GET https://192.0.2.0/callhome/endPointsPMRStatus
```

The following example retrieves the current status for two Call Home service tickets.

```
GET https://192.0.2.0/callhome/endPointsPMRStatus?list="USEODSBNWWS","USEODSBNXYZ"
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
followJobPatch	String	Job URI

The following example is returned if the request was successful. In this example, job ID 12 can be used to monitor the status and progress of the job.

```
{
    "followJobPath": "/jos/32"
```

/callhome/endPoints/list

Use this REST API to retrieve information about all archives that have been collected for the managed devices.

HTTP methods

GET

GET /callhome/endPoints/list

Use this method to return information about all archives that have been collected for the managed devices.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/callhome/endPoints/list`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
chassisName	String	Name of the managed device (regardless of the type) or the UUID if the device is not managed
collectDate	String	Timestamp when the archive file was created
eventID	String	ID of the event that generated archive file
fileName	String	Name of the archive file

Attributes	Type	Description
id	String	Counter
uid	String	UID of the FFDC archive file

The following example is returned if the request is successful.

```
[{
   "chassisName": "9BB59256A8B111E19F0EF3DD1922EE5B",
   "collectDate": "2015-03-04T11:58:04Z"
   "eventID": "40040201",
   "fileName": "8721_A1G_06D7374_CMM_20150304_065557.tgz",
   "id": "1",
   "uid": "9BB59256A8B111E19F0EF3DD1922EE5B/40040201/8721_A1G_06D7374_CMM_20150304_065557.tgz",
},
{
   "chassisName": "9BB59256A8B111E19F0EF3DD42643BC ",
   "collectDate": "2015-08-19T18:37:19Z",
   "eventID": "40040202",
   "fileName": "8721_HC1_06NTTY8_CMM_20150819_103641.tgz",
   "id": "2",
   "uid": "9BB59256A8B111E19F0EF3DD42643BC/40040202/8721_HC1_06NTTY8_CMM_20150819_103641.tgz"
}]
```

/callhome/pmrattach/*{record_id}*

Use this REST API to upload a diagnostic archive file for a specific service ticket that were generated by Call Home or to add an existing diagnostic archive file to a Call Home service ticket.

HTTP methods

POST

POST /callhome/pmrattach/*{record_uid}*

Use this method to upload a diagnostic archive file for a specific service ticket that were generated by Call Home or to add an existing diagnostic archive file to a Call Home service ticket.

This method starts a job that runs in the background to perform the operation. The response body includes a URI that represents the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job. If a job was not successfully started, refer to the response code and response body for details.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/callhome/pmrattach/{record_uid}`

where *{record_uid}* is the UID of the service ticket to be retrieved. To obtain the service-ticket UID, use the GET /callhome/endPointsPMR method.

Query parameters

Parameters	Required / Optional	Description
fileUID = *{file_ID}*	Optional	ID of the existing diagnostic archive file to be added to the target service ticket To obtain the file ID, use the GET /callhome/endPoints/list method.

The following example upload a diagnostic archive file for a specific Call Home service ticket.

```
GET https://192.0.2.0/callhome/pmrattach/USE0DSBNWWS?fileUID=20AE4F4200D911E890EB7ED30AEBD9DF/
20AE4F4200D911E890EB7ED30AEBD9DF/combined_7X02CTO1WW_J300518G_xcc_230912-090509.tzz"
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
followJobPath	String	Job URI

The following example is returned if the request is successful.

```
{
   "followJobPath": "/jobs/74"
}
```

/ffdc/endpoint/*{uuid}*

Use this REST API to collect and export the first failure data capture (FFDC) data for a specific managed device (CMM, server, storage device, or switch).

HTTP methods

GET

GET /ffdc/endpoint/*{uuid}*

Use this method to collect and export the first failure data capture (FFDC) data for a specific managed device (CMM, server, storage device, or switch).

This method returns a URI that contains the job ID for the job that is created to perform this request. You can use GET /tasks/*{job_list}* to monitor the status and progress of the job.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/ffdc/endpoint/{uuid}
```

where *{uuid}* is the UUID of the target device. To obtain the device UUID, use the GET /cmms, GET /nodes, or GET /switches method.

Query parameters

You must specify at least one of the following query parameters.

Parameters	Required / Optional	Description
componentName=*{name}*	Optional	Component name of the device. This is usually the name that is displayed in the devices list on the Service and Support page in the web interface.
fileUID=*{file_ID}*	Optional	Unique identifier of an already-downloaded FFDC file

The following example exports FFDC data for the SN component:

```
GET https://192.0.2.0/ffdc/device/183F4A35B84C47FC820F11989D2CEA27?componentName=SN
```

Request body

None

Response codes

Code	Description	Comments
201	Created	One or more new resources were successfully created.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

If the request was successful (if the response code is 200), the following attribute is returned in the response body.

Attributes	Type	Description
jobURL	String	URL for this job, including the job ID

The following example is returned if the request is successful. This example shows the URI that is returned which contains the job ID that you can use to monitor the job's progress and status. In this example, the job ID is 16.

```
{ "jobURL":"/jobs/16" }
```

If the request failed (if the response code is 400, 404, or 500), the following attributes are returned in the response body.

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request failed.

```
{
   "result":"fail",
   "messages":[{
      "explanation":"The required archive might have been erased.",
      "id":"FQXHMSS1064J",
      "recovery":{
         "text":"Please retry to download the archive.",
         "url":"",
      }
      "text":"The required archive is not available."
   }]
}
```

/service/callHome/pmr/notes/*{ticket_id}*

Use this REST API to send a note for a specific service ticket to the Lenovo Support Center.

HTTP methods

POST

POST /service/callHome/pmr/notes/*{ticket_id}*

Use this method to send a note to the Lenovo Support Center for a specific service ticket.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/service/callHome/pmr/notes/{ticket_id}`

where *{ticket_id}* is the UID of the service ticket to be retrieved. To obtain the service ticket UID, use GET /callhome/endPointsPMR.

Query parameters

None

Request body

Parameters	Required / Optional	Type	Description
content	Required	String	Note content
title	Required	String	Note title

The following example sends a note.

```
{
   "content" : "Final test 5",
   "title" : "Test 5"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/service/callHomeGeneral

Use this REST API to retrieve or modify the general Call Home configuration settings or to delete general Call Home configuration and associated service forwarders.

HTTP methods

PUT

PUT /service/callHomeGeneral

Use this method to modify the general Call Home configuration settings.

This request modifies the general Call Home configuration. When this request is made for the first time, it creates an associated Default Call Home forwarder that matches all devices from the management server.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/service/callHomeGeneral`

Query parameters

None

Request body

You can specify contact information using one of the following sets of attributes.

Table 106. Primary and secondary contacts

Attributes	Required / Optional	Type	Description
primaryContact	Optional	Object	Information about the primary contact
fullName	Optional	String	Contact name
companyName	Optional	String	Company name
contactEmail	Optional	String	Contact email address
contactPhone	Optional	String	Contact phone number
streetAddress	Optional	String	Address
city	Optional	String	City
stateProvince	Optional	String	State or province
postalCode	Optional	String	Postal code
country	Optional	String	Country
preferredContactMethod	Optional	String	Preferred contact method key To get at list of keys for supported contact methods, use GET /service/contactMethods.
secondaryContacts	Optional	Array of objects	Information about one or more secondary contacts
fullName	Optional	String	Contact name
companyName	Optional	String	Company name
contactEmail	Optional	String	Contact email address
contactPhone	Optional	String	Contact phone number
streetAddress	Optional	String	Address
city	Optional	String	City
stateProvince	Optional	String	State or province
postalCode	Optional	String	Postal code
country	Optional	String	Country or region
preferredContactMethod	Optional	String	Preferred contact method key To get at list of keys for supported contact methods, use GET /service/contactMethods.

The following example modifies the general Call Home configuration settings.

```
{
   "primaryContact": {
      "fullName": "John",
```

```
      "companyName": "SomeCompany",
      "country": "RO",
      "contactEmail": "john@company.com",
      "contactPhone": "+41234567890",
      "streetAddress": "Calea Floreasca 169A",
      "city": "Bucharest",
      "stateProvince": "BU",
      "postalCode": "012345"
      "preferredContactMethod": "any"
   },
   "secondaryContacts": [{
      "fullName": "Jane",
      "companyName": "SomeCompany",
      "contactEmail": "jane@company.com",
      "contactPhone": "+41234567891",
      "country": "RO",
      "streetAddress": "Calea Floreasca 169A",
      "city": "Bucharest",
      "stateProvince": "BU",
      "postalCode": "012345"
      "preferredContactMethod": "email"
   }]
}
```

Table 107. Contact and system information

Attributes	Required / Optional	Type	Description
companyName	Optional	String	Contact company
contactName	Optional	String	Contact name
email	Optional	String	Contact email
phoneNumber	Optional	String	Contact phone number
address	Optional	String	Contact address
city	Optional	String	Contact city
stateProvince	Optional	String	Contact state or province
zipCode	Optional	String	Contact zip code
countryAbv	Optional	String	Contact country or region abbreviation (for example, RO for Romania)
systemCompany	Optional	String	Contact company for the device
systemName	Optional	String	Contact name for the device
systemEmail	Optional	String	Contact email address for the device
systemPhoneNumber	Optional	String	Contact phone number for the device
systemAddress	Optional	String	Address where the device is located
systemCity	Optional	String	City where the device is located
systemZipCode	Optional	String	Zip code where the device is located

Table 107. Contact and system information (continued)

Attributes	Re-quired / Optional	Type	Description
systemStateProvince	Optional	String	State where the device is located
systemCountryAbv	Optional	String	Country or region abbreviation where the device is located

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   messages: [
      0: {
         explanation: "",
         id: "FQXHMSS1029I",
         recovery: {
            text: "",
            url: ""
         },
```

```
         text: "The configuration for Call Home was successfully saved. Forwarder 'Default Call Home'
            was created with this configuration.",
         result: "success"
      }
   ]
}
```

/service/contactMethods

Use this REST API to retrieve all possible contact methods for Call Home.

HTTP methods

GET

GET /service/contactMethods

Use this method to return all possible contact methods for Call Home.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/service/contactMethods`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
key	String	Contact method key
name	String	Contact method name

The following example is returned if the request is successful.

```
[{
   "key": "Any",
   "name": "Any"
},
{
   "key": "Email",
   "name": "Email"
},
{
```

```
   "key": "Phone",
   "name": "Phone"
}]
```

/service/customerNumber

Use this REST API to retrieve and configure default Lenovo customer number that is used when reporting problems with Lenovo XClarity Administrator.

HTTP methods

GET, POST

GET /service/customerNumber

Use this method to return the default Lenovo customer number that is used when reporting problems with Lenovo XClarity Administrator.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/service/customerNumber`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
customerNumber	String	Lenovo customer number

The following example is returned if the request is successful.

```
{
   "customerNumber" : "234567890dsf"
}
```

POST /service/customerNumber

Use this method to configure the default Lenovo customer number that is used when reporting problems with Lenovo XClarity Administrator. If a customer number is already defined, it is overwritten with the new number.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/service/customerNumber`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
customerNumber	Required	String	Lenovo customer number You can find your customer number in the proof-of-entitlement email that you received when you purchased Lenovo XClarity Pro.

The following example is returned if the request is successful.

```
{
   "customerNumber" : "234567890dsf"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

/service/forwarders/settings

Use this REST API to enable, disable, or retrieve information about whether service data is forwarded to the preferred service provider when a serviceable event that is on the list of excluded events occurs

HTTP methods

GET, PUT

GET /service/forwarders/settings

Use this method to return information about whether service data is forwarded to the preferred service provider when a serviceable event that is on the list of excluded events occurs.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/service/forwarders/settings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
excludeEvents	Boolean	Indicates whether service data is automatically forwarded when an excluded serviceable event occurs. This can be one of the following values. • **true**. Forwards excluded serviceable events • **false**. Does not forward excluded serviceable events.

The following example is returned if the request is successful.

```
{
   "excludeEvents":"true"
}
```

PUT /service/forwarders/settings

Use this method to enable or disable forwarding service data to the preferred service provider when a serviceable event that is on the list of excluded events occurs.

Authentication

Authentication with username and password is required.

Request URL

```
PUT https://{management_server_IP}/service/forwarders/settings
```

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
excludeEvents	Required	Boolean	Indicates whether service data is automatically forwarded when an excluded serviceable event occurs. This can be one of the following values. • **true**. Forwards excluded serviceable events • **false**. Does not forward excluded serviceable events

The following example enables forwarding excluded serviceable events to the preferred service provider

```
{
   "excludeEvents":"true"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/service/tickets

Use this REST API to retrieve information about all service tickets that were generated by a support service other than Call Home.

HTTP methods

GET, POST

GET /service/tickets

Use this method to return information about all service tickets that were generated by a support service other than Call Home.

Note: For service tickets that were generated by Call Home, use GET /callhome/endPointsPMR.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/service/tickets
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes		Type	Description
tickets		Array of objects	Information about each service ticket
	creationDate	Long	Timestamp when the service ticket was created
	deviceUUID	String	UUID of the device that generated service ticket
	eventID	String	ID of the event that generated service ticket
	eventSequenceID	Integer	Sequence ID of the event that generated the service ticket
	lastUpdateDate	Long	Timestamp when the service ticket was updated last
	machineModel	String	Model of the device that generated service ticket
	machineType	String	Machine type of the device that generated service ticket
	serialNumber	String	Serial number of the device that generated service ticket
	status	String	Status of the service ticket. This can be one of the following values. • **Processing** • **Answered** • **Cancelled** • **Closed** • **Created** • **Error** • **Initialized** • **Rejected** • **Submitted** • **Unknown** • **Waiting**
	ticketID	String	ID of the service ticket
	ticketType	String	Support service that generated the service ticket. This can be one of the following values. • **Cherwell** • **Service Now**

The following example is returned if the request is successful.

```
{"tickets":[{
    "creationDate": "1366146000000",
    "deviceUUID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "eventID": "FQXHMSS1045M",
    "eventSequenceID": 120,
    "lastUpdateDate": "1366147000000",
    "machineModel": "AC1",
    "machineType": "7903",
    "serialNumber": "NANC009",
    "status": "active",
    "ticketID": "USE0DSBNWWS",
    "ticketType": "Cherwell"
}]
}
```


POST /service/tickets

Use this method to create a service ticket that was generated by a support service other than Call Home.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/service/tickets`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
creationDate	Required	Long	Timestamp when the service ticket was created
deviceUUID	Required if **machineType** and **serialNumber** are not specified. Otherwise optional.	String	UUID of the device that generated service ticket This can be the UUID of a managed device or a device that is not managed by XClarity Administrator.
eventID	Optional	String	ID of the event that generated service ticket
eventSequenceID	Optional	Integer	Sequence ID of the event that generated the service ticket
lastUpdateDate	Optional	Long	Timestamp when the service ticket was updated last

Attributes	Required / Optional	Type	Description
machineModel	Required if **deviceUUID** is not specified. Otherwise optional.	String	Model of the device that generated service ticket
machineType	Required if **deviceUUID** is not specified. Otherwise optional.	String	Machine type of the device that generated service ticket
serialNumber	Required if **deviceUUID** is not specified. Otherwise optional.	String	Serial number of the device that generated service ticket
status	Required	String	Status of the service ticket. This can be one of the following values. • **Processing** • **Answered** • **Cancelled** • **Closed** • **Created** • **Error** • **Initialized** • **Rejected** • **Submitted** • **Unknown** • **Waiting**
ticketID	Required	String	ID of the service ticket
ticketType	Required	String	Support service that generated the service ticket. This can be one of the following values. • **Cherwell** • **Service Now**

The following example creates a service ticket that was generated by a support service other than Call Home.

```
{
   "creationDate": "1366146000000",
```

```
   "deviceUUID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
   "eventID": "FQXHMSS1045M",
   "eventSequenceID": 120,
   "lastUpdateDate": "1366147000000",
   "machineModel": "AC1",
   "machineType": "7903",
   "serialNumber": "NANC009",
   "status": "Created",
   "ticketID": "USEODSBNWWS",
   "ticketType": "Cherwell"
}
```


Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/service/tickets/*{record_id}*

Use this REST API to retrieve information about, create, modify, or delete a specific service ticket that was generated by a support service other than Call Home.

HTTP methods

GET, PUT, DELETE

GET /service/tickets/*{record_id}*

Use this method to return information about a specific service ticket that was generated by a support service other than Call Home.

Note: For service tickets that were generated by Call Home, use GET /callhome/endPointsPMR/*{record_uid}*.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/service/tickets/{record_id}`

where *{record_id}* is the ID of the problem record. To obtain the problem-record ID, use GET /service/tickets.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
creationDate	Long	Timestamp when the service ticket was created
deviceUUID	String	UUID of the device that generated service ticket
eventID	String	ID of the event that generated service ticket
eventSequenceID	Integer	Sequence ID of the event that generated the service ticket
lastUpdateDate	Long	Timestamp when the service ticket was updated last
machineModel	String	Model of the device that generated service ticket
machineType	String	Machine type of the device that generated service ticket
serialNumber	String	Serial number of the device that generated service ticket
status	String	Status of the service ticket. This can be one of the following values. • **Processing** • **Answered** • **Cancelled** • **Closed** • **Created** • **Error** • **Initialized** • **Rejected** • **Submitted** • **Unknown** • **Waiting**
ticketID	String	ID of the service ticket
ticketType	String	Support service that generated the service ticket. This can be one of the following values. • **Cherwell**

The following example is returned if the request is successful.


```
{
    "creationDate": "1366146000000",
    "deviceUUID": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    "eventID": "FQXHMSS1045M",
    "eventSequenceID": 120,
    "lastUpdateDate": "1366147000000",
    "machineModel": "AC1",
    "machineType": "7903",
    "serialNumber": "NANC009",
    "status": "active",
    "ticketID": "USE0DSBNWWS",
    "ticketType": "Cherwell"
}
```

PUT /service/tickets/*{record_id}*

Use this method to modify the status of a service ticket that was generated by a support service other than Call Home.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/service/tickets/{record_id}`

where *{record_id}* is the ID of the service ticket. To obtain the service ticket ID, use GET /service/tickets.

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
status	Required	String	Status of the service ticket. This can be one of the following values. • **Processing** • **Answered** • **Cancelled** • **Closed** • **Created** • **Error** • **Initialized** • **Rejected** • **Submitted** • **Unknown** • **Waiting**

The following example sets the service-ticket status to Created.

```
{
   "status": "Created"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /service/tickets/*{record_id_list}*

Use this method to delete one or more specific service tickets that were generated by a support service other than Call Home.

Note: For service tickets that were generated by Call Home, use DELETE /callhome/endPointsPMR.

Authentication

Authentication with username and password is required.

Request URL

`DELETE https://{management_server_IP}/service/tickets/{record_id_list}`

where *{record_id_list}* is one or more problem-record IDs, separated by a comma, To obtain the problem-record IDs, use GET /service/tickets.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/warranty

Use this REST API to refresh and retrieve the warranty data.

HTTP methods

GET, PUT

GET /warranty

Use this method to return or download the warranty information.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/warranty`

Query parameters

Parameters	Required / Optional	Description
formatType=csv	Optional	Returns information in CSV format
outputFormat=v2	Optional	Returns warranty information for all device, whether they are covered under a warranty or not. If a device is not under warranty, the warrant type is “Not Available.”

The following example returns warranty information for devices that are covered under a warranty.

```
GET https://192.0.2.0/warranty
```

The following example returns a CSV file that contains warranty information for devices that are covered under a warranty.

```
GET https://192.0.2.0/warranty?formatType=csv
```

The following example returns warranty information for devices, including devices that are not covered under a warranty.

```
GET https://192.0.2.0/warranty?outputFormat=v2
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

Table 108. Default output format

Attributes	Type	Description
children	Array of objects	Warranty information of each component of this device
children	Array of objects	Warranty information for each component in this device, using the same attributes as the parent
id	String	Component UUID
deviceType	String	Component type. This can be one of the following values. • **nodes**
detailsURL	String	
deviceName	String	Device name
deviceType	String	Device type. This can be one of the following values. • **Chassis** • **Edge Server**. ThinkSystem SE server • **IBM Tape**. IBM tape library • **Lenovo ThinkServer** • **Lenovo Storage** • **Rackswitch** • **Rack-Tower Server**. ThinkSystem SD, ThinkSystem SR, or ThinkSystem ST, System x, Converged, or NeXtScale server

Table 108. Default output format (continued)

Attributes	Type	Description
endDate	String	Warranty end date
groupName	Array of strings	List of names of the resource groups to which the device belongs
groupUUID	Array of strings	List of UUIDs of the resource groups to which the device belongs
id	String	Device UUID
machineModel	String	Machine model
machineType	String	Machine type
serialNumber	String	Device serial-number **Note:** For RackSwitch devices, this is the entitled serial number.
startDate	String	Warranty start date
status	String	Warranty status. This can be one of the following values. • **active** • **expired** • **NA**. Not applicable
warrantyType	String	Warranty type. This can be one of the following values. • **3PL** • **3XL** • **MS12** • **NA**. Not applicable

The following example is returned if the request is successful when the default output format is returned.


```
[{
    "children": [{
       "children": [{
          "children": [],
          "detailsURL": "compDetails/ITE/B672DEFF0F6C11E4A603DD6AA23A728A",
          "deviceName": "IMM2-40f2e990d8b1",
          "deviceType": "ITE",
          "endDate": "NA",
          "groupName": ["Not Available"],
          "groupUUID": [""],
          "id": 32184,
          "machineModel": "AC1",
          "machineType": "9532",
          "serialNumber": "DSYH03P",
          "startDate": "NA",
          "status": "NA",
          "warrantyType": "NA"
       }],
       "deviceType": "nodes",
       "id": "56"
    }],
    "deviceName": "MM5CF3FC25D733",
    "deviceType": "Chassis",
    "detailsURL": "compDetails/Chassis/3C8EEA1291FE4523985396B6266513FB",
    "endDate": "NA",
    "groupName": ["Not Available"],
    "groupUUID": [""],
    "id": 32183,
```

```
   "machineModel": "HC1",
   "machineType": "8721",
   "serialNumber": "23DWN32",
   "startDate": "NA",
   "status": "NA",
   "warrantyType": "NA"
}]
```


Table 109. V2 output format

Attributes	Type	Description
available	Boolean	
children	Array of objects	Warranty information of each component of this device This object contains the same attributes as the top level attributes.
deviceName	String	Device name
deviceURI	String	Device URI
expirationDate	String	Warranty end date
groups	Array of strings	List of names of the resource groups to which the device belongs
groupsUUIDs	Array of strings	List of UUIDs of the resource groups to which the device belongs
mtm	String	Device machine type model
productName	String	Device product name
serialNumber	String	Device serial-number **Note:** For RackSwitch devices, this is the entitled serial number.
startDate	String	Warranty start date
status	String	Warranty status. This can be one of the following values. • **active** • **expired** • **NA**. Not applicable
uuid	String	Device UUID
warrantyNumber	String	Warranty type. This can be one of the following values. • **3PL** • **3XL** • **MS12** • **NA**. Not applicable

The following example is returned if the request is successful when the default output format is returned.


```
{
   "available": true,
   "children": [{
      "available": true,
      "children": [],
      "deviceName": "Flex x240 M5 #1",
      "deviceURI": "/compDetails/ITE/22907D8F413811E7A840000E1E7D58F0",
      "expirationDate": "2020-05-27",
      "groups": [],
      "groupsUUIDs": [],
      "mtm": "9532/AC1",
      "productName": "Lenovo Flex System x240 M5 Compute Node",
      "serialNumber": "S40ET01",
```

```
      "startDate": "2017-05-28",
      "status": "Expired",
      "uuid": "22907D8F413811E7A840000E1E7D58F0",
      "warrantyNumber": "3XL"
   }],
   "deviceURI": "/chassisMap/2485D17451AD4590B236AD55DE77691B",
   "expirationDate": "2020-05-20",
   "groups": [],
   "groupsUUIDs": [],
   "deviceName": "Chassis.15",
   "mtm": "8721/HC2",
   "productName": "Lenovo Flex System Enterprise Chassis",
   "serialNumber": "S40EFR1",
   "startDate": "2017-05-21",
   "status": "Expired",
   "uuid": "2485D17451AD4590B236AD55DE77691B",
   "warrantyNumber": "3XL"
}
```


PUT /warranty

Use this method to refresh the warranty information on the management server.

Authentication

Authentication with username and password is required.

Request URL

`PUT https://{management_server_IP}/warranty`

Query parameters

None

Request body

Attributes	Required / Optional	Type	Description
refresh	Required	String	Type of refresh to perform. This can be one of the following values. • **normal**. Updates the warranty information based on the managed devices. • **total**. Updates the warranty information just like the normal refresh and attempts to rerun all the previously failed requests to the Lenovo warranty service.
groupUUID	Optional	Array of strings	Refreshes warranty information for one or more resource groups, specified by UUID

The following example refreshes the warranty information for two groups.


```
{
   "groupUUID": ["AAAAAAAAAAAAAAAAAAAAAAAA","BBBBBBBBBBBBBBBBBBBBBBBB"],
   "refresh": "normal"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
children	Array of objects	Warranty information for each component in this device
deviceName	String	Device name
deviceType	String	Component type. This can be one of the following values. • **Chassis** • **Edge Server**. ThinkSystem SE server • **IBM Tape**. IBM tape library • **Lenovo ThinkServer** • **Lenovo Storage** • **Rackswitch** • **Rack-Tower Server**. ThinkSystem SD, ThinkSystem SR, or ThinkSystem ST, System x, Converged, or NeXtScale server
endDate	String	Warranty end date
groupName	String	Name of the resource groups to which the device belongs. If the archive does not belong to a resource group, the value is “Not Available.”
groupUUID	String	UUID of the resource groups to which the device belongs
id	String	UUID of this object
serialNumber	String	Device serial-number **Note:** For RackSwitch devices, this is the entitled serial number.
startDate	String	Wwarranty start date
status	String	Warranty status. This can be one of the following values. • **active** • **expired** • **NA**. Not applicable
warrantyType	String	Warranty type. This can be one of the following values. • **3PL** • **3XL** • **MS12** • **NA**. Not applicable

The following example is returned if the request is successful.


```
{
   "children": [],
   "deviceName": "Chassis_1",
   "deviceType": "Chassis",
   "endDate": "",
   "groupName": ["Not Available"],
```

```
   "groupUUID": [],
   "id": "00DD973D1C2CE511B19E3C18A000F4F0",
   "serialNumber": "23FBX24",
   "startDate": "",
   "status": "Expired",
   "warrantyType": ""
}
```


/warranty/settings

Use this REST API to retrieve and modify global warranty settings.

HTTP methods

GET, PUT

GET /warranty/settings

Use this method to return global warranty settings.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/warranty/settings`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
warrantyThreshold	Integer	Number of days before the warranty expires for a managed device when you want to be warned about the expiration. The default is 30 days.

The following example is returned if the request is successful.


```
{
   "warrantyThreshold": 30
}
```


PUT /warranty/settings

Use this method to modify global warranty settings.

Authentication

Authentication with username and password is required.

Request URL

```
PUT https://{management_server_IP}/warranty/settings
```

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
warrantyThreshold	Required	Integer	Number of days before the warranty expires for a managed device when you want to be warned about the expiration. The default is 30 days.

The following example modifies the warranty threshold.

```
{
   "warrantyThreshold": 30
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
result	String	Results of the request. This can be one of the following values. • **success**. The request completed successfully. • **failed**. The request failed. A descriptive error message was returned. • **warning**. The request completed with a warning. A descriptive error message was returned.
messages	Array of objects	Information about one or more messages
id	String	Message identifier of a returned message
text	String	Message text associated with the message identifier
explanation	String	Additional information to clarify the reason for the message
recovery	Array of objects	Recovery information
text	String	User actions that can be taken to recover from the event
URL	String	Link to the help system for more information, if available

The following example is returned if the request is successful.

```
{
   "result": "success",
   "messages": [{
      "id": "FQXHMSS2080I",
      "text": "The Alert Period for warnings was updated successfully.",
      "recovery": {
         "text": "",
         "url": ""
      },
      "explanation": ""
   }]
}
```

Chapter 15. Metrics

The following resources are available for collecting and forwarding metrics for the devices that are managed by Lenovo XClarity Administrator.

/canisters/metrics

Use this REST API to retrieve sample metrics for all Flex System storage controllers (canisters). Each controller represents one of the node controllers in a Flex System storage device.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

- Minimum system input power
- Maximum system input power
- Average system input power
- Minimum system output power
- Maximum system output power
- Average system output power
- Average inlet air temperature
- Cooling subsystem air flow
- Outlet air temperature
- Minimum effective CPU speed
- Maximum effective CPU speed
- Average effective CPU speed
- Minimum memory subsystem power
- Maximum memory subsystem power
- Average memory subsystem power
- Inlet air temperature

HTTP methods

GET

GET /canisters/metrics

Use this method to return a set of sample metrics for all Flex System storage controllers (canisters). Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Note: Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metrics data.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/canisters/metrics`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=*<attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

The following example returns **averageSystemInputPower** and **averageSystemOutputPower** properties in addition to the base properties.

```
GET https://192.0.2.0/canisters/metrics?includeAttributes=averageSystemInputPower,averageSystemOutputPower
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
canisterList	Object	List of storage-controllers (canisters)
See GET /canisters/metrics/*{uuid}*	Array of objects	Energy metrics for each storage- controller

The following example is returned if the request is successful.

```
{
```

```
"canisterList": [{
    "energyMetrics": {
       "averageCPUSubsystemPower": [{
            "timeStamp": "2015-02-06T16:06:00Z",
            "metricValue": 0
        },
        ...,
        {
            "timeStamp": "2015-02-06T17:05:30Z",
            "metricValue": 0
         }],
        "minimumCPUSubsystemPower": [{
            "timeStamp": "2015-02-06T16:06:00Z",
            "metricValue": 0
        },
        ...,
        {
            "timeStamp": "2015-02-06T17:05:30Z",
            "metricValue": 0
        }],
         "maximumCPUSubsystemPower": [{
            "timeStamp": "2015-02-06T16:06:00Z",
            "metricValue": 0
        },
        ...,
        {
            "timeStamp": "2015-02-06T17:05:30Z",
            "metricValue": 0
        }],
        "averageEffectiveCPUSpeed": [{
            "timeStamp": "2015-02-06T16:06:00Z",
            "metricValue": 0
        },
        ...,
        {
            "timeStamp": "2015-02-06T17:05:30Z",
            "metricValue": 0
        }],
        "minimumEffectiveCPUSpeed": [{
            "timeStamp": "2015-02-06T16:06:00Z",
            "metricValue": 0
        },
        ...,
        {
            "timeStamp": "2015-02-06T17:05:30Z",
            "metricValue": 0
        }],
        "maximumEffectiveCPUSpeed": [{
            "timeStamp": "2015-02-06T16:06:00Z",
            "metricValue": 0
        },
        ...,
        {
            "timeStamp": "2015-02-06T17:05:30Z",
            "metricValue": 0
        }],
        "averageMemorySubsystemPower": [{
            "timeStamp": "2015-02-06T16:06:00Z",
            "metricValue": 0
        },
        ...,
```

```
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
"minimumMemorySubsystemPower": [{
    "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 0
},
...,
{
     "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
"maximumMemorySubsystemPower": [{
     "timeStamp": "2015-02-06T16:06:00Z",
     "metricValue": 0
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
"averageSystemInputPower": [{
    "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 12
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 12
}],
"minimumSystemInputPower": [{
    "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 0
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
     "metricValue": 0
}],
"maximumSystemInputPower": [{
     "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 20
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 20
}],
"averageSystemOutputPower": [],
"minimumSystemOutputPower": [],
"maximumSystemOutputPower": [],
"inletAirTemperature": [{
    "timeStamp": "2015-02-06T16:06:30Z",
    "metricValue": 21
},
...,
{
    "timeStamp": "2015-02-06T17:06:00Z",
    "metricValue": 21
}],
```

```
        "inletAirTemperature2": [{
            "timeStamp": "2015-02-06T16:06:30Z",
            "metricValue": 21.5
        },
        ...,
        {
            "timeStamp": "2015-02-06T17:06:00Z",
            "metricValue": 21.5
        }],
        "outletAirTemperature": []
        "powerSupplyList": [],
    },
    "name": "xpet-c3s3",
    "parent": {
        "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
        "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
    },
    "uri": "node/E33EB382679211E180BA5CF3FC7F1038",
    "uuid": "E33EB382679211E180BA5CF3FC7F1038"
}]
}
```


/canisters/metrics/*{uuid}*

Use this REST API to retrieve sample metrics for a specific Flex System storage controller (canister). Each controller represents one of the node controllers in a Flex System storage device.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

- Minimum System Input Power
- Maximum System Input Power
- Average System Input Power
- Minimum System Output Power
- Maximum System Output Power
- Average System Output Power
- Average Inlet Air Temperature
- Ccooling SubSystem Air Flow
- Outlet Air Temperature
- Minimum effective CPU speed
- Maximum effective CPU speed
- Average effective CPU speed
- Minimum Memory Subsystem Power
- Maximum Memory Subsystem Power
- Average Memory Subsystem Power
- Inlet Air Temperature

HTTP methods

GET

GET /canisters/metrics/*{uuid}*

Use this method to return a set of sample metrics for specific Flex System storage controller (canister). Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Request URL

`GET https://{management_server_IP}/canisters/metrics/{uuid}`

where *{uuid}* is the UUID of the storage controller to be retrieved. To obtain the storage-controller UUID, use the GET /canisters method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

The following example returns **averageSystemInputPower** and **averageSystemOutputPower** properties in addition to the base properties.

```
GET https://192.0.2.0/canisters/metrics/6ED2CB368C594C66C2BB066D5A306138?
includeAttributes=averageSystemInputPower,averageSystemOutputPower
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Each energy metric contains one or more arrays that include when the sample was taken (**timeStamp**) and the value of the sample (**metricValue**).

Attributes	Type	Description
energyMetrics	Object	Energy metrics for the storage controller
averageEffectiveCPUSpeed	Array	Average effective CPU speed samples
maximumEffectiveCPUSpeed	Array	Maximum effective CPU speed samples
minimumEffectiveCPUSpeed	Array	Minimum effective CPU speed samples
averageCPUSubsystemPower	Array	Average CPU subsystem power samples
maximumCPUSubsystemPower	Array	Maximum CPU subsystem power samples
minimumCPUSubsystemPower	Array	Minimum CPU subsystem power samples
averageMemorySubsystemPower	Array	Average memory subsystem power samples
maximumMemorySubsystemPower	Array	Maximum memory subsystem power samples
minimumMemorySubsystemPower	Array	Minimum memory subsystem power samples
averageSystemInputPower	Array	Average system input power samples
maximumSystemInputPower	Array	Maximum system input power samples
minimumSystemInputPower	Array	Minimum system input power samples
averageSystemOutputPower	Array	Average system output power samples
maximumSystemOutputPower	Array	Maximum system output power samples
minimumSystemOutputPower	Array	Minimum system output power samples
inletAirTemperature	Array	Inlet air temperature samples
inletAirTemperature2	Array	Inlet air temperature samples
outletAirTemperature	Array	Outlet air temperature samples
name	String	Storage-controller name
parent	Array	
uri	String	
uuid	String	
uri	String	Storage-controller URI
uuid	String	Storage-controller UUID

The following example is returned if the request is successful.


```
{
   "energyMetrics": {
      "averageCPUSubsystemPower": [{
         "timeStamp": "2015-02-06T16:06:00Z",
         "metricValue": 0
      },
      ...,
      {
         "timeStamp": "2015-02-06T17:05:30Z",
         "metricValue": 0
       }],
      "minimumCPUSubsystemPower": [{
         "timeStamp": "2015-02-06T16:06:00Z",
```

```
    "metricValue": 0
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
 "maximumCPUSubsystemPower": [{
    "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 0
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
"averageEffectiveCPUSpeed": [{
    "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 0
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
"minimumEffectiveCPUSpeed": [{
    "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 0
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
"maximumEffectiveCPUSpeed": [{
    "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 0
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
"averageMemorySubsystemPower": [{
    "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 0
},
...,
{
    "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
"minimumMemorySubsystemPower": [{
    "timeStamp": "2015-02-06T16:06:00Z",
    "metricValue": 0
},
...,
{
     "timeStamp": "2015-02-06T17:05:30Z",
    "metricValue": 0
}],
```

```
    "maximumMemorySubsystemPower": [{
        "timeStamp": "2015-02-06T16:06:00Z",
        "metricValue": 0
    },
    ...,
    {
       "timeStamp": "2015-02-06T17:05:30Z",
       "metricValue": 0
    }],
    "averageSystemInputPower": [{
       "timeStamp": "2015-02-06T16:06:00Z",
       "metricValue": 12
    },
    ...,
    {
       "timeStamp": "2015-02-06T17:05:30Z",
       "metricValue": 12
    }],
    "minimumSystemInputPower": [{
       "timeStamp": "2015-02-06T16:06:00Z",
       "metricValue": 0
    },
    ...,
    {
       "timeStamp": "2015-02-06T17:05:30Z",
        "metricValue": 0
    }],
    "maximumSystemInputPower": [{
        "timeStamp": "2015-02-06T16:06:00Z",
       "metricValue": 20
    },
    ...,
    {
       "timeStamp": "2015-02-06T17:05:30Z",
       "metricValue": 20
    }],
    "averageSystemOutputPower": [],
    "minimumSystemOutputPower": [],
    "maximumSystemOutputPower": [],
    "inletAirTemperature": [{
       "timeStamp": "2015-02-06T16:06:30Z",
       "metricValue": 21
    },
    ...,
    {
       "timeStamp": "2015-02-06T17:06:00Z",
       "metricValue": 21
    }],
    "inletAirTemperature2": [{
       "timeStamp": "2015-02-06T16:06:30Z",
       "metricValue": 21.5
    },
    ...,
    {
        "timeStamp": "2015-02-06T17:06:00Z",
       "metricValue": 21.5
    }],
    "outletAirTemperature": [],
},
"name": "xpet-c3s3",
"parent": {
```

```
      "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91",
      "uuid": "3D1D5931BDF84D30ADA976E21F08CB91"
   },
   "uri": "node/E33EB382679211E180BA5CF3FC7F1038",
   "uuid": "E33EB382679211E180BA5CF3FC7F1038"
}
```


/chassis/metrics

Use this REST API to retrieve sample metrics for all chassis.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

- Minimum System Input Power
- Maximum System Input Power
- Average System Input Power
- Average System Output Power
- Minimum System Output Power
- Maximum System Output Power
- Minimum Inlet Air Temperature
- Maximum Inlet Air Temperature
- Average Inlet Air Temperature
- Ccooling SubSystem Air Flow
- Outlet Air Temperature

HTTP methods

GET

GET /chassis/metrics

Use this method to return a set of sample metrics for all chassis. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Note: Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metric data.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/chassis/metrics
```

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
chassisList	Array	List of chassis
See GET /chassis/metrics/*{uuid}*	Object	Energy metrics for each chassis

The following example is returned if the request is successful.

```
{
   "chassisList": [{
      "energyMetrics": {
         "averageSystemInputPower": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 616
         },
         ...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 617
         },
         {
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 620
         }],
         "minimumSystemInputPower": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 616
         },
         ...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 617
         },
         {
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 620
         }],
         "maximumSystemInputPower": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 616
         }...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 617
         },
```

```
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 620
}],
"averageSystemOutputPower": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 548
},
...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 553
},
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 566
}],
"minimumSystemOutputPower": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 548
},
...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 553
},
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 566
}],
"maximumSystemOutputPower": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 548
},
...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 553
},
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 566
}],
"avgInletAirTemperature": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 2550
},
...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 2570
},
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 2570
}],
"minInletAirTemperature": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 2550
},
...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 2550
},
{
```

```
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 2550
         }],
         "maxInletAirTemperature": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 2550
         },
         ...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 617
         },
         {
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 620
         }],
         "coolingSubsystemAirFlow": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 237
         },
         ...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 240
         },
         {
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 238
         }],
         "outletAirTemperature": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 3015
         },
         ...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 3033
         },
         {
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 3013
         }]
      },
      "name": "SN#Y011BG31R02F",
      "uuid": "3D1D5931BDF84D30ADA976E21F08CB91",
      "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91"
   }]
}
```


/chassis/metrics/*{uuid}*

Use this REST API to retrieve sample metrics for a specific chassis.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue). metrics:

- Minimum System Input Power
- Maximum System Input Power
- Average System Input Power
- Average System Output Power
- Minimum System Output Power
- Maximum System Output Power
- Minimum Inlet Air Temperature

- Maximum Inlet Air Temperature
- Average Inlet Air Temperature
- Ccooling SubSystem Air Flow
- Outlet Air Temperature

HTTP methods

GET

GET /chassis/metrics/*{uuid}*

Use this method to return a set of sample metrics for specific chassis. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/chassis/metrics/{uuid}`

where *{uuid}* is the UUID of the chassis. To obtain the chassis UUID, use the GET /chassis method.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Each energy metric contains one or more arrays that include when the sample was taken (**timeStamp**) and the value of the sample (**metricValue**).

Attributes	Type	Description
energyMetrics	Object	Energy metrics for the chassis
averageSystemInputPower	Array of objects	Average system input power samples

Attributes		Type	Description
	minimumSystemInputPower	Array of objects	Minimum system input power samples
	maximumSystemInputPower	Array of objects	Maximum system input power samples
	averageSystemOutputPower	Array of objects	Average system output power samples
	minimumSystemOutputPower	Array of objects	Minimum system output power samples
	maximumSystemOutputPower	Array of objects	Maximum system output power samples
	avgInletAirTemperature	Array of objects	Average inlet air temperature samples
	minInletAirTemperature	Array of objects	Minimum inlet air temperature samples
	maxInletAirTemperature	Array of objects	Maximum inlet air temperature samples
	coolingSubsystemAirFlow	Array of objects	Cooling subsystem air flow samples
	outletAirTemperature	Array of objects	Outlet air temperature samples
name		String	Chassis name
uuid		String	Chassis UUID
uri		String	Chassis URI

The following example is returned if the request is successful.


```
{
   "energyMetrics": {
      "averageSystemInputPower": [{
         "timeStamp": "2015-02-06T18:35:00Z",
         "metricValue": 616
      },
      ...{
         "timeStamp": "2015-02-06T20:24:59Z",
         "metricValue": 617
      },
      {
         "timeStamp": "2015-02-06T20:30:01Z",
         "metricValue": 620
      }],
      "minimumSystemInputPower": [{
         "timeStamp": "2015-02-06T18:35:00Z",
         "metricValue": 616
      },
      ...{
         "timeStamp": "2015-02-06T20:24:59Z",
         "metricValue": 617
      },
      {
         "timeStamp": "2015-02-06T20:30:01Z",
         "metricValue": 620
```

```
}],
"maximumSystemInputPower": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 616
}...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 617
},
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 620
}],
"averageSystemOutputPower": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 548
},
...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 553
},
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 566
}],
"minimumSystemOutputPower": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 548
},
...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 553
},
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 566
}],
"maximumSystemOutputPower": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 548
},
...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 553
},
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 566
}],
"avgInletAirTemperature": [{
   "timeStamp": "2015-02-06T18:35:00Z",
   "metricValue": 2550
},
...{
   "timeStamp": "2015-02-06T20:24:59Z",
   "metricValue": 2570
},
{
   "timeStamp": "2015-02-06T20:30:01Z",
   "metricValue": 2570
}],
"minInletAirTemperature": [{
```

```
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 2550
        },
        ...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 2550
        },
        {
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 2550
        }],
        "maxInletAirTemperature": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 2550
        },
        ...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 617
        },
        {
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 620
        }],
        "coolingSubsystemAirFlow": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 237
        },
        ...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 240
        },
        {
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 238
        }],
        "outletAirTemperature": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 3015
        },
        ...{
            "timeStamp": "2015-02-06T20:24:59Z",
            "metricValue": 3033
        },
        {
            "timeStamp": "2015-02-06T20:30:01Z",
            "metricValue": 3013
        }]
    },
    "name": "SN#Y011BG31R02F",
    "uuid": "3D1D5931BDF84D30ADA976E21F08CB91",
    "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91"
}
```


/fans/metrics

Use this REST API to retrieve sample metrics for all Flex System fans.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

- Minimum Fan Power

- Maximum Fan Power
- Average Fan Power

HTTP methods

GET

GET /fans/metrics

Use this method to return a set of sample metrics for all Flex System fans. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Note: Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metrics data.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/fans/metrics`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.

Code	Description	Comments
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
fanList	Array	Information about each fan
See GET /fans/metrics/{uuid}	Object	Sample metrics for each fans

The following example is returned if the request is successful.


```
{
   "fanList": [{
      "energyMetrics": {
         "averageFanPower": [{
            "timeStamp": "2015-09-11T21:50:01Z",
            "metricValue": 7.0
         },
         ...,
         {
            "timeStamp": "2015-09-11T23:45:00Z",
            "metricValue": 8.0
         }],
         "maximumFanPower": [{
            "timeStamp": "2015-09-11T21:50:01Z",
            "metricValue": 8.0
         },
         ...,
         {
            "timeStamp": "2015-09-11T23:45:00Z",
            "metricValue": 8.0
         }]"minimumFanPower": [{
            "timeStamp": "2015-09-11T21:50:01Z",
            "metricValue": 7.0
         },
         ...,
         {
            "timeStamp": "2015-09-11T23:45:00Z",
            "metricValue": 8.0
         }],

      },
      "name": "Fan 08",
      "parent": {
         "uri": "chassis/8C070E3262114E36B7E68699386FBA53",
         "uuid": "8C070E3262114E36B7E68699386FBA53"
      },
      "uri": "fan/FD0021C1981E11E080EED0FD680CCBDA",
      "uuid": "FD0021C1981E11E080EED0FD680CCBDA"
   }]
}
```

/fans/metrics/*{uuid}*

Use this REST API to retrieve sample metrics for a specific Flex System fan.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

- Minimum Fan Power
- Maximum Fan Power
- s
- Average Fan Power

HTTP methods

GET

GET /fans/metrics/{uuid}

Use this method to return a set of sample metrics for a specific Flex System fans. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/fans/metrics/{uuid}`

where {uuid} is the UUID of the fan to be retrieved. To obtain the fan UUID, use the GET /fans method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Each energy metric contains one or more arrays that include when the sample was taken (**timeStamp**) and the value of the sample (**metricValue**).

Attributes	Type	Description
energyMetrics	Object	Energy metrics for the fan
averageFanPower	Array of objects	Average fan power samples
maximumFanPower	Array of objects	Maximum fan power samples
minimumFanPower	Array of objects	Minimum fan power samples
name	String	Fan name
parent	Array	
uri	String	
uuid	String	
uuid	String	Fan UUID
uri	String	Fan URI

The following example is returned if the request is successful.

```
{
   "energyMetrics": {
      "averageFanPower": [{
         "timeStamp": "2015-09-11T21:50:01Z",
         "metricValue": 7.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T23:45:00Z",
         "metricValue": 8.0
      }],
      "maximumFanPower": [{
         "timeStamp": "2015-09-11T21:50:01Z",
         "metricValue": 8.0
```

```
      },
      ...,
      {
         "timeStamp": "2015-09-11T23:45:00Z",
         "metricValue": 8.0
      }]
      "minimumFanPower": [{
         "timeStamp": "2015-09-11T21:50:01Z",
         "metricValue": 7.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T23:45:00Z",
         "metricValue": 8.0
      }],
   },
   "name": "Fan 08",
   "parent": {
      "uri": "chassis/8C070E3262114E36B7E68699386FBA53",
      "uuid": "8C070E3262114E36B7E68699386FBA53"
   },
   "uri": "fan/FD0021C1981E11E080EED0FD680CCBDA",
   "uuid": "FD0021C1981E11E080EED0FD680CCBDA"
}
```


/metrics_service/metrics/servers

Use this REST API to return metrics data for all managed servers or return a specific number of top metric values among all or specific managed servers.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

HTTP methods

GET, POST

GET /metrics_service/metrics/servers

Use this method to return metrics data for all managed servers.

Notes:

- Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metrics data.
- This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/metrics_service/metrics/servers
```

Query parameters

Parameter	Required / Optional	Description
interval={*integer*}	Optional	Returns metrics in the specified intervals, in seconds The minimum interval is 30 seconds. If the specified **interval** is greater than the specified **period**, the **startTimestamp** changes to the end timestamp minus the **interval**. If not specified, the default interval is the sent by baseboard management controller for each measurement is used. • **cpuTemp**. 60 second intervals • **averageCPUUtilization**. 30 second intervals • **averageMemoryUtilization.** 30 second intervals • **inletAirTemp**. 60 second intervals • **averageConsumedWatts**. 30 second intervals • **maxConsumedWatts**. 30 second intervals • **minConsumedWatts**. 30 second intervals • **powerOutputWatts**. 30 second intervals • **powerInputWatts**. 30 second intervals
metricsType=*{type}*	Optional	Returns data only for the specified type. This can be one or more of the following values, separated by a comma. • **cpuTemp**. Average temperature for all processors, in Celsius • **averageCPUUtilization**. Average processor usage, as a percentage • **averageMemoryUtilization.** Average memory usage, as a percentage. The metric is captured every minute. • **inletAirTemp**. Temperature, in Celsius, of the inlet air. The temperature is captured every minute. • **averageConsumedWatts**. Average power consumption for the device, in Watts • **maxConsumedWatts**. Maximum power consumption for the device, in Watts • **minConsumedWatts**. Minimum power consumption for the device, in Watts • **powerOutputWatts**. Maximum power output for all power supplies, in Watts • **powerInputWatts**. Average power input for all power supplies, in Watts If not specified, all metric types are returned.
period=*{integer}*	Optional	Returns data that was collected in the specified amount of time, in minutes You can specify from 1 – 1440 minutes. If not specified, 60 minutes of data is returned by default.
startTimestamp=*{timestamp}*	Optional	Returns data that was collected starting at the specified time, using ISO-8601 format (for example, 2019-06-24T17:34:58+00:00) If not specified, data is returned for the most recent period. This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.

The following example returns all metrics that were collected in the last hour.

```
GET https://192.0.2.0/metrics_service/metrics/servers
```

The following example returns power metrics that were collected in the last four hours.

```
GET https://192.0.2.0/metrics_service/metrics/servers?period=240
&metricsType=averageConsumedWatts,maxConsumedWatts,minConsumedWatts
```

The following example returns power metrics that were collected between noon and 2pm.

```
GET https://192.0.2.0/metrics_service/metrics/servers?metricsType=PowerMetrics
&startTimestamp=2020-07-01T012:00:00Z&period=120
```

The following example returns power-supply metrics that were collected between noon and 2pm, in 60 second intervals.

```
GET https://192.0.2.0/metrics_service/metrics/servers?metricsType=PowerSupplyStats
&startTimestamp=2020-07-01T012:00:00Z&period=120&interval=60
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
results	Array of objects	Information about metrics data that was collected for each server
energyMetrics	Array of objects	Data for each metric Each metric object includes the following attributes. • **metricValue**. Metric value, as an integer, that was collected at the specific timestamp • **slot**. Processor or power supply slot number • **timestamp**. Timestamp when the metric was collected This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
averageCPUUtilization	Array of objects	Average processor usage, as a percentage. The metric is captured every minute.
cpuTempEvent	Array of objects	Average temperature for all processors, in Celsius. The metric is captured every minute.
averageMemoryUtilization	Array of objects	Average memory usage, as a percentage. The metric is captured every minute.

Parameters	Type	Description
averageConsumedWatts	Array of objects	Average power consumption for the device, in Watts. These metrics are captured every 30 seconds.
maxConsumedWatts	Array of objects	Maximum power consumption for the device, in Watts. These metrics are captured every 30 seconds.
minConsumedWatts	Array of objects	Minimum power consumption for the device, in Watts. These metrics are captured every 30 seconds.
PowerInputWatts	Array of objects	Average power input for all power supplies, in Watts. These metrics are captured every 30 seconds.
PowerOutputWatts	Array of objects	Maximum power output for all power supplies, in Watts. These metrics are captured every 30 seconds.
inletAirTemperature	Array of objects	Temperature, in Celsius, of the inlet air. The temperature is captured every minute.
name	String	Server name
uri	String	Server URI
uuid	String	Server UUID

The following example is returned if the request is successful.


```
{
   "results": [{
      "energyMetrics": {
         "averageConsumedWatts": [{
            "metricValue": 324,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "averageCPUUtilization": [{
            "metricValue": 8,
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "averageMemoryUtilization": [{
            "metricValue": 0,
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "cpuTemp": [{
            "metricValue": 47,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "inletAirTemperature": [{
            "metricValue": 28,
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "maxConsumedWatts": [{
            "metricValue": 322,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "minConsumedWatts": [{
            "metricValue": 320,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "powerInputWatts": [{
```

```
            "metricValue": 325,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "powerOutputWatts": [{
            "metricValue": 322,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }]
      },
      "name": "",
      "uri": "node/F32D11A27A1C11EAB6B10A94EFAA959D",
      "uuid": "F32D11A27A1C11EAB6B10A94EFAA959D"
   },
   {
      "energyMetrics": {
         "averageConsumedWatts": [{
            "metricValue": 324,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"}
         ],
         "averageCPUUtilization": [{
            "metricValue": 8,
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "averageMemoryUtilization": [{
            "metricValue": 0,
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "cpuTempEvent": [{
            "metricValue": 47,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "inletAirTemperature": [{
            "metricValue": 28,
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "maxConsumedWatts": [{
            "metricValue": 322,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "minConsumedWatts": [{
            "metricValue": 320,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "PowerInputWatts": [{
            "metricValue": 325,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }],
         "PowerOutputWatts": [{
            "metricValue": 322,
            "slot": "1",
            "timeStamp": "2015-09-11T18:50:00Z"
         }]
      },
      "name": "",
      "uri": "node/85375E48DCD944D7948824935892CA4E",
```

```
      "uuid": "85375E48DCD944D7948824935892CA4E"
   }]
}
```

POST /metrics_service/metrics/servers

Use this method to return a specific number of top metric values among all or specific managed servers.

Notes:

- Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metrics data.
- This REST API requires Lenovo XClarity Administrator v3.4.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/metrics_service/metrics/servers`

Query parameters

You must specify either **function**, **top**, or **bottom** query parameters.

Parameter	Required / Optional	Description
bottom=*{integer}*	Required if **function** and **top** are not specified	Returns a certain number of bottom (lowest) metric values among the specified devices during the entire period. This can be one of the following values. • **10**. (default) Returns the 10 lowest values. • **50**. Returns the 50 lowest values. This is supported only when the metrics type is **PowerInputWatts**.
function=*{type}*	Required if **bottom** and **top** are not specified	Aggregates data using the specified function. This can be one of the following values. • **average**. Statistical mean • **max**. Maximum • **total**. Total in the period with specified interval This is supported for only the **PowerInputWatts** metric type. The **period** and **interval** attributes must be specified.
interval=*{integer}*	Optional	Returns metrics in the specified intervals, in seconds The minimum interval is 30 seconds. If the specified interval is greater than the specified period, the **startTimestamp** changes to the end timestamp minus the interval. If not specified, the default interval is the sent by baseboard management controller for each measurement is used. • **cpuTemp**. 60 second intervals • **averageCPUUtilization**. 30 second intervals • **averageMemoryUtilization.** 30 second intervals • **inletAirTemp**. 60 second intervals • **PowerInputWatts**. 30 second intervals • **PowerSupplyStats**. 30 second intervals

Parameter	Required / Optional	Description
metricsType=*{type}*	Optional	Returns data only for the specified type. This can be one or more of the following values, separated by a comma. • **cpuTemp**. Average temperature for all processors, in Celsius • **averageCPUUtilization**. Average processor usage • **averageMemoryUtilization**. Average memory usage • **inletAirTemp**. Average temperature of the inlet air, in Celsius. • **PowerInputWatts**. Total power consumption for all power supplies, in Watts • **PowerSupplyStats**. Total power consumption for all power supplies, in Watts If not specified, all metric types are returned.
period=*{integer}*	Required if **bottom** or **top** is specified	Returns data that was collected in the specified amount of time, in minutes You can specify from 1 – 1440 minutes. If not specified, 60 minutes of data is returned by default.
startTimestamp=*{timestamp}*	Optional	Returns data that was collected starting at the specified time, using ISO-8601 format (for example, 2019-06-24T17:34:58+00:00) If not specified, data is returned for the most recent period. This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
top=*{integer}*	Required if **bottom** and **function** are not specified	Returns a certain number of top (highest) metric values among the specified devices during the entire period. This can be one of the following values. • **10**. (default) Returns the 10 highest values. • **50**. Returns the 50 highest values This is supported only when the metrics type is **PowerInputWatts**.

The following example returns the average **averageMemoryUtilization** and **averageCPUUtilization** metrics during a 30-minute period starting at the specified timestamp, in 30-second intervals.

```
POST https://192.0.2.0/metrics_service/metrics/servers
?metricsType=averageCPUUtilization,averageMemoryUtilization
&function=average&interval=30&startTimestamp=2021-07-27T04:09:17.802Z
```

The following example returns the maximum **PowerInputWatts** metrics during a 12-minute period starting at the specified timestamp in 1-minute intervals.

```
POST https://192.0.2.0/metrics_service/metrics/servers?metricsType=PowerInputWatts
&function=max&period=12&interval=1
```

The following example returns the top 10 average power-input metrics during the past 12 minutes, in 30-second intervals

```
POST https://192.0.2.0/metrics_service/metrics/servers?metricsType=PowerInputWatts
&top=10&period=12
```

The following example returns bottom 10 average power-input metrics during a 12-minute period starting at the specified timestamp, in 30-second intervals.

```
POST https://192.0.2.0/metrics_service/metrics/servers?metricsType=PowerInputWatts
&bottom=10&period=12
```

Request body

Attributes	Required / Optional	Type	Description
uuids	Required	Array of strings	Returns metrics data for one or more specific servers, specified by UUIDs separated by a comma If not specified, statistics are returned all managed servers.

The following example returns metrics data for all managed servers.

```
{
   "uuids": []
}
```

The following example returns metrics data for specific managed servers.

```
{
   "uuids": ["65D5FDE03CC94343B772C881A06DDC96","E994C31710E03929884FBB1DBA8636EF"]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

The response varies based on the specified metric type.

Parameters	Type	Description
results	Array of objects	Information about metrics data that was collected for each server
energyMetrics	Object	Information about energy metrics
{metric_type}	Array of objects	List of data for the specified metric type. This can be one of the following types. • **cpuTemp**. Average temperature for all processors, in Celsius • **averageCPUUtilization**. Average processor usage • **averageMemoryUtilization**. Average memory usage • **inletAirTemp**. Average temperature of the inlet air, in Celsius. • **PowerInputWatts**. Total power consumption for all power supplies, in Watts • **PowerSupplyStats**. Total power consumption for all power supplies, in Watts

Parameters	Type	Description
index	Integer	Metric index, where 1 is the highest top value
slot	Integer	Slot located, if applicable
timestamp	String	Timestamp when the metric was collected, if applicable This timestamp is specified using ISO-8601 format (for example, 2019-05-02T19:28:14.000Z). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
uuid	String	UUID of the managed server
value	Integer	Metric value

The following example is returned if the request is successful for the top 10 power-input metrics for three specific servers.


```
{
   "results": [{
      "energyMetrics": {
         "PowerInputWatts": [{
            "index": 1,
            "uuid": "625052OBBOOEC21385165E09B719FB9E",
            "value": 103
         },
         {
            "index": 2,
            "uuid": "9B39E99CFE9A2D4FO5F742B8838833A8",
            "value": 103
         },
         {
            "index": 3,
            "uuid": "4640A41E125FEC3FFFD48B7A2C98318E",
            "value": 102
         }]
      }
   }]
}
```


The following example is returned if the request is successful for the top 10 processor-temperature metrics for a specific server.


```
{
   "results": [{
      "energyMetrics": {
         "cpuTemp": [{
            "index": 1,
            "slot": 2,
            "timeStamp": "2021-11-30T09:04:54.652Z",
            "uuid": "4673074666D7082E090685B14CDDD245",
            "value": 50
         }
      ]}
   }]
}
```


The following example is returned if the request is successful for the top 10 inlet air-temperature metrics for a specific server.


```
{
   "results": [{
      "energyMetrics": {
         "inletAirTemp": [{
```

```
            "timeStamp": "2021-12-14T14:26:54.954Z",
            "uuid": "7167F89D7DB1F1659842B4460AD1BEAD",
            "value": 41
         },
         {
            "timeStamp": "2021-12-14T14:30:26.861Z",
            "uuid": "C3548BD5AF2C9ADD03485147EA2595C7",
            "value": 50
         }]
      }
   }]
}
```

/metrics_service/metrics/servers/*{uuid}*

Use this REST API to return metrics data for a specific server.

Note: This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

HTTP methods

GET

GET /metrics_service/metrics/servers/*{uuid}*

Use this method to return metrics data for a specific server.

Notes:

- Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metrics data.
- This REST API requires Lenovo XClarity Administrator v3.3.0 or later.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/metrics_service/metrics/servers/{uuid}`

Query parameters

Parameter	Required / Optional	Description
metricsType=*{type}*	Optional	Returns data only for the specified type. This can be one or more of the following values, separated by a comma. • **cpuTemp**. Average temperature for all processors, in Celsius • **averageCPUUtilization**. Average processor usage, as a percentage • **averageMemoryUtilization.** Average memory usage, as a percentage. The metric is captured every minute. • **inletAirTemp**. Temperature, in Celsius, of the inlet air. The temperature is captured every minute. • **averageConsumedWatts**. Average power consumption for the device, in Watts • **maxConsumedWatts**. Maximum power consumption for the device, in Watts • **minConsumedWatts**. Minimum power consumption for the device, in Watts • **powerOutputWatts**. Maximum power output for all power supplies, in Watts • **powerInputWatts**. Average power input for all power supplies, in Watts If not specified, all metric types are returned.
period=*{integer}*	Optional	Returns data that was collected in the specified amount of time, in minutes You can specify from 1 – 1440 minutes. If not specified, 60 minutes of data is returned by default.
startTimestamp=*{timestamp}*	Optional	Returns data that was collected starting at the specified time, using ISO-8601 format (for example, 2019-06-24T17:34:58+00:00) If not specified, data is returned for the most recent period. This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.

The following example returns all metrics that were collected in the last hour.

```
GET https://192.0.2.0/metrics_service/metrics/servers/6ED2CB368C594C66C2BB066D5A306138
```

The following example returns power metrics that were collected in the last four hours.

```
GET https://192.0.2.0/metrics_service/metrics/servers?period=240
&metricsType=averageConsumedWatts,maxConsumedWatts,minConsumedWatts
```

The following example returns power metrics that were collected between noon and 2pm.

```
GET https://192.0.2.0/metrics_service/metrics/servers/6ED2CB368C594C66C2BB066D5A306138
?metricsType=PowerMetrics&startTimeStamp=2020-07-01T012:00:00Z&period=120
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
energyMetrics	Array of objects	Data for each metric Each metric object includes the following attributes. • **metricValue**. Metric value, as an integer, that was collected at the specific timestamp • **slot**. Processor or power supply slot number • **timestamp**. Timestamp when the metric was collected This date is specified using ISO-8601 format (for example, 2019-05-02). For information about ISO-8601 format, see the W3C Date and Time Formats webpage.
averageCPUUtilization	Array of objects	Average processor usage, as a percentage. The metric is captured every minute.
cpuTempEvent	Array of objects	Average temperature for all processors, in Celsius. The metric is captured every minute.
averageMemoryUtilization	Array of objects	Average memory usage, as a percentage. The metric is captured every minute.
averageConsumedWatts	Array of objects	Average power consumption for the device, in Watts. These metrics are captured every 30 seconds.
maxConsumedWatts	Array of objects	Maximum power consumption for the device, in Watts. These metrics are captured every 30 seconds.
minConsumedWatts	Array of objects	Minimum power consumption for the device, in Watts. These metrics are captured every 30 seconds.
PowerInputWatts	Array of objects	Average power input for all power supplies, in Watts. These metrics are captured every 30 seconds.
PowerOutputWatts	Array of objects	Maximum power output for all power supplies, in Watts. These metrics are captured every 30 seconds.
inletAirTemperature	Array of objects	Temperature, in Celsius, of the inlet air. The temperature is captured every minute.
name	String	Server name

Parameters	Type	Description
uri	String	Server URI
uuid	String	Server UUID

The following example is returned if the request is successful.


```
{
   "energyMetrics": {
      "averageConsumedWatts": [{
         "metricValue": 324,
         "slot": "1",
         "timeStamp": "2015-09-11T18:50:00Z"
      }],
      "averageCPUUtilization": [{
         "metricValue": 8,
         "timeStamp": "2015-09-11T18:50:00Z"
      }],
      "averageMemoryUtilization": [{
         "metricValue": 0,
         "timeStamp": "2015-09-11T18:50:00Z"
      }],
      "cpuTemp": [{
         "metricValue": 47,
         "slot": "1",
         "timeStamp": "2015-09-11T18:50:00Z"
      }],
      "inletAirTemperature": [{
         "metricValue": 28,
         "timeStamp": "2015-09-11T18:50:00Z"
      }],
      "maxConsumedWatts": [{
         "metricValue": 322,
         "slot": "1",
         "timeStamp": "2015-09-11T18:50:00Z"
      }],
      "minConsumedWatts": [{
         "metricValue": 320,
         "slot": "1",
         "timeStamp": "2015-09-11T18:50:00Z"
      }],
      "powerInputWatts": [{
         "metricValue": 325,
         "slot": "1",
         "timeStamp": "2015-09-11T18:50:00Z"
      }],
      "powerOutputWatts": [{
         "metricValue": 322,
         "slot": "1",
         "timeStamp": "2015-09-11T18:50:00Z"
      }]
   },
   "name": "",
   "uri": "node/F32D11A27A1C11EAB6B10A94EFAA959D",
   "uuid": "F32D11A27A1C11EAB6B10A94EFAA959D"
}
```


/metrics_service/subscriptions

Use this REST API to retrieve information about all metrics forwarders and create a metrics forwarder.

Metrics forwarders define the remote location to which the device metrics are forwarded. Lenovo XClarity Administrator collects metrics for managed devices with an Lenovo XClarity Controller (such as ThinkSystem and ThinkAgile servers) and then forwards the data using a REST web service.

HTTP methods

GET, POST

GET /metrics_service/subscriptions

Use this method to return information about all metrics forwarders.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/metrics_service/subscriptions`

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
description	String	Description for the metrics forwarder
enable	Boolean	Indicates whether the metrics forwarder is enabled. This can be one of the following values. • **true**. (default) The metrics forwarder is enabled. • **false**. The metrics forwarder is disabled.
id	String	ID of the metrics forwarder
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the metrics. For email, this is the SMTP server.
name	String	User-defined name for the metrics forwarder. This name must be unique for all metrics forwarders.
restPath	String	Resource path on which the forwarder is to post the metrics The default path is `/api/v1/inbound/metrics`.

The following example is returned if the request is successful.

```
[{
    "description": "Metrics  subscription",
```

```
    "enable": "true",
    "id": "1520009679583",
    "ipAddress": "192.0.2.40",
    "name": "Metrics_subscription",
    "restPath": "/api/v1/metrics"
}]
```


POST /metrics_service/subscriptions

Use this method to create a metrics forwarder.

Authentication

Authentication with username and password is required.

Request URL

`POST https://{management_server_IP}/metrics_service/subscriptions`

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
authUser	Required if **restAuthentication** is set to “basic”	String	Authentication user ID if authentication is used
authPassword	Required if **restAuthentication** is set to “basic”	String	Authentication password if authentication is used
description	Optional	String	Description for the metrics forwarder
enable	Optional	Boolean	Indicates whether the metrics forwarder is enabled. This can be one of the following values. • **true**. (default) The metrics forwarder is enabled. • **false**. The metrics forwarder is disabled.
ipAddress	Required	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the metrics. For email, this is the SMTP server.
name	Required	String	User-defined name for the metrics forwarder. This name must be unique for all metrics forwarders.
port	Optional	String	TCP/UDP port used for the connection

Parameter	Re-quired / Optional	Type	Description
restAuthentication	Optional	String	Authentication type. This can be one of the following values. • **basic**. (default) Authenticates to the specified server using the specified user ID (**authUser**) and password (**authPassword**). • **none**. (default) No authentication is used.
restPath	Optional	String	Resource path on which the forwarder is to post the metrics The default path is /api/v1/inbound/metrics.

The following example creates a metrics forwarder.

```
{
   "authUser": "ADMIN",
   "authPassword": "********",
   "description": "Metrics subscription",
   "enable": "true",
   "ipAddress": "192.0.2.40",
   "name": "Metrics_subscription",
   "port": "443",
   "restAuthentication": "basic",
   "restPath": "/api/v1/metrics"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
id	String	Metrics forwarder (subscription) ID

The following example is returned if the request is successful.

```
{
   "id": "5e3279917f30b2de48e905b5"
}
```

/metrics_service/subscriptions/*{id}*

Use this REST API to retrieve information about, update, or delete a specific metrics forwarder.

Metrics forwarders define the remote location to which the device metrics are forwarded. Lenovo XClarity Administrator collects metrics for managed devices with an Lenovo XClarity Controller (such as ThinkSystem and ThinkAgile servers) and then forwards the data using a REST web service.

HTTP methods

GET, PATCH, DELETE

GET /metrics_service/subscriptions/*{id}*

Use this method to return information about a specific metrics forwarder.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/metrics_service/subscriptions/{id}`

where *{id}* is the ID of the metrics forwarder (subscription). To obtain the forwarder IDs, use GET /metrics_service/subscriptions.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Parameters	Type	Description
authUser	String	Authentication user ID if authentication is used
description	String	Description for the metrics forwarder
id	String	ID of the metrics forwarder
ipAddress	String	IPv4 or IPv6 address or hostname of the remote system that is the target to receive the metrics. For email, this is the SMTP server.
name	String	User-defined name for the metrics forwarder. This name must be unique for all metrics forwarders.
port	String	TCP/UDP port used for the connection
restPath	String	Resource path on which the forwarder is to post the metrics The default path is /api/v1/inbound/metrics.

The following example is returned if the request is successful.


```
{
    "authUser": "ADMIN",
    "description": "Metrics subscription",
```

```
    "id": "1520009679583",
    "ipAddress": "192.0.2.40",
    "name": "Metrics_subscription",
    "port": "443",
    "restPath": "/api/v1/metrics"
}
```

PATCH /metrics_service/subscriptions/*{id}*

Use this method to modify properties for a specific metrics forwarder.

Authentication

Authentication with username and password is required.

Request URL

`PATCH https://{management_server_IP}/metrics_service/subscriptions/{id}`

where *{id}* is the ID of the metrics forwarder (subscription). To obtain the forwarder IDs, use GET /metrics_service/subscriptions.

Query parameters

None

Request body

Parameter	Required / Optional	Type	Description
description	Optional	String	Description for the metrics forwarder
enable	Optional	Boolean	Indicates whether the metrics forwarder is enabled. This can be one of the following values. • **true**. (default) The metrics forwarder is enabled. • **false**. The metrics forwarder is disabled.

The following example enables and changes the description for a metrics forwarder.

```
{
   "description": "Metrics subscription",
   "enable": "true"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

DELETE /metrics_service/subscriptions/*{id}*

Use this method to delete a specific metrics forwarder.

Authentication

Authentication with username and password is required.

Request URL

```
DELETE https://{management_server_IP}/metrics_service/subscriptions/{id}
```

where *{id}* is the ID of the metrics forwarder (subscription). To obtain the forwarder IDs, use GET /metrics_service/subscriptions.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	A specified resource cannot be found. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

None

/nodes/metrics

Use this method to return a set of sample metrics for all servers and Flex System storage devices.

Attention: This REST API will be deprecated in a future release. Use GET /metrics_service/metrics/servers instead.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

- Minimum System Input Power
- Maximum System Input Power
- Average System Input Power
- Minimum System Output Power
- Maximum System Output Power
- Average System Output Power
- Average Inlet Air Temperature
- Cooling SubSystem Air Flow
- Outlet Air Temperature
- Minimum effective CPU speed
- Maximum effective CPU speed
- Average effective CPU speed

- Minimum Memory Subsystem Power
- Maximum Memory Subsystem Power
- Average Memory Subsystem Power
- Inlet Air Temperature

HTTP methods

GET

GET /nodes/metrics

Use this method to return a set of sample metrics for all servers and Flex System storage devices. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Notes:

- Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metrics data.
- System usage data (including processor, memory, and I/O) and memory power usage data is not collected for ThinkSystem SR635, SR645, SR655, and SR665 servers.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/metrics`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
nodeList	Array	List of servers
See GET /nodes/metrics/*{uuid}*	Object	Sample metrics for each server

The following example is returned if the request is successful.


```
{
"nodeList": [{
   "energyMetrics": {
      "minimumMemorySubsystemPerformance": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "maximumCPUSubsystemPerformance": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "averageIOSubsystemPerformance": [],
      "minimumCPUSubsystemPower": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
            "metricValue": 0.0
      }],
      "averageSystemPerformance": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
```

```
},
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
   }],
"minimumSystemInputPower": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
   },
...,
   {
      "timeStamp": "2015-09-11T19:49:30Z",
      "metricValue": 0.0
   }],
"minimumSystemOutputPower": [],
"maximumSystemOutputPower": [],
"minimumCPUSubsystemPerformance": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
"timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"minimumIOSubsystemPerformance": [],
"maximumMemorySubsystemPower": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"averageCPUSubsystemPower": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
      "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"averageMemorySubsystemPerformance": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"minimumSystemPerformance": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
   ...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
```

```
    "metricValue": 0.0
}],
    "minimumEffectiveCPUSpeed": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 0.0
},
...,
{
    "timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 0.0
}],
"averageMemorySubsystemPower": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 0.0
},
...,
{
"timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 0.0
}],
"powerSupplyList": [],
"inletAirTemperature": [{
    "timeStamp": "2015-09-11T18:50:30Z",
    "metricValue": 18.0
},
...,
{
    "timeStamp": "2015-09-11T19:50:00Z",
    "metricValue": 17.5
}],
"maximumSystemPerformance": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 0.0
},
...,
{
    "timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 0.0
}],
"maximumMemorySubsystemPerformance": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 0.0
},
...,
{
    "timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 0.0
}],
"averageSystemInputPower": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 8.0
},
...,
{
    "timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 8.0
}],
"maximumEffectiveCPUSpeed": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 0.0
},
```

```
   ...,
   {
      "timeStamp": "2015-09-11T19:49:30Z",
      "metricValue": 0.0
      }],
   "minimumMemorySubsystemPower": [{
      "timeStamp": "2015-09-11T18:50:00Z",
      "metricValue": 0.0
   },
   ...,
   {
      "timeStamp": "2015-09-11T19:49:30Z",
      "metricValue": 0.0
   }],
   "maximumIOSubsystemPerformance": [],
   "maximumCPUSubsystemPower": [{
      "timeStamp": "2015-09-11T18:50:00Z",
      "metricValue": 0.0
   },
   ...,
   {
      "timeStamp": "2015-09-11T19:49:30Z",
      "metricValue": 0.0
   }],
   "maximumSystemInputPower": [{
      "timeStamp": "2015-09-11T18:50:00Z",
      "metricValue": 25.0
   },
   ...,
   {
      "timeStamp": "2015-09-11T19:49:30Z",
      "metricValue": 25.0
   }],
   "averageCPUSubsystemPerformance": [{
      "timeStamp": "2015-09-11T18:50:00Z",
      "metricValue": 0.0
   },
   ...,
   {
      "timeStamp": "2015-09-11T19:49:30Z",
      "metricValue": 0.0
   }],
   "inletAirTemperature2": [],
   "averageSystemOutputPower": [],
   "averageEffectiveCPUSpeed": [{
      "timeStamp": "2015-09-11T18:50:00Z",
      "metricValue": 0.0
   },
   ...,
   {
      "timeStamp": "2015-09-11T19:49:30Z",
      "metricValue": 0.0
   }],
   "outletAirTemperature": []
},
"name": "node12",
"parent": {
   "uri": "chassis/FBEF740B178F4EFAA846E7225EE256DC",
   "uuid": "FBEF740B178F4EFAA846E7225EE256DC"
},
"uri": "node/69BDF8912E5211E4998B40F2E99033F0",
```

```
   "uuid": "69BDF8912E5211E4998B40F2E99033F0"
},
{
   "energyMetrics": {
      "minimumMemorySubsystemPerformance": [],
      "maximumCPUSubsystemPerformance": [],
      "averageIOSubsystemPerformance": [],
      "minimumCPUSubsystemPower": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "averageSystemPerformance": [],
      "minimumSystemInputPower": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "minimumSystemOutputPower": [],
      "maximumSystemOutputPower": [],
      "minimumCPUSubsystemPerformance": [],
      "minimumIOSubsystemPerformance": [],
      "maximumMemorySubsystemPower": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "averageCPUSubsystemPower": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "averageMemorySubsystemPerformance": [],
      "minimumSystemPerformance": [],
      "minimumEffectiveCPUSpeed": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "averageMemorySubsystemPower": [{
         "timeStamp": "2015-09-11T18:50:00Z",
```

```
    "metricValue": 0.0
},
...,
{
    "timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 0.0
}],
"powerSupplyList": [],
"inletAirTemperature": [{
    "timeStamp": "2015-09-11T18:50:30Z",
    "metricValue": 21.5
},
...,
{
    "timeStamp": "2015-09-11T19:50:00Z",
    "metricValue": 21.0
}],
"maximumSystemPerformance": [],
"maximumMemorySubsystemPerformance": [],
"averageSystemInputPower": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 8.0
},
...,
{
    "timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 8.0
}],
"maximumEffectiveCPUSpeed": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 0.0
},
...,
{
    "timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 0.0
}],
"minimumMemorySubsystemPower": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 0.0
},
...,
{
    "timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 0.0
}],
"maximumIOSubsystemPerformance": [],
"maximumCPUSubsystemPower": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 0.0
},
...,
{
    "timeStamp": "2015-09-11T19:49:30Z",
    "metricValue": 0.0
}],
"maximumSystemInputPower": [{
    "timeStamp": "2015-09-11T18:50:00Z",
    "metricValue": 25.0
},
...,
```

```
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 25.0
      }],
      "averageCPUSubsystemPerformance": [],
      "inletAirTemperature2": [],
      "averageSystemOutputPower": [],
      "averageEffectiveCPUSpeed": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "outletAirTemperature": []
   },
   "name": "x240_3",
   "parent": {
      "uri": "chassis/FBEF740B178F4EFAA846E7225EE256DC",
      "uuid": "FBEF740B178F4EFAA846E7225EE256DC",
   },
   "uri": "node/0C0DAFD96C4E11E1AF035CF3FC6E4C90",
   "uuid": "0C0DAFD96C4E11E1AF035CF3FC6E4C90"
}]
}
```


/nodes/metrics/*{uuid}*

Use this method to return a set of sample metrics for a specific server or Flex System storage device.

Attention: This REST API will be deprecated in a future release. Use GET /metrics_service/metrics/servers instead.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

- Minimum System Input Power
- Maximum System Input Power
- Average System Input Power
- Minimum System Output Power
- Maximum System Output Power
- Average System Output Power
- Average Inlet Air Temperature
- Cooling Subsystem Air Flow
- Outlet Air Temperature
- Minimum effective CPU speed
- Maximum effective CPU speed
- Average effective CPU speed
- Minimum Memory Subsystem Power
- Maximum Memory Subsystem Power
- Average Memory Subsystem Power
- Inlet Air Temperature

HTTP methods

GET

GET /nodes/metrics/*{uuid}*

Use this method to return a set of sample metrics for a specific server or Flex System storage device. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Notes:

- Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metrics data.
- System usage data (including processor, memory, and I/O) and memory power usage data is not collected for ThinkSystem SR635, SR645, SR655, and SR665 servers.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/nodes/metrics/{uuid}`

where *{uuid}* is the UUID of the node to be retrieved. To obtain the node UUID, use the GET /nodes method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.

Code	Description	Comments
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Each energy metric contains one or more arrays that include when the sample was taken (**timeStamp**) and the value of the sample (**metricValue**).

Attributes	Type	Description
energyMetrics	Object	Energy metrics for the server
averageSystemInputPower	Array of objects	Average system input power samples
minimumSystemInputPower	Array of objects	Minimum system input power samples
maximumSystemInputPower	Array of objects	Maximum system input power samples
averageSystemOutputPower	Array of objects	Average system output power samples
minimumSystemOutputPower	Array of objects	Minimum system output power samples
maximumSystemOutputPower	Array of objects	Maximum system output power samples
averageEffectiveCPUSpeed	Array of objects	Average effective processor speed samples
minimumEffectiveCPUSpeed	Array of objects	Minimum effective processor speed samples
maximumEffectiveCPUSpeed	Array of objects	Maximum effective processor speed samples
averageCPUSubsystemPower	Array of objects	Average processor subsystem speed samples
minimumCPUSubsystemPower	Array of objects	Minimum processor subsystem speed samples
maximumCPUSubsystemPower	Array of objects	Maximum processor subsystem speed samples
averageMemorySubsystemPower	Array of objects	Average memory subsystem power samples
minimumMemorySubsystemPower	Array of objects	Minimum memory subsystem power samples
maximumMemorySubsystemPower	Array of objects	Maximum memory subsystem power samples
coolingSubSystemAirFlow	Array of objects	Cooling subsystem air flow samples

Attributes	Type	Description
inletAirTemperature	Array of objects	Inlet air temperature samples
inletAirTemperature2	Array of objects	Inlet air temperature samples
outletAirTemperature	Array of objects	Outlet air temperature samples
powerSupplyList	Array of objects	List of power supplies in the server
See GET /powerSupplies/metrics/*{uuid}*	Object	Sample metrics for each power supply
name	String	Server name
parent	Array	
uuid	String	
uri	String	
uuid	String	Server UUID
uri	String	Server URI

The following example is returned if the request is successful.

```
{
   "energyMetrics": {
      "minimumMemorySubsystemPerformance": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "maximumCPUSubsystemPerformance": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
         "metricValue": 0.0
      }],
      "averageIOSubsystemPerformance": [],
      "minimumCPUSubsystemPower": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
      ...,
      {
         "timeStamp": "2015-09-11T19:49:30Z",
            "metricValue": 0.0
      }],
      "averageSystemPerformance": [{
         "timeStamp": "2015-09-11T18:50:00Z",
         "metricValue": 0.0
      },
```

```
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
   }],
"minimumSystemInputPower": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
   },
...,
   {
      "timeStamp": "2015-09-11T19:49:30Z",
      "metricValue": 0.0
   }],
"minimumSystemOutputPower": [],
"maximumSystemOutputPower": [],
"minimumCPUSubsystemPerformance": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
"timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"minimumIOSubsystemPerformance": [],
"maximumMemorySubsystemPower": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"averageCPUSubsystemPower": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
      "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"averageMemorySubsystemPerformance": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"minimumSystemPerformance": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
   ...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
```

```
}],
   "minimumEffectiveCPUSpeed": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"averageMemorySubsystemPower": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
"timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"powerSupplyList": [],
"inletAirTemperature": [{
   "timeStamp": "2015-09-11T18:50:30Z",
   "metricValue": 18.0
},
...,
{
   "timeStamp": "2015-09-11T19:50:00Z",
   "metricValue": 17.5
}],
"maximumSystemPerformance": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"maximumMemorySubsystemPerformance": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 0.0
}],
"averageSystemInputPower": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 8.0
},
...,
{
   "timeStamp": "2015-09-11T19:49:30Z",
   "metricValue": 8.0
}],
"maximumEffectiveCPUSpeed": [{
   "timeStamp": "2015-09-11T18:50:00Z",
   "metricValue": 0.0
},
...,
```

```
    {
       "timeStamp": "2015-09-11T19:49:30Z",
       "metricValue": 0.0
       }],
    "minimumMemorySubsystemPower": [{
       "timeStamp": "2015-09-11T18:50:00Z",
       "metricValue": 0.0
    },
    ...,
    {
       "timeStamp": "2015-09-11T19:49:30Z",
       "metricValue": 0.0
    }],
    "maximumIOSubsystemPerformance": [],
    "maximumCPUSubsystemPower": [{
       "timeStamp": "2015-09-11T18:50:00Z",
       "metricValue": 0.0
    },
    ...,
    {
       "timeStamp": "2015-09-11T19:49:30Z",
       "metricValue": 0.0
    }],
    "maximumSystemInputPower": [{
       "timeStamp": "2015-09-11T18:50:00Z",
       "metricValue": 25.0
    },
    ...,
    {
       "timeStamp": "2015-09-11T19:49:30Z",
       "metricValue": 25.0
    }],
    "averageCPUSubsystemPerformance": [{
       "timeStamp": "2015-09-11T18:50:00Z",
       "metricValue": 0.0
    },
    ...,
    {
       "timeStamp": "2015-09-11T19:49:30Z",
       "metricValue": 0.0
    }],
    "inletAirTemperature2": [],
    "averageSystemOutputPower": [],
    "averageEffectiveCPUSpeed": [{
       "timeStamp": "2015-09-11T18:50:00Z",
       "metricValue": 0.0
    },
    ...,
    {
       "timeStamp": "2015-09-11T19:49:30Z",
       "metricValue": 0.0
    }],
    "outletAirTemperature": []
},
"name": "node12",
"parent": {
    "uri": "chassis/FBEF740B178F4EFAA846E7225EE256DC",
    "uuid": "FBEF740B178F4EFAA846E7225EE256DC"
},
"uri": "node/69BDF8912E5211E4998B40F2E99033F0",
"uuid": "69BDF8912E5211E4998B40F2E99033F0"
```

```
}
```

/powerSupplies/metrics

Use this REST API to retrieve sample metrics for all Flex System power supplies.

Attention: This REST API will be deprecated in a future release. Use GET /metrics_service/metrics/servers instead.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).
- Minimum Power Supply Input Power
- Maximum Power Supply Input Power
- Average Power Supply Input Power

HTTP methods

GET

GET /powerSupplies/metrics

Use this method to return a set of sample metrics for all Flex System power supplies. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Note: Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metrics data.

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/powerSupplies/metrics`

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
powerSupplyList	Array	List of power supplies in all chassis
See GET /powerSupplies/metrics/*{uuid}*	Object	Sample metrics for each power supply

The following example is returned if the request is successful.

```
{
   "powerSupplyList": [{
      "energyMetrics": {
         "averagePowerSupplyInputPower": [{
            "timeStamp": "2015-02-06T20:10:00Z",
            "metricValue": 127
         },
         ...{
            "timeStamp": "2015-02-06T22:00:01Z",
            "metricValue": 128
         },
         {
            "timeStamp": "2015-02-06T22:05:00Z",
            "metricValue": 127
         }],
         "minimumPowerSupplyInputPower": [{
            "timeStamp": "2015-02-06T20:10:00Z",
            "metricValue": 125
         },
         ...{
            "timeStamp": "2015-02-06T22:00:01Z",
            "metricValue": 125
         },
         {
            "timeStamp": "2015-02-06T22:05:00Z",
            "metricValue": 126
         }],
         "maximumPowerSupplyInputPower": [{
            "timeStamp": "2015-02-06T20:10:00Z",
            "metricValue": 129
```

```
         },
         ...{
            "timeStamp": "2015-02-06T22:00:01Z",
            "metricValue": 130
         },
         {
            "timeStamp": "2015-02-06T22:05:00Z",
            "metricValue": 129
         }],
         "averagePowerSupplyOutputPower": [{
            "timeStamp": "2015-02-06T20:10:00Z",
            "metricValue": 102
         },
         ...{
            "timeStamp": "2015-02-06T22:00:01Z",
            "metricValue": 106
         },
         {
            "timeStamp": "2015-02-06T22:05:00Z",
            "metricValue": 109
         }]"minimumPowerSupplyOutputPower": [{
            "timeStamp": "2015-02-06T20:10:00Z",
            "metricValue": 98
         },
         ...{
            "timeStamp": "2015-02-06T22:00:01Z",
            "metricValue": 102
         },
         {
            "timeStamp": "2015-02-06T22:05:00Z",
            "metricValue": 101
         }],
         "maximumPowerSupplyOutputPower": [{
            "timeStamp": "2015-02-06T20:10:00Z",
            "metricValue": 112
         },
         ...{
            "timeStamp": "2015-02-06T22:00:01Z",
            "metricValue": 113
         },
         {
            "timeStamp": "2015-02-06T22:05:00Z",
            "metricValue": 113
         }],

      },
      "name": "Power Supply 01",
      "parent": {
         "uuid": "3D1D5931BDF84D30ADA976E21F08CB91",
         "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91"
      },
      "uuid": "D15D67FD1FBC40A09BEDF97C061A160A",
      "uri": "powerSupply/D15D67FD1FBC40A09BEDF97C061A160A"
   }]
}
```


/powerSupplies/metrics/*{uuid}*

Use this REST API to retrieve sample metrics for a specific Flex System power supply.

Attention: This REST API will be deprecated in a future release. Use GET /metrics_service/metrics/servers instead.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).
- Minimum Power Supply Input Power
- Maximum Power Supply Input Power
- Average Power Supply Input Power

HTTP methods

GET

GET /powerSupplies/metrics/*{uuid}*

Use this method to return sample metrics for a specific Flex System power supply. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/powerSupplies/metrics/{uuid}`

where *{uuid}* is the unique ID of the power supply to be retrieved.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=<*attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Each energy metric contains one or more arrays that include when the sample was taken (**timeStamp**) and the value of the sample (**metricValue**).

Attributes	Type	Description
energyMetrics	Object	Energy metrics for the power supply
averagePowerSupplyInputPower	Array of objects	Average power-supply input power samples.
maximumPowerSupplyInputPower	Array of objects	Minimum power-supply input power samples
maximumPowerSupplyOutputPower	Array of objects	Maximum power-supply input power samples
minimumPowerSupplyOutputPower	Array of objects	Average power-supply output power samples
minimumPowerSupplyInputPower	Array of objects	Minimum power-supply output power samples
averagePowerSupplyOutputPower	Array of objects	Maximum power-supply output power samples
name	String	Power supply name
parent	Object	Information about the device that contains the power supply
uuid	String	Parent UUID
uri	String	Parent URI
uuid	String	Power supply UUI
uri	String	Power supply URI

The following example is returned if the request is successful.

```
{
   "energyMetrics": {
      "averagePowerSupplyInputPower": [{
         "timeStamp": "2015-02-06T20:10:00Z",
         "metricValue": 127
```

```
},
...{
   "timeStamp": "2015-02-06T22:00:01Z",
   "metricValue": 128
},
{
   "timeStamp": "2015-02-06T22:05:00Z",
   "metricValue": 127
}],
"minimumPowerSupplyInputPower": [{
   "timeStamp": "2015-02-06T20:10:00Z",
   "metricValue": 125
},
...{
   "timeStamp": "2015-02-06T22:00:01Z",
   "metricValue": 125
},
{
   "timeStamp": "2015-02-06T22:05:00Z",
   "metricValue": 126
}],
"maximumPowerSupplyInputPower": [{
   "timeStamp": "2015-02-06T20:10:00Z",
   "metricValue": 129
},
...{
   "timeStamp": "2015-02-06T22:00:01Z",
   "metricValue": 130
},
{
   "timeStamp": "2015-02-06T22:05:00Z",
   "metricValue": 129
}],
"averagePowerSupplyOutputPower": [{
   "timeStamp": "2015-02-06T20:10:00Z",
   "metricValue": 102
},
...{
   "timeStamp": "2015-02-06T22:00:01Z",
   "metricValue": 106
},
{
   "timeStamp": "2015-02-06T22:05:00Z",
   "metricValue": 109
}]"minimumPowerSupplyOutputPower": [{
   "timeStamp": "2015-02-06T20:10:00Z",
   "metricValue": 98
},
...{
   "timeStamp": "2015-02-06T22:00:01Z",
   "metricValue": 102
},
{
   "timeStamp": "2015-02-06T22:05:00Z",
   "metricValue": 101
}],
"maximumPowerSupplyOutputPower": [{
   "timeStamp": "2015-02-06T20:10:00Z",
   "metricValue": 112
},
...{
```

```
            "timeStamp": "2015-02-06T22:00:01Z",
            "metricValue": 113
         },
         {
            "timeStamp": "2015-02-06T22:05:00Z",
            "metricValue": 113
         }],

   },
   "name": "Power Supply 01",
   "parent": {
      "uuid": "3D1D5931BDF84D30ADA976E21F08CB91",
      "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91"
   },
   "uuid": "D15D67FD1FBC40A09BEDF97C061A160A",
   "uri": "powerSupply/D15D67FD1FBC40A09BEDF97C061A160A"
}
```


/switches/metrics

Use this REST API to retrieve sample metrics for all Flex System switches.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue). metrics:
- Average Switch Input Power
- Minimum Switch Input Power
- Maximum Switch Input Power

HTTP methods

GET

GET /switches/metrics

Use this method to return a set of sample metrics for all Flex System switches. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Note: Depending on your environment and the number of managed hardware resources, it might take several minutes to retrieve the requested metrics data.

Authentication

Authentication with username and password is required.

Request URL

```
GET https://{management_server_IP}/switches/metrics
```

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=*<attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
switchesList	Array	List of switches.
See GET /switches/metrics/*{uuid}*	Object	Sample metrics for each Flex System switch.

The following example is returned if the request is successful.

```
{
   "switchesList": [{
      "energyMetrics": {
         "averageSwitchModulePower": [{
            "timeStamp": "2015-02-06T18:35:00Z",
            "metricValue": 29
         },
         ...{
            "timeStamp": "2015-02-06T18:49:59Z",
            "metricValue": 30
```

```
            },
            ],
            "minimumSwitchModulePower": [{
               "timeStamp": "2015-02-06T18:35:00Z",
               "metricValue": 29
            },
            ...{
               "timeStamp": "2015-02-06T18:45:00Z",
               "metricValue": 28
            },
            ],
            "maximumSwitchModulePower": [{
               "timeStamp": "2015-02-06T18:35:00Z",
               "metricValue": 31
            },
            ...{
               "timeStamp": "2015-02-06T18:45:00Z",
               "metricValue": 32
            },
            ]
         },
         "name": "IO Module 02",
         "parent": {
            "uuid": "3D1D5931BDF84D30ADA976E21F08CB91",
            "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91"
         },
         "uuid": "1E3B957727F8E11180000002C96317EC",
         "uri": "switch/1E3B957727F8E11180000002C96317EC"
      }]
}
```


/switches/metrics/*{uuid}*

Use this REST API to retrieve sample metrics for a specific Flex System switch.

The following sample metrics are retrieved. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue). metrics:

- Average Switch Input Power
- Minimum Switch Input Power
- Maximum Switch Input Power

HTTP methods

GET

GET /switches/metrics/*{uuid}*

Use this method to return a set of sample metrics for a specific Flex System switch. Each sample is represented in terms of when the sample was taken (timeStamp) and the value of the sample (metricValue).

Authentication

Authentication with username and password is required.

Request URL

`GET https://{management_server_IP}/switches/metrics/{uuid}`

where *{uuid}* is the UUID of the switch to be retrieved. To obtain the switch UUID, use the GET /switches method.

Query parameters

Parameters	Required / Optional	Description
excludeAttributes=*{attributes}*	Optional	Returns a response that excludes the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored. • The response is filtered based on attribute name, not the attribute value. • Base attributes cannot be excluded.
includeAttributes=*<attributes}*	Optional	Returns a response that includes the base attributes and the specified attributes for each resource. You can specify one or more attributes that are listed in the response body, separated by a comma. **Notes:** • The response is filtered based on attribute name, not the attribute value. • If this attribute is not specified, all attributes are returned by default.

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter or request attribute is missing or not valid, or the operation is not supported. A descriptive error message is returned in the response body.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body. Ensure that you have privileges to perform the request.
409	Conflict	There is a conflict with the current state of the resource. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

Each energy metric contains one or more arrays that include when the sample was taken (**timeStamp**) and the value of the sample (**metricValue**).

Attributes	Type	Description
energyMetrics	Object	Energy metrics for the Flex System switch
averageSwitchModulePower	Array of objects	Average switch-module power samples
minimumSwitchModulePower	Array of objects	Minimum switch-module power samples
maximumSwitchModulePower	Array of objects	Maximum switch-module power samples
name	String	Switch name

Attributes	Type	Description
parent	Object	Information about the chassis that contains the switch
uuid	String	Chassis UUID
uri	String	Chassis URI
uuid	String	Switch UUID
uri	String	Switch URI

The following example is returned if the request is successful


```
{
    "energyMetrics": {
        "averageSwitchModulePower": [
            {
                "timeStamp": "2015-02-06T18:35:00Z",
                "metricValue": 29
            },
            ...
            {
                "timeStamp": "2015-02-06T18:49:59Z",
                "metricValue": 30
            },
        ],
        "minimumSwitchModulePower": [
            {
                "timeStamp": "2015-02-06T18:35:00Z",
                "metricValue": 29
            },
            ...
            {
                "timeStamp": "2015-02-06T18:45:00Z",
                "metricValue": 28
            },
        ],
        "maximumSwitchModulePower": [
            {
                "timeStamp": "2015-02-06T18:35:00Z",
                "metricValue": 31
            },
            ...
            {
                "timeStamp": "2015-02-06T18:45:00Z",
                "metricValue": 32
            },
        ]
    },
    "name": "IO Module 02",
    "parent": {
        "uuid": "3D1D5931BDF84D30ADA976E21F08CB91",
        "uri": "chassis/3D1D5931BDF84D30ADA976E21F08CB91"
    },
    "uuid": "1E3B957727F8E11180000002C96317EC",
    "uri": "switch/1E3B957727F8E11180000002C96317EC"
}
```