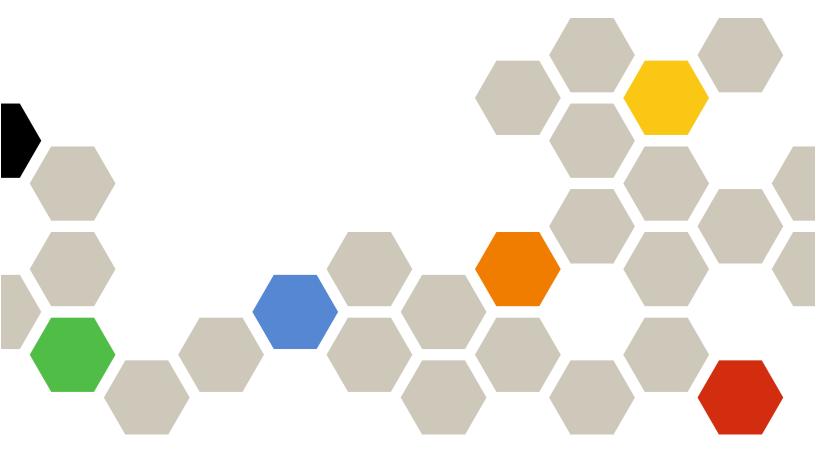# Lenovo XClarity Orchestrator
REST API Reference

Version 2.1

Note

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

Contents

Summary of changes in the REST API for v2.1

Lenovo XClarity Orchestrator v2.1 supports enhancements to the Open REST API.

For a summary of changes to the REST API in other releases, see Summary of changes in the REST API in the XClarity Orchestrator online documentation.

This documentation includes new methods and parameters that apply to the current XClarity Orchestrator release and later. If you are using an earlier release of XClarity Orchestrator, 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 Orchestrator online documentation.

The following methods were added or updated in this release.

- **Orchestrator**

  - (New) POST /api/v1/maintenance/powerOption. Reboot or shut down the orchestrator server.

- **Resources**

  - POST /api/v1/boarding/management. Added a response body for managing and discovering servers in bulk.

  - GET /api/v1/managers-management/managers and GET /api/v1/managers-management/managers/*{id}*. Added the **XClarity Management Hub 2.0** value to the **type** response attribute.

  - POST /api/v1/managers-management/managers. Add support to manage Lenovo XClarity Management Hub 2.0.

- **Jobs**

  - (New) GET /api/v1/jobs-management/schedules. Returns a list of all scheduled jobs.

  - (New) POST /api/v1/jobs-management/schedules. Creates a scheduled job.

  - (New) GET /api/v1/jobs-management/schedules/*{id}*. Returns information about a specific schedule job.

  - (New) DELETE /api/v1/jobs-management/schedules/*{id}*. Cancels a scheduled job.

Chapter 1. Using this REST API

Review this information to learn about how to use the Lenovo XClarity Orchestrator REST API, including authentication requirements, response codes and error handling, and filtering and sorting.

Authorization and authentication

When programming with the Lenovo XClarity Orchestrator 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 XClarity Orchestrator web interface to configure the authorizations that provide access to XClarity Orchestrator tasks and resources (see Creating users in the XClarity Orchestrator online documentation).

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

Paginating, scoping, filtering, sorting, including data, and excluding data in responses

You can use query parameters to limit the number of returned objects and to include, exclude, filter, and sort data in the response body.

Paginating data

If a request returns all resource instances in the response body, you can use query parameters to limit the number of objects that are returned at one time. This is especially useful for the user interface when only a limited number of rows are displayed in a table.

You can use the **limit** query parameter to identify the number of elements to return at one time. The default limit is `10`.

You can use the **offset** query parameter to it identify the offset. The default offset is `0`.

The following example returns the first 20 users.
`/api/v1/auth/users`

The following example returns the next 20 users.
`/api/v1/auth/users?limit=20&offset=20`

The following example returns all users without pagination.
`/api/v1/auth/users?limit=0&offset=0`

Scoping data

If a request returns multiple resource instances in the response body, can narrow the scope of data to only those resources that are in specific resource managers and groups

You can use the following scoping query parameters, based on the resources that you want to scope.

- **managerIDs**. Returns data for all resources that are managed by the specified resource managers.
  `?managerIDs={ID_list}`
  Where *{ID_list}* is one or more resource manager IDs, separated by a comma. The following example scopes the returned data to devices that are managed by specific resource managers.
  `?managerIDs=2A04DFF7DDA8777EBCCD3DAF9F9BEDFD,8D735FCEFBCD49118C68169312166C68`

- **groupIDs**. Returns data for all resources that are members of the specified groups.
  `?groupIDs={ID_list}`
  Where *{ID_list}* is one or more resource group IDs, separated by a comma. The following example scopes the returned data to devices that are managed by specific resource groups.
  `?groupIDs=2A04DFF7DDA8777EBCCD3DAF9F9BEDFD,8D735FCEFBCD49118C68169312166C68`

You can use scoping query parameters in addition to other filtering query parameters. The response body returns only data that matches *all* queries.

Including data

You can use the **includeAttributes** query parameter to include specific attributes in the response body. If this query parameter is present, only the specified attributes are returned. If it is missing, all attributes are returned by default.

`?includeAttributes={attributes_list}`

Where *{attributes_list}* is one or more attributes that are listed in the response body, separated by a comma.

Notes:

- To specify child attributes, use a JSON path separated by a period (for example, drives.capacity).
- When the **includeAttributes** query parameter is specified, the **excludeAttributes** query parameter is ignored.
- *Base attributes* are essential attributes that are always returned in the response body unless excluded using **excludeAttributes** query parameter.

The following example returns data for the base attributes plus two additional attributes (name and severity) in the response body.
`?includeAttributes=name,severity`

Excluding data

You can use the **excludeAttributes** query parameter to exclude specific attributes from the response body. If this query parameter is present, the specified attributes are not returned. If it is missing, all attributes are returned by default.

`?excludeAttributes={attributes_list}`

Where *{attributes_list}* is one or more attributes that are listed in the response body, separated by a comma.

The following example does not return data for two attributes (name and severity). Data for all other attributes are returned in the response body.

`?excludeAttributes=name,severity`

Note: To specify child attributes, use a JSON path separated by a period (for example, drives.capacity).

Filtering resources

If a request returns all resource instances in the response body, you can use the filter query parameters to return data for only those resources that match all the specified criteria.

A single filter query contains two keys-value pairs, separated by an ampersand (&): one pair to specify the response attribute and another pair set to specify the value for that attribute. You can also use an ampersand to separate multiple filter queries in the same URI. If you specify multiple filter queries, data is returned only if it matches all filter queries individually.

You can use the following filter query parameters, based on the type of filter that you want to perform.

- **filterContains[]**. Returns data that contains a specific pattern. Within the same filter query, data matches the query if the value of any one of the specified attributes contains any one of the specified patterns.
  ```
  ?filterContains[{index}][attributes]={attribute_list}
  &filterContains[{index}][values]={pattern_list}
  ```

- **filterNotContains[]**. Returns data that does not contain a specific pattern. Within the same filter query, data matches the query if the value of any one of the specified attributes does not contain any of the specified patterns.
  ```
  ?filterNotContains[{index}][attributes]={attribute_list}
  &filterNotContains[{index}][values]={pattern_list}
  ```

  Note: If you specify **filterContains[]** and **filterNotContains[]** with the same attributes and values, the result is an empty array.

- **filterEquals[]**. Returns data that exactly matches a specific pattern. Within the same filter query, data matches the query if the value of any one of the specified attributes exactly matches any one of the specified patterns.
  ```
  ?filterEquals[{index}][attributes]={attribute}
  &filterEquals[{index}][values]={pattern_list}
  ```

- **filterNotEquals[]**. Returns data that does not exactly match a specific pattern. Within the same filter query, data matches the query if the value of any one of the specified attributes does not exactly match any of the specified patterns.
  ```
  ?filterNotEquals[{index}][attributes]={attribute}
  &filterNotEquals[{index}][values]={pattern_list}
  ```

  Note: If you specify **filterEquals[]** and **filterNotEquals[]** with the same attributes and values, the result is an empty array.

- **filterRange[]**. Returns data that exactly matches a pattern in a specific range. Within the same filter query, data matches the query if the value of any one of the specified attributes exactly matches a pattern in any one of the specified ranges.
  ```
  ?filterRange[{index}][attributes]={attribute_list}
  &filterRange[{index}][values]={pattern_list}
  ```

Where:

- *{index}*. Index number for the filter query. This number must be the same for the attribute and value filters. If there is only one filter query of specific type in the URI, the index number is not required.

- *{attribute_list}*. Zero or more attributes that are associated with the resource, separated by a comma. If an attribute name is not provided, all attributes are evaluated.You *can* specify:
  - Attributes that are associated with the resource, regardless of the whether the attributes are included in the response for the REST API.

    If you choose an attribute that is not in the base response, you can add it to the response by using the **includeAttributes** query parameter.
  - Attributes at the any level. To specify child attributes, use a JSON path separated by a period (for example, drives.capacity).
  - Attributes that contain string values for **filterContains[]**, **filterNotContains[]**, **filterEquals[]**, and **filterNotEquals[]** queries.
  - Attributes that contain timestamp (string) or numerical values for **filterRange[]**queries.

- *{pattern_list}*. One or more patterns, separated by a comma. Patterns are not case sensitive.For **filterRange[]** queries:

  - Each pattern can be a range of timestamps or numbers.

  - Each range contains the start and end values in the range, separated by a comma. Multiple ranges are also separated by a comma.

- If the first value in the range is later than second value, the values are swapped during processing.
- A timestamp must be 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.

Sorting data

If a request returns all resource instances in the response body, you can use the **sort[]** query parameter to sort the returned data. If this query parameter is present, the data is sorted in the order specified. If it is missing, the data is sorted using the default sorting order for the base attributes. The default sorting order varies depending on the resource, and can be determined from the metadata response attribute (see Metadata).

```
?sort[{sort_priority}]={attribute},{sort_order}
```

Where:
- *{sort_priority}*. Sort priority. This can be an integer, where the lowest number is sorted first. If a number is not specified, the priority defaults to the order of the **sort[]** query parameter.
- *{attribute}*. Response attribute name to sort by.
- *{sort_order}*. Sort order. This can be **asc** (ascending) or **desc** (descending).Dates and numbers are sorted in descending order by default. Other strings are sorted in ascending order by default.

The following example sorts data first by name in ascending order and then by severity in descending order.

```
?sort[]=name,asc&sort[]=severity,desc
```

The following example sorts data first by severity in descending order and then by name in ascending order.

```
?sort[1]=name,asc&sort[0]=severity,desc
```

Response codes

The Lenovo XClarity Orchestrator REST APIs use the HTTP protocol for sending and retrieving data. Client code using the REST APIs makes an HTTP request to the XClarity Orchestrator server and processes the HTTP response accordingly. Included with the HTTP response data is the HTTP status code. The status code provides some indication as to the success of the HTTP request and can provide information about 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. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.
201	Created	One or more new resources were successfully created.
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.
204	No Content	The request completed successfully, but no response content is returned (for example, a successful DELETE request).
205	Reset Content	One or more new resources were successfully replaced.

Code	Description	Comments
206	Partial Content	Partial content was returned for a multi-part response. The response header includes a content-range header field indicating the range that is included in the response body for each part.
400	Bad Request	A query parameter 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. For GET requests, this code is returned when the user session is expired because the web inactivity session time-out expired or the mandatory session expiration time was exceeded. You must log in again to view data. For information about session time-outs, see Configuring user security settings in the XClarity Orchestrator online documentation.
403	Forbidden	The orchestrator server was prevented from fulfilling the request. A descriptive error message is returned in the response body.
404	Not found	The resource cannot be found. A descriptive error message is returned in the response body.
405	Method Not Allowed	The resource is invalid. A descriptive error message is returned in the response body.
406	Not Acceptable	The request cannot be fulfilled. A descriptive error message is returned in the response body. POST, PUT, PATCH, and DELETE requests return 406 when the user session is expired because the Web inactivity session for full operations timeout expired or the mandatory session expiration time was exceeded. You must log in again to modify data. For information about session timeouts, see Configuring user security settings in the XClarity Orchestrator online documentation.
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.
410	Gone	The resource no longer available. 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 resource is currently locked and unavailable. A descriptive error message is returned in the response body.
424	Failed Dependency	Clients relies on a previous request that failed, and the server cannot process the request. A descriptive error message is returned in the response body.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Links

Each GET request returns information about the URIs for the resource or resource instance.

Requests that can return only a single resource or a single instance of a resource

Attributes	Type	Description
_links	Object	Information about the URI
rel	String	Relationship. This value is always "self."
uri	String	URI for the current resource

In the following example, the request can return information about only a single resource. This object identifies the URI for that resource.

```
{
    "_links": {
        "rel": "self",
        "uri": "/api/v1/data/devices/AAAAAAAAAAAAAAAAAAAA"
    }
}
```

Requests that can return multiple instances of a resource

Attributes	Type	Description
_metadata	Object	Information about the request, including the request URI, base attributes, sorting, and filtering for the specified query For information about other metadata attributes, see Metadata.
_links	Object or Array of objects	Information about the URI
rel	String	Relationship. This can be one of the following values. • **prev**. Link information for the previous set of members. • **self**. Link information for the current set of members. • **next**. Link information for the next set of members.
uri	String	URI for the current resource

In the following example, pagination is used to return information for multiple devices in chunks of 20. The **_links** attribute is an array of objects. The first object in the array identifies information about the URI for the current response body, with the first 20 devices. The first object in the array identifies information about the URI for the next response body, with next 20 devices

```
{
    "_links": [{
        "rel": " self ",
        "uri": "/api/v1/data/devices?offset=0&limit=20"
    },
    {
        "rel": " next ",
        "uri": "/api/v1/data/devices?offset=20&limit=20"
    }]
}
```

In the following example, all devices are returned in the current response body. (Pagination is not used).

```
{
    "_links": [{
        "rel": "self",
        "uri": "/api/v1/data/devices?offset=0&limit=0"
    }]
}
```

Metadata

If a GET request returns multiple instances of a resource type, the response body returns the **_metadata** attribute. The _metadata attribute contains information that describes the returned data, including the request URL, total number of resources instances, pagination information, and the common query parameters that are supported by the request. If common query parameters are not specified, default values are returned.

Note: If a GET request returns a single resource or a single instance of a resource, the **_metadata** attribute is not returned.

The following table describes the attributes that can be returned in the **_metadata** attribute.

For more information about common query parameters, see Paginating, scoping, filtering, sorting, including data, and excluding data in responses.

Attributes		Type	Description
_metadata		Object	Information about the request, including the request URL, base attributes, sorting, and filtering for the specified query
	limit	Integer	Number of resource instances that can be returned on the page (for pagination) If set to 0, all instances are returned.
	offset	Integer	Offset at which to start the set of resource instances to be returned (for pagination)
	total	Integer	Total number of resource instances that are available (for pagination)
	baseAttributes	Array of objects	Information about essential (default) attributes that are returned in the response body
	name	String	Name of the base attribute
	sortOrder	String	Default sort order for the attribute. This can be one of the following values. • **asc**. Ascending order • **desc**. (default) Descending order
	excludeAttributes	Array of strings	List of attributes, separated by a comma, that are excluded in the response body This attribute is returned only when the **excludeAttributes** query parameter is supported. **Note:** When both **excludeAttributes** and **includeAttributes** query parameters are specified, the **excludeAttributes** query is ignored; in this case, the value of the **excludeAttributes** attribute is empty.
	includeAttributes	Array of strings	List of attributes, separated by a comma, that are included in the response body **Note:** If the **excludeAttributes** query parameter is specified, the **includeAttributes** attribute is empty.
	filterOptions	Array of objects	List of criteria that is used to limit the resources that are returned in the response body when a filter query parameter is specified **Note:** If filter query parameters are not specified, the **filterOptions** attribute is empty.

Attributes			Type	Description
filterContains			Array of objects	Information about filter queries that search for data that *contains* a specific value Within the same filter query, data matches the query if the value of any one of the specified attributes contains any one of the specified patterns
	attributes		String	List of zero or more attribute names in the filter query, separated by a comma If an attribute name is not provided, all attributes are evaluated.
	values		String	List of one or more patterns, separated by a comma
filterNotContains			Array of objects	Information about filter queries that search for data that *exactly matches* a specific value Within the same filter query, data matches the query if the value of any one of the specified attributes contains any one of the specified patterns
	attributes		String	List of zero or more attribute names in the filter query, separated by a comma If an attribute name is not provided, all attributes are evaluated.
	values		String	List of one or more patterns, separated by a comma
filterEquals			Array of objects	Information about filter queries that search for data that *exactly matches* a specific value Within the same filter query, data matches the query if the value of any one of the specified attributes contains any one of the specified patterns
	attributes		String	List of zero or more attribute names in the filter query, separated by a comma If an attribute name is not provided, all attributes are evaluated.
	values		String	List of one or more patterns, separated by a comma
filterNotEquals			Array of objects	Information about filter queries that search for data that *exactly matches* a specific value Within the same filter query, data matches the query if the value of any one of the specified attributes contains any one of the specified patterns
	attributes		String	List of zero or more attribute names in the filter query, separated by a comma If an attribute name is not provided, all attributes are evaluated.
	values		String	List of one or more patterns, separated by a comma
filterRange			Array of objects	Information about filter queries that search for data that matches a value in a specific range Within the same filter query, data matches the query if the value of any one of the specified attributes contains any one of the specified patterns
	attributes		String	List of zero or more attribute names in the filter query, separated by a comma If an attribute name is not provided, all attributes are evaluated.

Attributes			Type	Description
		values	String	List of one or more patterns, separated by a comma Each range contains the start and end values in the range, separated by a comma. Multiple ranges are also separated by a comma. 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.
	sortOptions		Array of objects	List of criteria that is used to sort the resources that are returned in the response body when the **sort** query parameter is specified **Tip:** The order of the returned attributes identifies the sort order of the attributes.
		name	String	Name of the attribute to sort by
		order	String	Sort order. This can be one of the following values. • **asc**. Ascending order • **desc**. (default) Descending order
	_links		Object or Array of objects	Request URL (see Links)

The following example returns metadata for a specific request when no query parameters are specified.

```
{
    "metadata": {
        "offset": 0,
        "limit": 0,
        "total": 2,
        "baseAttributes": [{
            "name": "msg"
        },
        {
            "name": "service"
        },
        {
            "name": "severity"
        },
        {
            "name": "systemName "
        },
        {
            "name": "systemType "
        },
        {
            "name": "timeStamp",
            "sortOrder": "asc"
        }],
        "excludeAttributes": [],
        "includeAttributes": [
            "msg",
            "service",
            "severity",
            "systemName",
            "systemType",
            "timeStamp"
        ],
        "filterOptions": {},
        "sortOptions": [{
```

```
            "name": "timeStamp",
            "order": "asc"
        }],
        "_links": {
            "rel": "self",
            "uri": "/api/v1/inbound/events?offset=0&limit=0"
        }
    }
}
```

Status messages

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

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.

GET requests that are successful (2xx response code) *do not* include a status-message attributes. 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.

Note: If the server returns multiple messages for a single request, the top-level attributes are used to describe the overall status of the request, and each message is returned in the **messages** array.RL

Attributes		Type	Description
status		String	Overall status of the request. This can be one of the following values. • **Informational**. The request completed successfully. • **Warning**. The request completed with warnings. • **Critical**. The request failed. In case there are messages in the **messages** array, then this is the most severe from all the messages.
code		String	Message code (see Event and alert messages in the XClarity Orchestrator online documentation)
text		String	Message text that is associated with the message ID
description		String	Additional information to clarify the reason for the message
userAction		String	User actions that can be taken to recover from the error
recoveryURL		String	Link to more information or recovery actions, if available
messages		Array of objects	Information about multiple messages
	status	String	Status of the request. This can be one of the following values. • **Informational**. The request completed successfully. • **Warning**. The request completed with warnings. • **Critical**. The request failed. In case there are messages in the **messages** array, then this will be the most severe from all the messages.
	code	String	Message ID (see Event and alert messages in the XClarity Orchestrator online documentation)
	text	String	Message text that is associated with the message ID
	description	String	Additional information to clarify the reason for the message

Attributes	Type	Description
userAction	String	User actions that can be taken to recover from the error
recoveryURL	String	Link to more information or recovery actions, if available

The following example is returned for a single-message response.

```
{
    "status": "Informational",
    "code": "FQXXOSE0001I",
    "text": "The request completed successfully.",
    "description": "",
    "userAction": "Information only; no action is required.",
    "recoveryURL": ""
}
```

The following example is returned for a multi-message response.

```
{
    "status": "Critical",
    "code": "",
    "text": " There was an error parsing the input.",
    "description": "",
    "userAction": "",
    "recoveryURL": "",
    "messages": [{
        "status": "Critical",
        "code": "FQXDM0558G",
        "text": " A specified attribute is not compatible with the value of another attribute.",
        "description": "The field {1} is not allowed when field {2} has value {3}.",
        "userAction": "Correct the values, and attempt the request again.",
        "recoveryURL": ""
    },
    {
        "status": "Critical",
        "code": "FQXDM0557G",
        "text": "Incompatible fields were specified.",
        "description": "The field {1} is not allowed when field {2} is specified.",
        "userAction": " Correct the values, and attempt the request again.",
        "recoveryURL": ""
    }]
}
```

Chapter 2. Orchestrator server

The following REST APIs are available for working with the Lenovo XClarity Orchestrator.

/api/v1/maintenance/powerOption

Use this REST API to reboot or shutdown the orchestrator server.

Note: This REST API requires Lenovo XClarity Orchestrator v2.1 or later.

HTTP methods

POST

POST /api/v1/maintenance/powerOption

Use this method to reboot or shut down the orchestrator server.

Note: This REST API requires Lenovo XClarity Orchestrator v2.1 or later.

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{orchestrator_server_IP}*/api/v1/maintenance/powerOption

Query parameters

None

Request body

Attributes	Re- quired / Optional	Type	Description
powerOption	Required	String	Power action to perform on the orchestrator server. This can be one of the following values. • **Reboot** • **Shutdown**

The following example restarts the orchestrator server.
```
{
   "powerOption": "Reboot"
}
```

The following example shuts down the orchestrator server.
```
{
   "powerOption": "Shutdown"
}
```

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
{message_attributes}	*varies*	Status messages (see Status messages)

Chapter 3. Security

The following REST APIs are available for managing security.

/api/v1/maintenance/certificate

Use this REST API to retrieve, export, or regenerate the XClarity Orchestrator server certificate.

HTTP methods

GET, DELETE

GET /api/v1/maintenance/certificate

Use this method to return information about or save (export) the XClarity Orchestrator server certificate.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/maintenance/certificate`

Query parameters

Parameters	Re-quired / Optional	Description
format=*{type}*	Optional	Response format. This can be one of the following values. • **pem**. Export the server certificate as a file in PEM format. • **json**. (default) Return the server certificate in the response body in JSON format.

The following example retrieves the server certificate in JSON format.
GET `https://192.0.2.0/api/v1/communications/certificates/7633531801c5688f7d3b830d57cdea73`

The following example exports the server certificate as a file in PEM format.
GET `https://192.0.2.0/api/v1/communications/certificates/7633531801c5688f7d3b830d57cdea73?format=pem`

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a query parameter is specified and the value of that parameter has no matches, the response body returns default values.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

When **format=pem** is specified, the response body is returned only when the request generates an error (see Status messages).

When **format=json** is specified and the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
pem	String	Server certificate, in PEM format
_links	Object	Server certificate URI (see Links)

The following example is returned if the request is successful.

```
{
    "pem": "-----BEGIN CERTIFICATE-----\nMIIDuDCCAqCgAwIBAgIUQ1JWiK2/OUvzWcreE
YEtuQ6TgiYwDQYJKoZIhvcNAQEL\nBQAwSzEMMAoGA1UECwwDRENHMQ8wDQYDVQQKDAZMZW5vdm8x
EDAOBgNVBAcMB1Jh\nbGVpZ2gxCzAJBgNVBAgMAk5DMQswCQYDVQQGEwJVUzAeFw0yMDEwMDgxNDU
OMDRa\nFw0zMDEwMDYxNDU0MDRaMIGSMQswCQYDVQQGEwJVUzEPMAOGA1UECgwGTGVub3Zv\nMUUw
QwYDVQQDDDxHZW5lcmF0ZWQgYnkgTGVub3ZvIE1hbmFnZW1lbnQgRWNvc3lz\ndGVtIG9uIElQIDE
wLjIOMy4xNy4xMDgxCzAJBgNVBAgMAk5DMQwwCgYDVQQLDANE\nQ0cxEDAOBgNVBAcMB1JhbGVpZ2
gwggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEK\nAoIBAQCfkDRxfvLmzd3QswmdFwZRR6X3jlxTh
RfHca7AwiyKX/CgOI9Vh/TCkw5W\nANlB3DdKFJSntgXTNhrjWk4y1boNDaBmr1eHFhjQYGRteHVr
fPPafSYkOAKEIsV9\nX9h8iOe7HJZeCqaON6GqK8/uTo62kInFqqREOYqWkO/jFdFnKFj69Nf9JOu
qABPc\nnb+tlXkWggRDrizvZMs3qRdjktd7Cl+8pbDKJuaUw9ZyfnNFWd2Rv8edITez15pU\nbJjl
YqUzGeaAr/PnxUBrlZlS9qDPUj6ZxlnxQ2yxy5xsUYVkBUmwZq5nCdQ2yLqw\nOqB5LFUvJKo3I6m
7dXLO9IN8gOhDAgMBAAGjTDBKMB8GA1UdIwQYMBaAFD+FiELg\nA+OFa+IexISpy9kHuj9eMAkGA1
UdEwQCMAAwCwYDVROPBAQDAgTwMA8GA1UdEQQI\nMAaHBArzEWwwDQYJKoZIhvcNAQELBQADggEBA
E1iJVWCtYAQ8lVtegoOnWhscUXn\nV9lwxuCUtwyKUk9eMF7syrC4TYBad3KLZT8eUvLhn2rA47dN
YHc92I9YPRR+DZZQ\nCmH3epUXcAKaeCJXSvIRPqGXHO7Ziv6xi6yvu2AVbz/bQOeSrAbFnYnvXTm
mQjhx\nO6mLU3vYlG13fuJZlVRDg+ekOyKEbEyBxMPFFbz2yh/J/dJ4RzSVsOxOtcqAv+8U\nW9yq
DhK9L7ywhlblhUdeDBS/AcOyLnRIvVPUtRKOOMnCoJqEAYD1W28TGaUfqB2+\nOv4SuSuv7v6oyDS
H3bARQ4ykmyXBlzuMNjD3Pgwp6Kpq6+CEcWcB9SYQgjw=\n-----END CERTIFICATE-----\n",
    "_links": {
        "rel": "self",
        "uri": "/api/v1/maintenance/certificate"
    }
}
```

DELETE /api/v1/maintenance/certificate

Use this method to delete and regenerate the Lenovo XClarity Orchestrator server certificate.

Authentication

Authentication with username and password is required.

Resource URI

DELETE https://*{orchestrator_server_IP}*/api/v1/maintenance/certificate

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
{message_attributes}	varies	Status messages (see Status messages)

/api/v1/maintenance/certificateSettings

Use this REST API to return and modify the XClarity Orchestrator server certificate settings.

HTTP methods

GET, PUT

GET /api/v1/maintenance/certificateSettings

Use this method to return information about the XClarity Orchestrator server certificate settings.

Note: You can retrieve setting using this GET request only after you first modify the settings using PUT /api/ v1/maintenance/certificateSettings.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/maintenance/certificateSettings`

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.

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Response body

Attributes	Type	Description
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) To retrieve the country or region codes, use GET /api/v1/service/ countryCodes.
notAfter	String	Timestamp before which the created certificate is not 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.
notBefore	String	Timestamp after which the created certificate is not 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.
organization	String	Organization (company) that owns the certificate. Typically, this is the legal incorporate name of a company. It should include any suffixes, such as Ltd., Inc., or Corp.
organizationUnit	String	Organizational unit that owns the certificate
stateLocality	String	Full name of the locality (city) to be associated with the certificate
stateProvince	String	Full name of the state or province to be associated with the certificate
_links	Object	Server certificate URI (see Links)

The following example is returned if the request is successful.

```
{
    "commonName": "Generated by Lenovo Management Ecosystem on IP 10.243.17.108",
    "country": "US",
    "notAfter": "2030-10-06T14:54:04.000Z",
    "notBefore": "2020-10-08T14:54:04.000Z",
    "organization": "Lenovo",
    "organizationUnit": "DCG",
    "stateLocality": "Raleigh",
    "stateProvince": "NC",
    "_links": {
        "rel": "self",
        "uri": "/api/v1/maintenance/certificateSettings"
    }
}
```

PUT /api/v1/maintenance/certificateSettings

Use this method to modify the Lenovo XClarity Orchestrator server certificate settings.

Authentication

Authentication with username and password is required.

Resource URI

PUT `https://{orchestrator_server_IP}/api/v1/maintenance/certificateSettings`

Query parameters

None

Request body

This PUT request updates the entire resource. To clear a value, set the attribute to null (if applicable). If an array is specified, the entire array is replaced (unless stated otherwise). If an optional attribute is not specified, that attribute is not changed. If an immutable (unchangeable) attribute is specified, it is ignored.

Attributes	Re- quired / 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.
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) To retrieve the country or region codes, use GET /api/v1/ service/countryCodes.
notAfter	Optional	String	Timestamp before which the created certificate is not 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.
notBefore	Optional	String	Timestamp after which the created certificate is not 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.
organization	Optional	String	Organization (company) that owns the certificate. Typically, this is the legal incorporate name of a company. It should include any suffixes, such as Ltd., Inc., or Corp. The length of this value cannot exceed 60 characters.
organizationUnit	Optional	String	Organizational unit that owns the certificate The length of this value cannot exceed 60 characters.
stateLocality	Optional	String	Full name of the locality (city) to be associated with the certificate The length of this value cannot exceed 50 characters.
stateProvince	Optional	String	Full name of the state or province to be associated with the certificate

The following example modifies the server certificate settings.

```
{
    "commonName": "Generated by Lenovo System Management Software",
    "country": "US",
    "notAfter": "2069-12-31T23:59:59Z",
    "notBefore": "1970-01-01T00:00:00Z",
    "organization": "Lenovo",
```

```
    "organizationUnit": "EBG",
    "stateLocality": "Raleigh",
    "stateProvince": "North Carolina"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter 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_attributes}	*varies*	Status messages (see Status messages)

/api/v1/maintenance/certificateSigningRequest

Use this REST API to return the current Certificate Signing Request (CSR) or generate a new CSR.

HTTP methods

GET, POST

GET /api/v1/maintenance/certificateSigningRequest

Use this method to return or save (export) the current Certificate Signing Request (CSR).

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/maintenance/certificateSigningRequest`

Query parameters

Parameters	Re-quired / Optional	Description
format=*{type}*	Optional	Response format. This can be one of the following values. • **pem**. Export the CSR as a file in PEM format. • **json**. (default) Return the CSR in the response body in JSON format.

The following example retrieves the current CSR in JSON format.
GET `https://192.0.2.0/api/v1/maintenance/certificateSigningRequest`

The following example exports the current CSR as a file in PEM format.
GET `https://192.0.2.0/api/v1/maintenance/certificateSigningRequest?format=pem`

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a query parameter is specified and the value of that parameter has no matches, the response body returns default values.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response body

When **format=pem** is specified, the response body is returned only when the request generates an error (see Status messages).

When **format=json** is specified and the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
pem	String	CSR, in PEM format
_links	Object	CSR URI (see Links)

The certificate signing request is returned if the request is successful, for example:

```
{
    "pem": "-----BEGIN CERTIFICATE REQUEST-----MIIDjDCCAnQCAQAwgYoxCzAJBgNVBA
YTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UECh
McR2VuZXJhdGVkIGJ5IFNlcnZlciBGaXJtd2FyZTEaMBgGA1UECxMRT3JnYW5pemF0aW9uIHVuaX
QxDTALBgNVBAMTBExYQQEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCMwy8q5PrWhH
tLv1c00dVJiXTHK3JNcQXicWXzL3/+vhGkgfd8rqqCvvxjTg7N2hYaFlQghEFTEWDhMmxvMFZtAh
QfBnzcdiWj23I3MSRqDWBa8NsqHWffxyqcOEqhoGiOMCjHW9zdkSkJOfZvFJ5RTPmhY+Xnt92lZg
SGwmnTcGq9dxNvV6ixMvnHzWE9+MguTxsfGMSRZJ4Rf+d35X9ovQHEge1jMaqOcoBuqVMK9TkWsb
101GJ2tggDR5tp8YHws7wakp1isXc4AtDDIzrKfhxvxqTHqsAppREQD79srzsG+jNsOYvg7Jd7bm
2/zP9gxMwVFUYOm7DYg8HF6mZ9AgMBAAGggbswgbgGCSqGSIb3DQEJDjGBqjCBpzCBpAYDVRORBI
GcMIGZhxD+gAAAAAAAAoAJ//+zQ6Dgh5mZTgwOjA6MDowOmEwMDoyN2ZmOmZlY2Q6ZTgzJTKHBA
rxieCCIGlwMTAtMjQxLTEzNyOyMjQubGFicy5sZW5vdm8uY29thxAAAAAAAAAAAAAAAAAAAAABgg
lsb2NhbGdhvc3SHBH8AAAGCCWxvY2FsaG9zdIIJbG9jYWxob3NOqqgRMWENBMAOGCSqGSIb3DQEBCw
UAA4IBAQACBKc6nxzo/8NBQOxuRe+wOMNzrAg9cIyh7cFCcTbSVmamOxAauRHvVIsgE/x/xQP3tQ
FvfJOqYr4eyJvEqHINY71ZgQjIunMVX9Oqf5MEdbYEsQE7g/2WzVXIDZ6p1qewjW85YeunHVS3fg
WfD3jXZ66BXZyEB4l7xRtOr85E6bCkhlymj3O6OLHCdmeCewT/rOaOKnR9trSBB2zSkqTPSaxJQX
B+6rKS+DGu+lSCNHYLr8cKYloLaGO8GaRZF4kedPQ1JSoz4jXOdgkPzqAXJlOJVWPUEkKLpGUomB
BBUK5PwBN1OkuB8c/wXhB9+ki3CpcolGXoBpJk+fM6ij/8-----END CERTIFICATE REQUEST-----",
    "_links": {
        "rel": "self",
        "uri": "/api/v1/maintenance/certificateSigningRequest"
    }
}
```

POST /api/v1/maintenance/certificateSigningRequest

Use this method to generate a Certificate Signing Request (CSR) using specific server-certificate settings or regenerate the CSR using the current settings. The existing CSR is overwritten with the new CSR.

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{orchestrator_server_IP}*/api/v1/maintenance/certificateSigningRequest

Query parameters

None

Request body

Attributes		Required / Optional	Type	Description
altNames		Optional	Array of objects	Information about the Subject Alternative Names to be included in Certificate Signing Request
	name	Required	String	Subject Alternative Name
	type	Required	String	RFC 5280 GeneralName type of this Subject Alternative Name
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 LXCO.
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) To retrieve the country or region codes, use GET /api/v1/ service/countryCodes. 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 following example generates the certificate signing request using the specified server certificate settings

```
{
    "altNames": [{
```

```
    "name": "bar.example.org",
    "type": "DNS"
},
{

    "name": "foo.example.org",
    "type": "DNS"
},
{

    "name": "10.241.54.111",
    "type": "IP"
},
{

    "name": "test@test.com",
    "type": "email"
}],
"commonName": "10.241.54.169",
"country": "US",
"organization": "Lenovo",
"organizationUnit": "LXCO",
"stateLocality": "Raleigh",
"stateProvince": "North Carolina"
}
```

Response codes

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

Response header

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

/api/v1/maintenance/signedCertificate

Use this REST API to upload a new signed Lenovo XClarity Orchestrator server certificate that was generated using a certificate signing request.

HTTP methods

POST

POST /api/v1/maintenance/signedCertificate

Use this method to update the signed Lenovo XClarity Orchestrator server certificate that was generated using a certificate signing request.

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

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{orchestrator_server_IP}*/api/v1/maintenance/signedCertificate

Query parameters

None

Request body

Provide the server certificate, in PEM format, that was created from the certificate signing request using the GET /api/v1/maintenance/certificateSigningRequest or downloaded from the XClarity Orchestrator user interface. The following example is provided in the request body

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDjDCCAnQCAQAwgYoxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJv
bGluYTEQMA4GA1UEBxMHUmFsZWlnaDElMCMGA1UEChMcR2VuZXJhdGVkIGJ5IFNl
cnZlciBGaXJtd2FyZTEaMBgGA1UECxMRT3JnYW5pemF0aW9uIHVuaXQxDTALBgNV
BAMTBExYQOEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCMwy8q5PrW
hHtLv1cOOdVJiXTHK3JNcQXicWXzL3/+vhGkgfd8rqqCvvxjTg7N2hYaFlQghEFT
EWDhMmxvMFZtAhQfBnzcdiWj23I3MSRqDWBa8NsqHWffxyqcOEqhoGiOMCjHW9zd
kSkJOfZvFJ5RTPmhY+Xnt92lZgSGwmnTcGq9dxNvV6ixMvnHzWE9+MguTxsfGMSR
ZJ4Rf+d35X9ovQHEge1jMaqOcoBuqVMK9TkWsb101GJ2tggDR5tp8YHws7wakp1i
sXc4AtDDIzrKfhxvxqTHqsAppREQD79srzsG+jNsOYvg7Jd7bm2/zP9gxMwVFUYO
m7DYg8HF6mZ9AgMBAAGggbswgbGCSqGSIb3DQEJDjGBqjCBpzCBpAYDVRORBIGc
MIGZhxD+gAAAAAAAAoAJ//+zQ6Dgh5mZTgwOjA6MDowOmEwMDoyN2ZmOmZlY2Q6
ZTgzJTKHBArxieCCIGlwMTAtMjQxLTEzNyOyMjQubGFicy5sZW5vdm8uY29thxAA
AAAAAAAAAAAAAAAAAAABgglsb2NhbGhvc3SHBH8AAAGCCWxvY2FsaG9zdIIJbG9j
YWxob3N0ggRMWENBMA0GCSqGSIb3DQEBCwUAA4IBAQACBKc6nxzo/8NBQOxuRe+w
OMNzrAg9cIyh7cFCcTbSVmamOxAauRHvVIsgE/x/xQP3tQFvfJOqYr4eyJvEqHIN
Y71ZgQjIunMVX9Oqf5MEdbYEsQE7g/2WzVXIDZ6p1qewjW85YeunHVS3fgWfD3jX
Z66BXZyEB4l7xRtOr85E6bCkhlymj3O6OLHCdmeCewT/rOaOKnR9trSBB2zSkqTP
SaxJQXB+6rKS+DGu+lSCNHYLr8cKYloLaGO8GaRZF4kedPQ1JSoz4jXOdgkPzqAX
JlOJVWPUEkKLpGUomBBBUK5PwBN1OkuB8c/wXhB9+ki3CpcolGXoBpJk+fM6ij/8
-----END CERTIFICATE REQUEST-----
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter 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

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

/api/v1/service/countryCodes

Use this REST API to return a list of country and region codes.

HTTP methods

GET

GET /api/v1/service/countryCodes

Use this method to return a list of country and region codes.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/service/countryCodes

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes		Type	Description
results		Array of objects	Information about each country or region
	abbreviation	String	Two-letter ISO 3166 code for the country or region
	name	String	Country or region name
_links		Object	Resource URI (see Links)

The following example is returned if the request is successful.

```
{
    "result": [
        {
            "abbreviation": "AO",
            "name": "ANGOLA"
        },
        {
            "abbreviation": "AR",
            "name": "ARGENTINA"
        },
        ...,
        {
            "abbreviation": "ZM",
            "name": "ZAMBIA"
        },
        {
            "abbreviation": "ZW",
            "name": "ZIMBABWE"
        }
    ],
    "_links": {
        "rel": "self",
        "uri": "/api/v1/service/countryCodes"
    }
}
```

Chapter 4. Authentication and authorization

The following REST APIs are available for managing authentication and access control.

/api/v1/auth/heartbeat

Use this REST API to determine whether the current user session is active.

HTTP methods

GET

GET /api/v1/auth/heartbeat

Use this method to return whether the current user session is active and has a valid access token.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/auth/heartbeat`

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.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
secondsLeftInFullOperationTime-out	Integer	Amount of time, in seconds, that is left before the full-operations timeout expires When the session is active, the timer resets every time the user performs any action. If this timeout value is exceeded but the primary view-operations timeout value *is not* exceeded, the user can continue to perform view-only actions (such as opening or refreshing a page) until the primary view-operations timeout value is exceeded; however, if the user attempts to perform an action that modifies data, the user session expires and the login page is displayed. This value is **0** if the timeout expired. This value is **-1** if the timeout is disabled.
secondsLeftInViewOperationTi-meout	Integer	Amount of time, in seconds, that is left before the view-operations timeout expires When the session is active, the timer resets every time the user performs any action. After the timeout value is exceeded, the login page is displayed the next time the user attempts to perform an action. This value is **0** if the timeout expired. This value is **-1** if the timeout is disabled.

The following example is returned if the request is successful.

```
{
    "secondsLeftInFullOperationTimeout": 1157,
    "secondsLeftInViewOperationTimeout": 85757
}
```

/api/v1/auth/roles

Use this REST API to return a list of all roles .

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

HTTP methods

GET

GET /api/v1/auth/roles

Use this method to return a list of all roles.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/auth/roles

Query parameters

This REST API supports query parameters for paginating, filtering, sorting, including data, and excluding data in the response. For more information about these common query parameters, see Paginating, scoping,

filtering, sorting, including data, and excluding data in responses. For a list of supported attributes, see GET /api/v1/auth/roles/*{id}*.

The following example returns a list of predefined roles.
```
GET https://192.0.2.0/api/v1/auth/roles
?filterEquals[][attributes]=type&filterEquals[][values]=predefined
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
results	Array of objects	Information about each role
id	String	Role ID
description	String	Role description
name	String	Role name
type	String	Role type (translated). This can be one of the following values. • **custom** • **predefined**
typeKey	String	Role type key. This can be one of the following values. • **custom** • **predefined**
_links	Object	Resource URI (see Links)
_metadata	Object	Request metadata (see Metadata)

The following example is returned if the request is successful.
```
{
   "results": [{
      "id": "A573CEDC",
      "description": "Allows user to view only the orchestrator server configuration and view
                  data for accessible resources.",
      "name": "Operator",
      "type": "Predefined",
      "typeKey": "Predefined",
      "_links": [{
         "rel": "self",
         "uri": "/api/v1/auth/roles/A573CEDC"
      }]
   },
```

```
{
    "id": "97A7A3BA",
    "description": "Allows user to view status and perform certain actions on accessible
                    resources(such as managing inventory, alerts and service tickets).
                    This role prohibits users from updating software or firmware on managed
                    esources, creating resource groups and from customizing analytics.",
    "name": "Operator Legacy",
    "type": "Predefined",
    "typeKey": "Predefined",
    "_links": [{
       "rel": "self",
       "uri": "/api/v1/auth/roles/97A7A3BA"
    }]
},
{
    "id": "B72BE093",
    "description": "Allows user to view status, view and customize analytics, and perform
                    actions on accessible resources. This role prohibits users from updating software or
                    firmware on managed resources.",
    "name": "Hardware Administrator",
    "type": "Predefined",
    "typeKey": "Predefined",
    "_links": [{
       "rel": "self",
       "uri": "/api/v1/auth/roles/B72BE093"
    }]
},
{
    "id": "09C606ED",
    "description": "Allows user to modify security settings and perform security-related
                    actions on the orchestrator server, view data for accessible resources, and view
                    predefined analytics.",
    "name": "Security Administrator",
    "type": "Predefined",
    "typeKey": "Predefined",
    "_links": [{
       "rel": "self",
       "uri": "/api/v1/auth/roles/09C606ED"
    }]
},
{
    "id": "016C2E7E",
    "description": "Allows user to view data about and perform all available actions on the
                    orchestrator server and all managed resources (resource managers and devices). Users that
                    are assigned this role always have access to all managed resources. You cannot restrict
                    access to resources for this role.",
    "name": "Supervisor",
    "type": "Predefined",
    "typeKey": "Predefined",
    "_links": [{
       "rel": "self",
       "uri": "/api/v1/auth/roles/016C2E7E"
    }]
},
{
    "id": "4383E7BF",
    "name": "Updates Administrator",
    "description": "Allows user to manage the updates repository, create update-compliance
                    policies, deploy those policies to managed resources, view data for accessible resources,
                    and view predefined analytics.",
    "type": "Predefined",
```

```
        "typeKey": "Predefined",
        "_links": [{
            "rel": "self",
            "uri": "/api/v1/auth/roles/4383E7BF"
        }]
    }],
    "_metadata": {…}
}
```

/api/v1/auth/roles/*{id}*

Use this REST API to return information about .

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

HTTP methods

GET

GET /api/v1/auth/roles/*{id}*

Use this method to return information about a specific role.

Note: This REST API requires Lenovo XClarity Orchestrator v1.2 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://`*{orchestrator_server_IP}*`/api/v1/auth/roles/`*{id}*

where *{id}* is the ID of the role. To obtain the role IDs, use GET /api/v1/auth/roles

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
id	String	Role ID
description	String	Role description
functions	Array of strings	Information about each function that this role can perform
id	String	Function ID
name	String	Function name
uri	String	Function URI
name	String	Role name
type	String	Role type (translated). This can be one of the following values. • **custom** • **predefined**
typeKey	String	Role type key. This can be one of the following values. • **custom** • **predefined**
userGroups	Array of objects	Information about each user group that is associated with the role
id	String	User group ID
name	String	User group name
uri	String	User group URI
_links	Object	Roles URI (see Links)

The following example is returned if the request is successful.

```
{{
    "id":"61f403c6d9197241f2f8ea7a",
    "description": "HCI admin description",
    "functions": [{
        "id": "19A6C913",
        "name": "functionName",
        "uri": "/api/v1/auth/functions/19A6C913"
    }, {
        "id": "46CFE971",
        "name": "functionName",
        "uri": "/api/v1/auth/functions/46CFE971"
    }],
    "name": "HCI Admin",
    "type": "Custom",
    "typeKey": "CustomTranslated",
    "userGroups": [{
        "id": "19A6C945",
        "name": "userGrName",
        "uri": "/api/v1/auth/userGroups/19A6C945"
    }, {
        "id": "19A6C343",
        "name": "userGrName",
        "uri": "/api/v1/auth/userGroups/19A6C343"
    }],
    "_links": [{
        "rel":    "self",
        "uri":    "/api/v1/auth/roles/61f403c6d9197241f2f8ea7a"
```

```
    }]
}
```

Chapter 5. Resources

The following REST APIs are available for working with resource managers and their managed devices and infrastructure resources.

/api/v1/boarding/agentInstaller

Use this method to create a Lenovo Universal Device Client (UDC) agent installation package for specific devices. This UDC agent must be installed on ThinkEdge Client devices so that the devices can be securely discovered and managed by a Lenovo XClarity Management Hub resource manager.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

HTTP methods

POST

POST /api/v1/boarding/agentInstaller

Use this method to create a Lenovo Universal Device Client (UDC) agent installation package for specific ThinkEdge Client devices. This UDC agent must be installed on ThinkEdge Client devices so that the devices can be securely discovered and managed by a Lenovo XClarity Management Hub resource manager.

After the UDC-agent installation package is created, you can download the package the local system using GET /api/v1/boarding/agentInstaller/*{filename}*.

An asynchronous job is created to complete this request. The response header returns the job URI and job ID.

A successful response code indicates that the job was successfully transmitted and accepted by the hub. 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 Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{orchestrator_server_IP}*/api/v1/boarding/agentInstaller

Query parameters

None

Request body

Attributes	Re- quired / Optional	Type	Description
expirationTimeInDays	Optional	Integer	Number of days before the UDC agent installer becomes unusable after it is downloaded. This can be one of the following values. • **10** • **30** (default) • **60** • **90**
managerID	Required	String	Lenovo XClarity Management Hub resource manager ID
maxUsageLimit	Optional	Integer	Number of times that you plan to install the UDC agent on a server. This is typically the number of servers on which you need to install the UDC agent. The minimum value is **1**, and the maximum value is **1,000,000**. The default is **10** usages.
operatingSystem	Required	String	Operating system that is installed on the server • **LinuxARM** • **LinuxX86** • **Windows**

The following example create a UDC-agent installation package for up to 10 Windows-based ThinkEdge Client devices that can be installed within 7 days and can be managed by a specific Lenovo XClarity Management Hub resource manager.

```
{
    expirationTimeInDays: 7,
    managerID: "48331a223bf34fba90732b379b837b9c",
    maxUsageLimit: 10,
    operatingSystem: "Windows"
}
```

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.

Response header

The URI and ID of the root job are returned in the **Location** and **JobID** fields respectively.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
installer	String	File name of the UDC agent installer, in the following format: edgeInstaller_{operatingSystem}_{managerID}_{timestamp}.gz for Linux or zip for Windows}
jobID	Integer	Job ID
_links	Object	Resource URI (see Links)

The following example is returned if the request is successful.

```
{
    installer: "edgeInstaller_Windows_Hub1_2019-05-02T19:28:14.000Z.zip",
    jobID: 1 // The job id which was triggered when making the POST
}
```

/api/v1/boarding/agentInstaller/*{filename}*

Use this REST API to download a specific Lenovo Universal Device Client (UDC) agent installation package to the local system. This UDC agent must be installed on ThinkEdge Client devices so that the devices can be securely discovered and managed by a Lenovo XClarity Management Hub resource manager.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

HTTP methods

GET

GET /api/v1/boarding/agentInstaller/*{filename}*

Use this method to download a specific Lenovo Universal Device Client (UDC) agent installation package to the local system. This UDC agent must be installed on ThinkEdge Client devices so that the devices can be securely discovered and managed by a Lenovo XClarity Management Hub resource manager.

To create a UDC-agent-installation package for a specific device, use POST /api/v1/boarding/agentInstaller.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/boarding/agentInstaller/*{filename}*

where *{filename}* is the filename of the management-agent installer. The file name is returned in the response body when you create the installer using POST /api/v1/boarding/agentInstaller.

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.

Response body

Attributes	Type	Description
{message_attributes}	varies	Status messages (see Status messages)

/api/v1/boarding/devices

Use this REST API to return a list of all discovered (but not managed) Lenovo devices with or without baseboard management controllers.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

HTTP methods

GET

GET /api/v1/boarding/devices

Use this method to return a list of all discovered (but not managed) Lenovo devices with or without baseboard management controllers.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/boarding/devices

Query parameters

This REST API supports query parameters for paginating, filtering, sorting, including data, and excluding data in the response. For more information about these common query parameters, see Paginating, scoping, filtering, sorting, including data, and excluding data in responses. For a list of supported attributes, see GET /api/v1/boarding/devices/*{id}*.

The following example return a list of all discovered Lenovo devices.
GET https://192.0.2.0/api/v1/boarding/devices

The following example return a list of all discovered Lenovo servers
GET https://192.0.2.0/api/v1/boarding/devices
?filterContains[0][attributes]=type&filterContains[0][values]=server

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.
206	Partial Content	Partial content was returned for a multi-part response. The response header includes a content-range header field indicating the range that is included in the response body for each part.
400	Bad Request	A query parameter 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.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes			Type	Description
results			Array of objects	Information about each discovered device
	id		String	Device ID **Tip:** The device ID is made up of the UUID of the device and the UUID of the resource manager that manages the device, separated by a dash.
	deviceName		String	Device name
	discoveredBy		Array of objects	Information about each resource manager that discovered this device
		id	String	Manager ID
		name	String	Manager name
		uri	String	Manager URI
	ipv4Addresses		Array of strings	List of IPv4 addresses that are assigned to this device
	ipv6Addresses		Array of strings	List of IPv6 addresses that are assigned to this device
	jobId		Integer	ID of the job through which this device was discovered
	name		String	Name that is displayed in the user interface for this device
	overallHealthState		String	Highest severity of all devices (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**

Attributes	Type	Description
powerStatus	String	Power status (translated). This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
productName	String	Product name
uuid	String	Device UUID
_links	Array of objects	User URI (see Links)
_metadata	Object	Request metadata (see Metadata)

The following example is returned if the request is successful.
```
{
    "results": [{
        "id": "ABC31213310B11EAAC96A252EC8212C0-1CB64754EA1543E0AAAA46C1D45CD549",
        "deviceName": "Steel-AMD-53-125",
        "discoveredBy": [{
            "id": "1CB64754EA1543E0AAAA46C1D45CD549",
            "name": "10.241.54.149",
            "uri": "/api/v1/managers-management/managers/1CB64754EA1543E0AAAA46C1D45CD549"
        }],
        "ipv4Addresses": ["10.241.53.125"],
        "ipv6Addresses": ["fd55:faaf:e1ab:21bb::125","fe80::a94:efff:feaa:9393"],
        "jobId": 29,
        "name": "Steel-AMD-53-125",
        "overallHealthState": "Unknown",
        "powerStatus": "Off",
        "productName": null,
        "uuid": "ABC31213310B11EAAC96A252EC8212C0"
        "_links": [{
            "rel": "self",
            "uri": "/api/v1/boarding/devices/ABC31213310B11EAAC96A252EC8212C0-1CB64754EA1543E0AAAA46C1D45CD549"
        }]
    "_metadata": {…}
}
```

/api/v1/boarding/devices/*{id}*

Use this REST API to return information about a specific discovered (but not managed) Lenovo device with or without baseboard management controllers.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

HTTP methods

GET

GET /api/v1/boarding/devices/*{id}*

Use this method to return information about a specific discovered (but not managed) Lenovo device with or without baseboard management controllers.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/boarding/devices/{id}`

where *{id}* is the ID of the discovered device. To obtain the discovered device IDs, use GET /api/v1/boarding/ devices.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.
206	Partial Content	Partial content was returned for a multi-part response. The response header includes a content-range header field indicating the range that is included in the response body for each part.
400	Bad Request	A query parameter 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.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
id	String	Device ID **Tip:** The device ID is made up of the UUID of the device and the UUID of the resource manager that manages the device, separated by a dash.
accessState	String	Access state of the device (translated). This can be one of the following values. • **Online** • **Offline** • **Offline Managed** • **Partial** • **Pending** • **Unknown**

Attributes	Type	Description
accurateHealth	Boolean	Indicates whether the health status is accurate. This can be one of the following values. • **true**. The accessState is Offline Managed, Online, or partial. • **false**. The acccessState is Offline, Pending, or Unknown.
canisters	Array of objects	(Storage devices only) Information about each canister in the device
id	String	Canister ID
cmmDisplayName	String	Chassis name
cmmHealthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
cmms	Array of objects	(Chassis only) Information about each CMM
accessState	String	Access state (translated) of the chassis. This can be one of the following values. • **Online** • **Offline** • **Offline Managed** • **Partial** • **Pending** • **Unknown**
accessStateKey	String	Access state key of the chassis. This can be one of the following values. • **Online** • **Offline** • **Offline Managed** • **Partial** • **Pending** • **Unknown**
accurateHealth	Boolean	Indicates whether the health status is accurate. This can be one of the following values. • **true**. The accessState is Offline Managed, Online, or partial. • **false**. The acccessState is Offline, Pending, or 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.
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** • **Warning** • **Critical** • **Unknown**

Attributes		Type	Description
dataHandle		Long	Time stamp of the last status update
description		String	Description that was provided by the CMM
deviceTypeKey		String	
domainName		String	User-defined domain name
dnsHostnames		Array of strings	
errorFields		Array of objects	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** • **Warning** • **Critical** • **Unknown**
firmware		Array of objects	Information about CMM firmware
	build	String	Firmware build
	classifications	Array of integers	Firmware type codes
	date	String	Firmware date
	name	String	Firmware name
	deviceTypeKey	String	
	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	CMM FRU part number
fruSerialNumber		String	CMM FRU serial number
hostConfig		Array of objects	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 of objects	Information about each IP interface
	IPv4assignments		Array of objects	Information about each IPv4 assignment
		id	Integer	IPv4 assignment ID
		address	String	IPv4 address
		deviceTypeKey	String	
		gateway	String	IPv4 gateway
		subnet	String	IPv4 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**
	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 assignment

Attributes			Type	Description
		id	Integer	IPv6 assignment ID
		address	String	IPv6 address
		gateway	String	IPv6 gateway
		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
leds			Array of objects	Information about server LEDs

Attributes			Type	Description
	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**
macAddresses			Array of strings	List of MAC addresses
machineType			String	Server machine type
manufacturer			String	Manufacturer
manufacturerId			String	Manufacturer ID
mgmtProcIPaddress			String	IP address used by XClarity Orchestrator to manage this resource
model			String	CMM model
name			String	Name that is displayed in the user interface for this device
overallHealthState			String	Highest severity of all alerts. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
overallHealthStateKey			String	Highest severity key. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
parent			Object	Information about the parent device
	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

Attributes	Type	Description
powerStatus	String	
powerStatusKey	String	
productId	String	CMM product ID
role	String	Role of the CMM. This can be one of the following values. • **primary** • **backup**
serialNumber	String	CMM serial number
slots	Array of integers	CMM primary slot
type	String	Resource type. This value is always **CMM**.
userDefinedName	String	User-defined name for the device
userDescription	String	Description that was defined by the user
uri	String	CMM URI
uuid	String	CMM UUID
deviceInfo	Object	Information about the device
domainName	String	Domain name
entitleSerialNumber	String	Entitled serial number
groups	Array of strings	List of IDs for groups that include this device
id	String	Groups ID
name	String	Group name
type	String	Group type
uri	String	Group URI
healthStatus	String	Highest severity of all alerts (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
hostname	String	Hostname
ipv4Addresses	Array of strings	List of IPv4 addresses
ipv6Addresses	Array of strings	List of IPV6 addresses
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

Attributes			Type	Description
machineType			String	Machine type
model			String	Device model
powerStatus			String	Power status (translated). This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
productName			String	Product name
serialNumber			String	Device serial number
userDefinedName			String	User-defined name for the device
uuid			String	Device UUID
_ui			Object	Information about web-interface-specific attributes.
	healthStatusKey		String	Severity key of the highest severity of all devices. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
	powerStatusKey		String	Power status key. This can be one of the following values: • **off** • **on** • **standby** • **unknown**
deviceName			String	Device name
deviceType			String	Device name
discoveredBy			Array of objects	Information about each resource manager that discovered this device
id			String	Manager ID
name			String	Manager name
uri			String	Manager URI
displayName			String	Display name
driveBays			String	Domain name
drives			Integer	Number of drive bays
bay			Integer	Drive bay
blockSize			Integer	Block size
capacity			Long	Drive capacity
description			String	Description
diskState			String	Disk-drive state
firmware			Array of objects	Information about add-in card firmware
	build		String	Firmware build

Attributes			Type	Description
		classifications	Array of integers	Firmware type codes
		date	String	Firmware date
		name	String	Firmware name
		deviceTypeKey	String	
		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	Highest severity of all alerts. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
	healthStateKey		String	Highest severity key. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
	interfaceType		String	(ThinkServer servers only) Drive interface type
	largestAvailableSize		Integer	
	m2Location		String	(M.2 drives only) Location of M.2 drive and bay
	manufacturer		String	Manufacturer
	mediaType		String	Media type
	model		String	Model
	name		String	Drive name
	numberOfBlocks		Integer	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**. Percent of remaining life • **-1**. Unknown (default) • **-2**. Information is not available • **-3**. The drive is not an SSD

Attributes	Type	Description
serialNumber	String	Serial number
temperature	String	Device temperature
uuid	String	Storage device UUID
drivesInstalled	Integer	(Storage devices only) Number of installed drives
enclosureFormFactor	String	Form factor of the chassis. This can be one of the following values. • **dense-computing** • **edge-computing** • **rack-tower**
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 of objects	Information about each firmware
build	String	Firmware build
date	String	Firmware date
version	String	Firmware version
fruNumber	String	Device FRU number
groups	Array of objects	Information about each group that include this device
id	String	Group ID
name	String	Group name
uri	String	Group URI
hostname	String	Hostname
ipv4Addresses	Array of strings	List of IPv4 addresses that are assigned to this device
ipv6Addresses	Array of strings	List of IPv6 addresses that are assigned to this device
isEmbeddedisEmbedded	Boolean	
jobId	Integer	ID of the job through which this device was discovered
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

Attributes	Type	Description
machineType	String	Device machine type
managementProcessor	String	Management controller type. This can be one of the following values. • **integrated-management-module** • **integrated-management-module2** • **lenovo-xclarity-controller** • **chassis-management-module**
manufacturer	String	Manufacturer
mgmtProcType	String	Type of management controller. This can be one of the following values. • **FSP** • **IMM2** • **XCC** • **XCC2** • **XCC3** • **UNKNOWN**
model	String	Device model
mtm	String	Device machine type and model, separate by a forward slash (for example, 8387/AC1
name	String	Name that is displayed in the user interface for this device
overallHealthState	String	Highest severity of all devices (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
powerStatus	String	Power status (translated). This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
powerSupplies	Array of objects	(Rack servers only) Information about power supplies
cmmDisplayName	String	Assigned component name
cmmHealthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
dataHandle	Long	Time stamp of the last status update
description	String	Assigned component description
deviceTypeKey	String	
excludedHealthState	String	Highest severity alert with exclusions. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
firmware	Array of objects	Information about firmware

Attributes			Type	Description
		build	String	Firmware build
		classifications	Array of integers	Firmware type codes
		date	String	Firmware date
		deviceTypeKey	String	
		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 part number
	fruSerialNumber		String	FRU serial number
	hardwareRevision		String	Hardware revision
	healthState		String	Health state (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
	healthStateKey		String	Health state key. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
	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 power-supply LEDs.

Attributes			Type	Description
	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
manufacturer			String	Manufacturer name
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				Highest severity of all power supplies(translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
overallHealthStateKey				Highest severity key. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
parent			Object	Information about the parent device, if applicable
	uri		String	Parent URI
	uuid		String	Parent UUID
partNumber			String	Part number
posID			String	Position ID
powerAllocation			Object	Information about the power allocation

Attributes		Type	Description
	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	Power-supply primary slot
	type	String	Resource type. This value is always **PowerSupply**
	uri	String	URI
	userDescription	String	User description
	uuid	String	UUID
	vpdID	String	VPD ID
productName		String	Product name
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.
	publicAccess	Boolean	Indicates whether the device can be accessed by all role groups. This can be one of the following values. • **true**. The resource can be access by all role group. • **false**. The resource is restricted to specific role groups.

Attributes			Type	Description
roleGroups			Array of strings	List of role groups that are permitted to view and manage this device
storedCredentials			object	Information about the stored credential that is associated with this device, if applicable
	id		String	Description of the stored credential
	description		String	ID of the stored credential
	userName		String	Name of the stored credential
	uri		String	URI of the device
serialNumber			String	Device serial number
server-type			String	Server type. This can be one of the following values. • **ITE**. Flex System server • **DenseChassis** • **Edge Server**. ThinkSystem SE server • **NeXtScale**. NeXtScale server • **Rack-Tower Server**. ThinkAgile, ThinkSystem SD, ThinkSystem SR, ThinkSystem ST , Converged, System x
status			Object	Information about management status
name			String	Status. This is always **UNMANAGED**.
message			String	Status message. This is always **Unmanaged**.
systemBoard			Object	Information about the system board
machineType			String	Device machine type
model			String	Device model
productName			String	Product name
serialNumber			String	Device serial number
uuid			String	Device UUID
type			String	Resource type (translated). This can be one of the following values. • **chassis** • **server** • **storage** • **switch**
userDefinedName			String	User-defined name for the device
uuid			String	Device UUID
_id			String	Device internal ID
_links			Object	Devices URI (see Links)
_rawDeviceData			Object	Raw data about the device data from the resource manager
_ui			Object	Information about web-interface-specific attributes

Attributes	Type	Description
overallHealthStateKey	String	Severity key of the highest severity of all devices. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
powerStatusKey	String	Power status key. This can be one of the following values. • **off** • **on** • **standby** • **unknown**

The following example is returned if the request is successful.

```
{
   "id": "ABC31213310B11EAAC96A252EC8212C0-1CB64754EA1543E0AAAA46C1D45CD549",
   "accurateHealth": true,
   "deviceInfo": {
      "domainName": null,
      "entitleSerialNumber": null,
      "healthStatus": "Unknown",
      "hostname": "XCC-SR665",
      "ipv4Addresses": ["10.241.53.125"],
      "ipv6Addresses": ["fd55:faaf:e1ab:21bb::125","fe80::a94:efff:feaa:9393"],
      "location": null,
      "machineType": "7D2W",
      "model": "RCZ000",
      "powerStatus": "Off",
      "productName": null,
      "serialNumber": "1234567890",
      "userDefinedName": null,
      "uuid": "ABC31213310B11EAAC96A252EC8212C0",
      "_ui": {
         "powerStatusKey": "Off",
         "healthStatusKey": "Unknown"
      }
   },
   "deviceName": "Steel-AMD-53-125",
   "discoveredBy": [{
      "id": "1CB64754EA1543E0AAAA46C1D45CD549",
      "name": "10.241.54.149",
      "uri": "/api/v1/managers-management/managers/1CB64754EA1543E0AAAA46C1D45CD549"
   }],
   "displayName": "Steel-AMD-53-125",
   "enclosureFormFactor": "rack-tower",
   "firmware": [],
   "fruNumber": "02YE183",
   "groups": [],
   "hostname": "XCC-SR665",
   "ipv4Addresses": ["10.241.53.125"],
   "ipv6Addresses": ["fd55:faaf:e1ab:21bb::125","fe80::a94:efff:feaa:9393"],
   "jobId": 29,
   "model": "RCZ000",
   "machineType": "7D2W",
   "managementProcessor": "lenovo-xclarity-controller",
   "mtm": "7D2W/RCZ000",
   "name": "Steel-AMD-53-125",
   "overallHealthState": "Unknown",
   "powerStatus": "Off",
```

```
   "productName": null,
   "serialNumber": "1234567890",
   "server-type": "Rack-Tower Server",
   "systemBoard": {
       "machineType": "7D2W",
       "model": "RCZ000",
       "productName": null,
       "serialNumber": "1234567890",
       "uuid": "ABC31213310B11EAAC96A252EC8212C0"
   },
   "type": "server",
   "uuid": "ABC31213310B11EAAC96A252EC8212C0",
   "_id": "62c6e4632d1860bf666e12c6",
   "_links": {
       "rel": "self",
       "uri": "/api/v1/boarding/devices/ABC31213310B11EAAC96A252EC8212C0-1CB64754EA1543E0AAAA46C1D45CD549"
   }
}
"_rawDeviceData": {
   "displayName": "Steel-AMD-53-125",
   "enclosureFormFactor": "rack-tower",
   "firmware": [{
       "build": "D8BT37L",
       "date": "2022-04-20",
       "version": "4.10"
   },
   {
       "build": "D8E101P",
       "date": "2019-12-26",
       "version": "1.00"
   }],
   "fruNumber": "02YE183",
   "hostname": "XCC-SR665",
   "ipAddresses": ["10.241.53.125","fd55:faaf:e1ab:21bb::125","fe80::a94:efff:feaa:9393"],
   "machineType": "7D2W",
   "managementPorts": [{
       "enabled": false,
       "port": 5988,
       "protocol": "cimxml-http"
   },
   ...,
   {
       "enabled": true,
       "port": 443,
       "protocol": "https"
   }],
   "managementProcessor": "lenovo-xclarity-controller",
   "model": "RCZ000",
   "name": "Steel-AMD-53-125",
   "securityDescriptor": {
       "managedAuthEnabled": true,
       "managedAuthSupported": true,
       "publicAccess": false,
       "roleGroups": [],
       "uri": "nodes/ABC31213310B11EAAC96A252EC8212C0"
   },
   "serialNumber": "1234567890",
   "server-type": "Rack-Tower Server",
   "status": {
       "manageable": true,
       "message": "Unmanaged",
       "name": "UNMANAGED"
```

```
        },
        "subType": "",
        "type": "server",
        "uuid": "ABC31213310B11EAAC96A252EC8212C0"
    },
    "_ui": {
        "overallHealthStateKey": "Unknown",
        "powerStatusKey": "Off"
    }
}
```

/api/v1/boarding/discovery

Use this REST API to directly discovers manageable Lenovo devices with or without baseboard management controllers.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

HTTP methods

GET

POST /api/v1/boarding/discovery

Use this method to directly discover manageable Lenovo devices with or without baseboard management controllers by specifying an individual IP addresses or hostname, range of IP addresses, or subnet.

An asynchronous job is created to complete this request. The response header returns the job URI and job ID.

A successful response code indicates that the job was successfully transmitted and accepted by the hub. 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 Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{orchestrator_server_IP}*/api/v1/boarding/discovery

Query parameters

None

Request body

Attributes		Re-quired / Optional	Type	Description
hosts		Optional	Array of objects	Information about individual IP addresses or fully-qualified domain name
	host	Required	String	IPv4 address, IPv6 address, or fully-qualified domain name
	managerID	Required	String	Resource manager ID

Attributes	Required / Optional	Type	Description
ranges	Optional	Array of objects	Information about each range of IP addresses
start	Required	String	First IPv4 or IPV6 address in the range
end	Required	String	Last IPv4 or IPV6 address in the range
managerID	Required	String	Resource manager ID
subnets	Optional	Array of objects	Information about each subnet
ipAddress	Required	String	IPv4 or IPV6 address
mask	Required	String	Subnet mask (for IPv4) or a routing prefix length (for IPv6)
managerID	Required	String	Resource manager ID

The following example discovers devices using individual IP address, individual hostname, range of IP addresses, and subset.

```
{
    "hosts": [{
        "host": "10.241.54.10",
        "managerID": "48331a223bf34fba90732b379b837b9c"
    },
    {
        "host": "id-lxc.labs.lenovo.com",
        "managerID": "48331a223bf34fba90732b379b837b9c"
    }],
    "ranges": [{
        "start": "10.241.54.10",
        "end": "10.241.54.15",
        "managerID": "48331a223bf34fba90732b379b837b9c"
    }],
    "subnets": [{
    {
        "ipAddress": "10.241.55.15",
        "mask": "255.255.255.0",
        "managerID": "48331a223bf34fba90732b379b837b9c"
    }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter 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.

Response header

The URI and ID of the root job are returned in the **Location** and **JobID** fields respectively.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

/api/v1/boarding/discoverySettings

Use this REST API to return or modify the discovery settings.

HTTP methods

GET, PUT

GET /api/v1/boarding/discoverySettings

Use this method to return the discovery settings.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/boarding/discoverySettings`

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).

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**. (default) Automatic discovery using SLP is enabled.XClarity Orchestrator attempts to discover new devices every 15 minutes and at every user login. • **false**. Automatic discovery using SLP is disabled.
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 Orchestrator communicates with the device (through the resource manager) 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 the resource manager that was chosen to manage the device. **Attention:** If encapsulation is enabled and the resource manager that was chosen to manage the device becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. • **false**. (default) 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.
offlineDevicesCleanup	Boolean	Indicates whether Lenovo XClarity Orchestrator automatically unmanages devices that are offline for a specific amount of time. This can be one of the following values. • **true**. Enables automatic unmanagement of offline devices.XClarity Orchestrator checks for offline devices every hour. If a device is offline for at least the amount of time specified by **offlineDevicesTimeout**, XClarity Orchestrator automatically unmanages that device. • **false**. (default) Disables automatic unmanagement of offline devices.
offlineDevicesTimeout	Boolean	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.
registerRequestEnabled	Boolean	Indicates whether Lenovo XClarity Administrator resource managers accept discovery requests from a baseboard management controller when the management controller uses DNS to find Lenovo XClarity Administrator instances. • **true**. (default) Management controller can register with Lenovo XClarity Administrator instances as a discovered device. • **false**. Management controller cannot register with Lenovo XClarity Administrator instances as a discovered device.
_links	Object	Resource URI (see Links)

The following example is returned if the request is successful.

```
{
    "autoDiscoveryEnabled": true,
    "offlineDevicesCleanup": true,
```

```
    "offlineDevicesTimeout": 24,
    "encapsulationEnabled": true,
    "registerRequestEnabled": true,
    "_links": {
        "rel": "self",
        "uri": "/api/v1/boarding/discoverySettings"
    }
}
```

PUT /api/v1/boarding/discoverySettings

Use this method to modify the discovery settings.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

PUT https://*{orchestrator_server_IP}*/api/v1/boarding/discoverySettings

Query parameters

None

Request body

This PUT request updates the entire resource. To clear a value, set the attribute to null (if applicable). If an array is specified, the entire array is replaced (unless stated otherwise). If an optional attribute is not specified, that attribute is not changed. If an immutable (unchangeable) attribute is specified, it is ignored.

Attributes	Required / Optional	Type	Description
autoDiscoveryEnabled	Optional	Boolean	Indicates whether you can automatically discover baseboard management controllers using the SLP discovery method. This can be one of the following values. • **true**. (default) Automatic discovery using SLP is enabled.XClarity Orchestrator attempts to discover new devices every 15 minutes and at every user login. • **false**. Automatic discovery using SLP is disabled. **Note:** The SLP Discovery setting that you choose in XClarity Orchestrator overrides any SLP discovery setting chosen for Lenovo XClarity Administrator instances that are managed by XClarity Orchestrator. If the SLP Discovery setting is changed in Lenovo XClarity Administrator, it will be synchronized with XClarity Orchestrator.
offlineDevicesCleanup	Optional	Boolean	Indicates whether Lenovo XClarity Orchestrator automatically unmanages devices that are offline for a specific amount of time. This can be one of the following values. • **true**. Enables automatic unmanagement of offline devices.XClarity Orchestrator checks for offline devices every hour. If a device is offline for at least the amount of time specified by **offlineDevicesTimeout**, XClarity Orchestrator automatically unmanages that device. • **false**. (default) Disables automatic unmanagement of offline devices.
offlineDevicesTimeout	Optional	Boolean	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.

Attributes	Required / Optional	Type	Description
encapsulationEnabled	Optional	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 Orchestrator communicates with the device (through the resource manager) 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 the resource manager that was chosen to manage the device. **Attention:** If encapsulation is enabled and the resource manager that was chosen to manage the device becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. • **false**. (default) 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.
registerRequestEnabled	Optional	Boolean	Indicates whether Lenovo XClarity Administrator resource managers accept discovery requests from a baseboard management controller when the management controller uses DNS to find Lenovo XClarity Administrator instances. • **true**. (default) Management controller can register with Lenovo XClarity Administrator instances as a discovered device. • **false**. Management controller cannot register with Lenovo XClarity Administrator instances as a discovered device.

The following example modifies the discovery settings.

```
{
    "autoDiscoveryEnabled": true,
    "offlineDevicesCleanup": true,
    "offlineDevicesTimeout": 24,
    "encapsulationEnabled": true,
    "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.

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.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

/api/v1/boarding/management

Use this REST API to directly manage or unmanage Lenovo devices with or without baseboard management controllers.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

HTTP methods

POST, DELETE

POST /api/v1/boarding/management

Use this method to directly manage discovered devices with or without baseboard management controllers.

When you manage a chassis, all devices in the chassis are managed. You cannot manage individual devices in a chassis.

Attention: Before managing a device, the devices must have been previously discovered using the POST /api/v1/boarding/discovery method.

An asynchronous job is created to complete this request. The response header returns the job URI and job ID.

A successful response code indicates that the job was successfully transmitted and accepted by the hub. 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 Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{orchestrator_server_IP}*/api/v1/boarding/management

Query parameters

None

Request body

Table 1. Manage discovered devices

Attributes			Re-quired / Optional	Type	Description
chassis			Optional	Object	Information about the chassis to be managed
	config		Required	Object	Information about chassis configuration
		forceManage	Optional	Boolean	Indicates whether to force management of the chassis. This can be one of the following values. • **true**. Force management. • **false**. (default) Do not force management. **Note:** Use the 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. **Notes:** • If the managing resource manager failed and cannot be recovered.If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the Force management option. • If the managing resource manager was taken down before the devices were unmanaged. • If the devices were not unmanaged successfully. **Attention:** Devices can be managed by only one resource manager at a time. Management by multiple resource manager is not supported. If a device is managed by one resource manager, and you want to manage it with another resource manager, you must first unmanage the device from the original resource manager, and then manage it with the new resource manager.
		newPassword	Optional	String	New password to be used for managed authentication
		password	Required	String	Current password to access the chassis
		recoveryPassword	Required	String	Recovery password to be used for the chassis
		username	Required	String	User ID to be used to access the chassis
	ids		Optional	Array of strings	List of IDs of chassis to be managed
		managerId	Optional	String	Manager identifier
		resourceId	Optional	String	Resource identifier
servers			Optional	Object	Information about the servers to be managed
	config		Required	Object	Information about server configuration

Table 1. Manage discovered devices (continued)

Attributes			Re-quired / Optional	Type	Description
		forceManage	Optional	Boolean	Indicates whether to force management of the servers. This can be one of the following values. • **true**. Force management. • **false**. (default) Do not force management. **Attention:** Use the 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. **Attention:** • If the managing resource manager failed and cannot be recovered.If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the Force management option. • If the managing resource manager was taken down before the devices were unmanaged. • If the devices were not unmanaged successfully. **Attention:** Devices can be managed by only one resource manager at a time. Management by multiple resource manager is not supported. If a device is managed by one resource manager, and you want to manage it with another resource manager, you must first unmanage the device from the original resource manager, and then manage it with the new resource manager.
		newPassword	Optional	String	New password to be used for managed authentication
		password	Required	String	Current password to access the servers
		recoveryPassword	Optional	String	Recovery password to be used for the servers
		username	Required	String	User ID to be used to access the servers
	ids		Optional	Array of strings	List of IDs of servers to be managed
		managerId	Optional	String	Manager identifier
		resourceId	Optional	String	Resource identifier
storage			Optional	Object	Information about the storage devices to be managed
	config		Required	Object	Information about storage-device configuration

Table 1. Manage discovered devices (continued)

Attributes			Re-quired / Optional	Type	Description
		forceManage	Optional	Boolean	Indicates whether to force management of the storage device. This can be one of the following values. • **true**. Force management. • **false**. (default) Do not force management. **Attention:** Use the 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. **Attention:** • If the managing resource manager failed and cannot be recovered.If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the Force management option. • If the managing resource manager was taken down before the devices were unmanaged. • If the devices were not unmanaged successfully. **Attention:** Devices can be managed by only one resource manager at a time. Management by multiple resource manager is not supported. If a device is managed by one resource manager, and you want to manage it with another resource manager, you must first unmanage the device from the original resource manager, and then manage it with the new resource manager.
		password	Required	String	Current password to access the storage device
		username	Required	String	User ID to be used to access the storage device
	ids		Optional	Array of strings	List of IDs of storage devices to be managed
		managerId	Optional	String	Manager identifier
		resourceId	Optional	String	Resource identifier

The following example manages multiple devices.

```
{
    "chassis": {
        "config": {
            "forceManage": false,
            "newPassword": "*************",
            "password": "*************",",
            "recoveryPassword": "*************",
            "username": " User1"
        },
        "ids": [
            {
                "managerId":"823CC2575E0DABAAC6C1D45CD2221CB87",
                "resourceId":"FBB43C13D103511E785F2E4A2CED78753"
            }
        ],
```

```
    },
    "servers": {
       "config": {
          "forceManage": false,
          "newPassword": "*************",
          "password": "************",
          "recoveryPassword": "*************",
          "username": "User1"
       },
       "ids": [
             {
                "managerId":"1CB64754EA1543E0AAAA46C1D45CD549",
                "resourceId":"3015DE7E2B6011E881940A94EF5F5B65"
             }
       ],
    }
    "storage": {
          "forceManage": false,
          "password": "************",
          "username": "User1"
       },
       "ids": [
             {
                "managerId":"754EA1543E0BDACCB6C1D45CD5491CB6",
                "resourceId":"2376F7C628FB11E1B72B5CF3fC3C1448"
             }
       ],
    }
}
```

Table 2. Manage and discover servers in bulk

Attributes		Re-quired / Optional	Type	Description
managerID		Required	String	ID of the resource manager to use to manage servers in bulk
servers		Required	Object	Information about the servers to be managed
	config	Required	Object	Information about server configuration

Table 2. Manage and discover servers in bulk (continued)

Attributes			Re-quired / Optional	Type	Description
		forceManage	Optional	Boolean	Indicates whether to force management of the servers. This can be one of the following values. • **true**. Force management. • **false**. (default) Do not force management. **Attention:** Use the 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. **Attention:** • If the managing resource manager failed and cannot be recovered.If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the Force management option. • If the managing resource manager was taken down before the devices were unmanaged. • If the devices were not unmanaged successfully. **Attention:** Devices can be managed by only one resource manager at a time. Management by multiple resource manager is not supported. If a device is managed by one resource manager, and you want to manage it with another resource manager, you must first unmanage the device from the original resource manager, and then manage it with the new resource manager.
		ipAddresses	Required	Array of strings	List of IP addresses for servers that you want to manage in bulk
		newPassword	Optional	String	New password to be used for managed authentication
		password	Required	String	Current password to access the servers
		recoveryPassword	Optional	String	Recovery password to be used for the servers
		username	Required	String	User ID to be used to access the servers

The following example manages and discovers devices in bulk.
```
{
   "managerID": "F95463A1A4AB4187A76553F0E2B1DEB2",
   "servers": {
      "config": {
         "forceManage": true,
         "ipAddresses": ["192.02.7", "192.0.2.8"],
         "newPassword": "Func2test",
         "password": "Func2test",
         "recoveryPassword": "Func2test",
         "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.
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.

Response header

The URI and ID of the root job are returned in the **Location** and **JobID** fields respectively.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

DELETE /api/v1/boarding/management

Use this method to unmanage devices.

When you unmanage a chassis, all devices in the chassis are unmanaged. You cannot unmanage individual devices in a chassis.

An asynchronous job is created to complete this request. The response header returns the job URI and job ID.

A successful response code indicates that the job was successfully transmitted and accepted by the hub. 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 Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

DELETE https://*{orchestrator_server_IP}*/api/v1/boarding/management

Query parameters

Parameters	Re- quired / Optional	Description
ids=*{uuids}*	Required	List of UUIDs of devices to be unmanaged, separated by a comma
force=*{Boolean}*	Optional	Indicates whether to force the unmanagement operation. This can be one of the following values. • **true**. Force unmanagment even if the device is not reachable. • **false**. (default) Do not force unmanagement.

The following example unmanages multiple devices without force.
DELETE https://*{management_server_IP}*/api/v1/boarding/management
?ids=fbb43c13103511e785f2e4a2ced78753,48331a223bf34fba90732b379b837b9c

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.
400	Bad Request	A query parameter 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.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

/api/v1/boarding/managementSettings

Use this REST API to retrieve and save the UDS Portal credentials, to return the credentials, or to delete the credentials.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

HTTP methods

GET, PUT, DELETE

GET /api/v1/boarding/managementSettings

Use this method to return the UDS Portal credentials.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/boarding/managementSettings

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
udsClientId	String	Client ID If the client ID is not saved, this value is null.
udsClientSecret	Boolean	Indicates whether the secret exists. This can be one of the following values. • **true**. The client secret exists. • **false**. The client secret does not exist.

The following example is returned if the request is successful.
```
{
    udsClientId: "EDGE-ISG-BridgeAccount",
    udsClientSecret: "true"
}
```

PUT /api/v1/boarding/managementSettings

Use this method to retrieve and verify the UDS Portal credentials, and then save the credentials in the vault.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

PUT https://*{orchestrator_server_IP}*/api/v1/boarding/managementSettings

Query parameters

None

Request body

Attributes	Re- quired / Optional	Type	Description
udsClientId	Required	String	Client ID
udsClientSecret	Required	String	Client secret

The following example retrieves and saves the UDS Portal credentials.
```
{
```

```
    udsClientId: "EDGE-ISG-BridgeAccount",
    udsClientSecret: "rbDeFXO5ll3SmEh4yR7OqhTzO7W1m6M7"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

DELETE /api/v1/boarding/managementSettings

Use this method to delete the stored UDS Portal credentials.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

DELETE https://*{orchestrator_server_IP}*/api/v1/boarding/managementSettings

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

/api/v1/connector/managers

Use this REST API to return a list of all resource managers, connect resource managers, or update credentials for one or more resource managers.

Attention: This REST API will be deprecated in a future release.

HTTP methods

GET, POST, PUT

GET /api/v1/connector/managers

Use this method to return a list of all resource managers.

Attention: This REST API will be deprecated in a future release. Use GET /api/v1/managers-management/ managers instead.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/connector/managers`

Query parameters

This REST API supports query parameters for paginating, scoping, filtering, sorting, including data, and excluding data in the response. For more information about these common query parameters, see Paginating, scoping, filtering, sorting, including data, and excluding data in responses. For a list of supported attributes, see GET /api/v1/connector/managers/*{id}*.

The following example returns a list of all resource managers.
`GET https://192.0.2.0/api/v1/connector/managers`

The following example returns a list of all unhealthy resource managers.
`GET https://192.0.2.0/api/v1/connector/managers`
`?filterNotEquals[][attributes]=healthState&filterNotEquals[][values]=Normal`

The following example returns a list of all resource managers running version 1.0.
`GET https://192.0.2.0/api/v1/connector/managers`
`?filterEquals[][attributes]=updateMetadata.components.version.number&filterEquals[][values]=1.0`

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.
206	Partial Content	Partial content was returned for a multi-part response. The response header includes a content-range header field indicating the range that is included in the response body for each part.
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

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes		Type	Description
results		Array of objects	Information about each resource manager
	id	String	Resource manager ID
	connectTimestamp	String	Timestamp when the resource manager was registered with XClarity Orchestrator 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.
	healthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
	healthStateKey	String	Health state key. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
	name	String	Resource manager name **Note:** For Lenovo XClarity Administrator, this is the IP address of the management server.
	type	String	Type of resource manager. This can be one of the following values. • **XClarity Management Hub 2.0** • **XClarity Management Hub** • **XClarity Administrator** • **XClarity Orchestrator** • **Schneider EcoStruxure IT** • **VMware vRealize Operations Manager**
	_links	String	Resource manager URI (see Links)
_metadata		Object	Request metadata (see Metadata)

The following example is returned if the request is successful.

```
{
   "results": [{
      "id": "00000000000000000000000000000000",
      "healthState": "Normal",
      "healthStateKey": "Normal",
      "name": "XClarity Orchestrator",
      "type": "XClarity Orchestrator",
      "_links": {
```

```
            "rel": "self",
            "uri": "/api/v1/connector/managers/00000000000000000000000000000000"
        }
    },
    {
        "id": "23C87F0A2CB64910974889193447A655C",
        "connectTimestamp": "2022-04-25T15:13:43.833Z",
        "healthState": "Normal",
        "healthStateKey": "Normal",
        "name": "xhmc194.labs.lenovo.com",
        "type": "XClarity Administrator",
        "_links": {
            "rel": "self",
            "uri": "/api/v1/connector/managers/23C87F0A2CB64910974889193447A655C"
        }
    }],
    "_metadata": {…}
}
```

POST /api/v1/connector/managers

Use this method to connect (register) one or more resource managers.

Attention: This REST API will be deprecated in a future release. Use POST /api/v1/managers-management/ managers instead.

An asynchronous job is created to complete this request. The response header returns the job URI and job ID.

A successful response code indicates that the job was successfully transmitted and accepted by the hub. 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.

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

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{orchestrator_server_IP}*/api/v1/connector/managers

Query parameters

None

Request body

Table 3. **XClarity Management Hub 2.0 and** *Lenovo XClarity Administrator resource managers*

Attributes			Re-quired / Optional	Type	Description
managers			Required	Array of objects	Information about each resource manager
	authentication		Required	Object	Information about authentication settings
		password	Required	String	Password to use for basic authentication

Table 3. XClarity Management Hub 2.0 and Lenovo XClarity Administrator resource managers (continued)

Attributes			Re-quired / Optional	Type	Description
		type	Required	String	Authentication type. This is always **basic**.
		username	Required	String	username to use for basic authentication
	connection		Required	Object	Information about connection settings
		hostname	Required	String	Resource manager host name
		port	Required	Integer	Resource manager port
	options		Required	Object	Information about options
		enableDriveAnalyticsData	Required	Boolean	Indicates whether drive analytics data collection is enabled. This can be one of the following values. • **true**. Drive analytics data collection is enabled. • **false**. Drive analytics data collection is disabled. **Note:** This attribute is supported by XClarity Administrator v3.3 and later.
	type		Required	String	Type of resource manager. This is always **XClarity Administrator**.

Table 4. Schneider Electric EcoStruxure IT Expert resource managers

Attributes			Re-quired / Optional	Type	Description
managers			Required	Array of objects	Information about each resource manager
	authentication		Required	Object	Information about authentication settings
		token	Required	String	Token value
		type	Required	String	Authentication type. This is always **token**.
	connection		Optional	Object	Information about connection settings
		url	Optional	String	Resource manager URL
	name		Required	String	Resource manager name
	type		Required	String	Type of resource manager. This is always **Schneider EcoStruxure IT**.

Table 5. VMware vRealize Operations Manager resource managers

Attributes			Re-quired / Optional	Type	Description
managers			Required	Array of objects	Information about each resource manager
	authentication		Required	Object	Information about authentication settings
		password	Required	String	Password to use for basic authentication
		username	Required	String	Username to use for basic authentication

Attributes		Re-quired / Optional	Type	Description
authSource		Optional	String	Name of the authentication source for users and groups To obtain a list of available authorization sources, use GET /api/v1/connector/vrealizeAuthSources.
connection		Required	Object	Information about connection settings
	hostname	Required	String	Resource manager host name
	port	Required	Integer	Resource manager port
type		Required	String	Type of resource manager. This is always **vRealize Operations Manager**

The following example connects to XClarity Administrator and vRealize Operations Manager resource manager.

```
{
    "managers": [{
        "authentication": {
            "password": "CME44len",
            "type": "basic",
            "username": "USERID"
        },
        "connection": {
            "hostname": "192.0.1.102",
            "port": 443
        },
        "options": {
            "enableDriveAnalyticsData": true
        },
        "type": "XClarity Administrator"
    },
    {
        "authentication": {
            "token": "AK1/2sixskmmc06wj/1i6v3epcz5c25rc29jv1tOOhce1pjahyobux63 ",
            "type": "token"
        },
        "connection": {
            "url": "https://api.ecostruxureit.com/rest/v1/organizations"
        },
        "name": "Croco 1",
        "type": "Schneider EcoStruxure IT"
    },
    {
        "authentication": {
            "password": "********",
            "username": "USERID"
        },
        "authSource": "All vCenter Servers",
        "connection": {
            "hostname": "192.0.1.103",
            "port": 443
        },
        "type": "vRealize Operations Manager"
    }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter 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.

Response header

The URI and ID of the root job are returned in the **Location** and **JobID** fields respectively.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

/api/v1/connector/managers/*{id}*

Use this REST API to return information about, modify, or disconnect a specific resources manager.

Attention: This REST API will be deprecated in a future release.

HTTP methods

GET, PATCH, DELETE

GET /api/v1/connector/managers/*{id}*

Use this method to return information about a specific resource manager.

Attention: This REST API will be deprecated in a future release. Use GET /api/v1/managers-management/managers/*{id}* instead.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/connector/managers/{id}`

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.

Response body

The returned attributes vary depending on the type of resource manager.
- Lenovo XClarity Orchestrator resource managers
- XClarity Management Hub 2.0 and Lenovo XClarity Administrator resource managers
- Schneider Electric EcoStruxure IT Expert resource managers
- VMware vRealize Operations Manager resource managers

Table 6. Lenovo XClarity Orchestrator resource managers

Attributes	Type	Description
id	String	Resource manager ID
connectDate	String	Timestamp when the resource manager was registered with XClarity Orchestrator 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.
connection	Object	Information about connection settings
hostname	String	Resource manager host name
port	Integer	Resource manager port
details	Object	Information about the resource manager properties
build	String	Resource manager build number
buildNumber	String	Resource manager build number
uuid	String	Resource manager UUID
version	String	Resource manager version
versionNumber	String	Resource manager version number
groups	Array of object	Information about each group in which this resource manager is a member
id	String	Group ID
name	String	Group name
type	String	Group type. This value is always **ManagerGroup**.
uri	String	Group URI

Table 6. Lenovo XClarity Orchestrator resource managers (continued)

Attributes	Type	Description
healthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
healthStateKey	String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
issues	Array of strings	Reason for an unhealthy status If **healthState** is **Normal**, this attribute is set to null. If **healthState** is not **Normal**, this attribute can be one of the following values. • **InvalidCredentials** • **ConnectionProblems**
lastInventorySyncTimestamp	String	Timestamp when XClarity Orchestrator last refreshed the inventory for the resource manager 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.
lastSyncDate	String	Timestamp when XClarity Orchestrator last refreshed the information about the resource manager 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.
name	String	Resource manager name
type	String	Type of resource manager. This is always XClarity Orchestrator.
_links	Object	Resource manager URI (see Links)

The following example is returned if the request is successful for XClarity Orchestrator.

```
{
    "id": "00000000000000000000000000000000",
    "connectDate": null,
    "connection": null,
    "details": {
        "build": "186",
        "buildNumber": 186,
        "uuid": "21A727A22EECA0B85DCE38F16C7CEB1F",
        "version": "1.6.0",
        "versionNumber": 160
    },
    "groups": [],
    "healthState": "Normal",
    "healthStateKey": "Normal",
```

```
      "issues": [],
      "lastInventorySyncDate": null,
      "lastSyncDate": null,
      "name": "XClarity Orchestrator",
      "type": "XClarity Orchestrator",
      "_links": {
         "rel": "self",
         "uri": "/api/v1/connector/managers/00000000000000000000000000000000"
      }
}
```

Table 7. **XClarity Management Hub 2.0 and** *Lenovo XClarity Administrator resource managers*

Attributes	Type	Description
id	String	Resource manager ID
connectTimestamp	String	Timestamp when the resource manager was registered with XClarity Orchestrator 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.
connection	Object	Information about connection settings
hostname	String	Resource manager host name
port	Integer	Resource manager port
details	Object	Information about the resource manager properties
build	String	Resource manager build number
buildNumber	String	Resource manager build number
forwarderID	String	ID of the event forwarder in XClarity Administrator that pushes events to this XClarity Orchestrator instance
metricsSubscriptionID	String	ID of the metrics subscription in XClarity Administrator that pushes metrics to this XClarity Orchestrator instance
networkSettings	Object	Information about network settings for the resource manager
domainName	String	Domain
hostname	String	Host name
ipv4Addresses	Array of strings	List of IPv4 addresses
ipv6Addresses	Array of strings	List of IPv6 addresses
uuid	String	Resource manager UUID
version	String	Resource manager version
versionNumber	String	Resource manager version number
groups	Array of object	Information about each group in which this resource manager is a member
id	String	Group ID
name	String	Group name
type	String	Group type. This value is always **ManagerGroup**.

Table 7. XClarity Management Hub 2.0 and Lenovo XClarity Administrator resource managers (continued)

Attributes	Type	Description
uri	String	Group URI
healthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
healthStateKey	String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
issues	Array of strings	Reason for an unhealthy status If **healthState** is **Normal**, this attribute is set to null. If **healthState** is not **Normal**, this attribute can be one of the following values. • **InvalidCredentials** • **ConnectionProblems**
lastInventorySyncTimestamp	String	Timestamp when XClarity Orchestrator last refreshed the inventory for the resource manager 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.
lastSyncTimestamp	String	Timestamp when XClarity Orchestrator last refreshed the information about the resource manager 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.
name	String	Resource manager name
options	Object	Information about options
enableDriveAnalyticsData	Boolean	Indicates whether drive analytics-data collection is enabled. This can be one of the following values. • **true**. Drive analytics data collection is enabled. • **false**. Drive analytics data collection is disabled.
type	String	Type of resource manager. This is always XClarity Administrator.
updates	Object	(XClarity Administrator and EcoStruxure IT Expert only) Information about the update history for the resource manager
identifier	String	Update ID
components	Array of objects	Information about each update component
componentID	String	Component ID

Table 7. XClarity Management Hub 2.0 and Lenovo XClarity Administrator resource managers (continued)

Attributes				Type	Description
		name		String	Component name
		targetVersion		Object	Information about the target update for the component based on the assigned policy If a policy is not assigned, this value is null.
			identifier	String	Version ID
			number	String	Version number
			releaseTimestamp	String	Timestamp when the version was released 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.
		upgradeable		Boolean	Indicates whether the component can be updated. This can be one of the following values. • **true**. The component can be updated. • **false**. The component cannot be updated.
		version		Object	Information about the update that is currently installed for the component
			identifier	String	Version ID
			number	String	Version number
			releaseTimestamp	String	Timestamp when the version was released 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.
	policy			Object	Information about the update-compliance policy that is assigned to this device If a policy is not assigned, this value is null.
		id		String	Policy ID
		name		String	Policy name
	policyState			String	Policy state (translated). This can be one of the following values. • **No Policy Assigned** • **Policy Assigned**
	policyStateKey			String	Policy state key. This can be one of the following values. • **No Policy Assigned** • **Policy Assigned**
_links				Object	Resource manager URI (see Links)

The following example is returned if the request is successful for XClarity Administrator.

```
{
   "id": "23C87F0A2CB64910974891934447A655C",
   "connectTimestamp": "2022-04-25T15:13:43.833Z",
   "connection": {
      "hostname": "10.243.2.107",
      "port": 443
   },
   "details": {
      "build": "41",
      "buildNumber": 41,
```

```
        "forwarderID": "1650899611143",
        "metricsSubscriptionID": "6266baa3fac263b8917b9181",
        "networkSettings": {
            "domainName": "labs.lenovo.com",
            "hostname": "xhmc194",
            "ipv4Addresses": ["10.243.2.107"],
            "ipv6Addresses": ["fd55:faaf:e1ab:2021:5054:ff:fec4:df97","fe80:0:0:0:5054:ff:fec4:df97"]
        },
        "uuid": "23C87F0A2CB6491097489193447A655C",
        "version": "3.6.0",
        "versionNumber": 360
    },
    "groups": [],
    "healthState": "Normal",
    "healthStateKey": "Normal",
    "issues": [],
    "lastInventorySyncTimestamp": "2022-04-25T15:14:33.480Z",
    "lastSyncTimestamp": "2022-04-25T15:13:43.833Z",
    "name": "xhmc194.labs.lenovo.com",
    "options": {
        "enableDriveAnalyticsData": true
    },
    "type": "XClarity Administrator",
    "updates": {
        "identifier": "lxca",
        "components": [{
            "componentID": "lxca",
            "name": "Lenovo XClarity Administrator 3.6.0",
            "targetVersion": null,
            "upgradeable": true,
            "version": {
                "identifier": "41",
                "number": "3.6.0",
                "releaseTimestamp": null
            }
        }],
        "policy": {
            "id": null,
            "name": "No Assignment"
        },
        "policyState": "No Policy Assigned",
        "policyStateKey": "NoPolicyAssigned",
    },
    "_links": {
        "rel": "self",
        "uri": "/api/v1/connector/managers/23C87F0A2CB6491097489193447A655C"
    }
}
```

Table 8. Schneider Electric EcoStruxure IT Expert resource managers

Attributes	Type	Description
id	String	Resource manager ID
connectTimestamp	String	Timestamp when the resource manager was registered with XClarity Orchestrator 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.

Attributes	Type	Description
connection	Object	Information about connection settings
url	String	Resource manager URL
details	Object	Information about the resource manager properties
build	String	Resource manager build number
uuid	String	Resource manager UUID
version	String	Resource manager version
versionNumber	String	Resource manager version number
groups	Array of object	Information about each group in which this resource manager is a member
id	String	Group ID
name	String	Group name
type	String	Group type. This value is always **ManagerGroup**.
uri	String	Group URI
healthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
healthStateKey	String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
issues	Array of strings	Reason for an unhealthy status If **healthState** is **Normal**, this attribute is set to null. If **healthState** is not **Normal**, this attribute can be one of the following values. • **InvalidCredentials** • **ConnectionProblems**
lastInventorySyncTimestamp	String	Timestamp when XClarity Orchestrator last refreshed the inventory for the resource manager 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.
lastSyncTimestamp	String	Timestamp when XClarity Orchestrator last refreshed the information about the resource manager 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.

Table 8. Schneider Electric EcoStruxure IT Expert resource managers (continued)

Attributes			Type	Description
name			String	Resource manager name
type			String	Type of resource manager. This is always Schneider EcoStruxure IT.
updates			Object	Information about the update history for the resource manager
	identifier		String	Update ID
	components		Array of objects	Information about each update component
		componentID	String	Component ID
		name	String	Component name
		targetVersion	Object	Information about the target update for the component based on the assigned policy If a policy is not assigned, this value is null.
		identifier	String	Version ID
		number	String	Version number
		releaseTimestamp	String	Timestamp when the version was released 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.
		upgradeable	Boolean	Indicates whether the component can be updated. This can be one of the following values. • **true**. The component can be updated. • **false**. The component cannot be updated.
		version	Object	Information about the update that is currently installed for the component
		identifier	String	Version ID
		number	String	Version number
		releaseTimestamp	String	Timestamp when the version was released 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.
	policy		Object	Information about the update-compliance policy that is assigned to this device If a policy is not assigned, this value is null.
		id	String	Policy ID
		name	String	Policy name
	policyState		String	Policy state (translated). This can be one of the following values. • **No Policy Assigned** • **Policy Assigned**
	policyStateKey		String	Policy state key. This can be one of the following values. • **No Policy Assigned** • **Policy Assigned**
_links			Object	Resource manager URI (see Links)

The following example is returned if the request is successful for an Schneider Electric EcoStruxure IT Expert.

```
{
    "id": "b17c3accec1e2a94e28b108ed757a6705c77066d",
    "connectTimestamp": "2021-02-16T12:36:40.809Z",
    "connection": {
        "url": "https://api.ecostruxureit.com/rest/v1/organizations"
    },
    "details": {
        "build": null,
        "uuid": null,
        "version": null,
        "versionNumber": null
    },
    "groups": [],
    "healthState": "Normal",
    "healthStateKey": "Normal",
    "issues": [],
    "lastInventorySyncTimestamp": null,
    "lastSyncTimestamp": "2021-02-16T12:36:40.809Z",
    "name": "Demo Ecox manager1",
    "type": "Schneider EcoStruxure IT",
    "updates": null,
    "_links": {
        "rel": "self",
        "uri": "/api/v1/connector/managers/b17c3accec1e2a94e28b108ed757a6705c77066d"
    }
}
```

Table 9. VMware vRealize Operations Manager resource managers

Attributes	Type	Description
id	String	Resource manager ID
authSource	String	Name of the authentication source for users and groups
connectTimestamp	String	Timestamp when the resource manager was registered with XClarity Orchestrator 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.
connection	Object	Information about connection settings
hostname	String	Resource manager host name
port	Integer	Resource manager port
details	Object	Information about the resource manager properties
build	String	Resource manager build number
uuid	String	Resource manager UUID
version	String	Resource manager version
versionNumber	String	Resource manager version number
groups	Array of object	Information about each group in which this resource manager is a member
id	String	Group ID

Table 9. VMware vRealize Operations Manager resource managers (continued)

Attributes		Type	Description
	name	String	Group name
	type	String	Group type. This value is always **ManagerGroup**.
	uri	String	Group URI
healthState		String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
healthStateKey		String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
issues		Array of strings	Reason for an unhealthy status If **healthState** is **Normal**, this attribute is set to null. If **healthState** is not **Normal**, this attribute can be one of the following values. • **InvalidCredentials** • **ConnectionProblems**
lastInventorySyncTimestamp		String	Timestamp when XClarity Orchestrator last refreshed the inventory for the resource manager 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.
lastSyncTimestamp		String	Timestamp when XClarity Orchestrator last refreshed the information about the resource manager 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.
name		String	Resource manager name
type		String	Type of resource manager. This is always VMware vRealize Operations Manager.
_links		Object	Resource manager URI (see Links)

The following example is returned if the request is successful for a VMware vRealize Operations Manager.

```
{
   "id": "b17c3accec1e2a94e28b108ed757a6705c77066d",

   "authSource": "",
   "connectTimestamp": null,
   "connection": {
      "hostname": "10.243.2.107",
      "port": 443
```

```
    },
    "details": {
        "build": "41",
        "uuid": "21A727A22EECA0B85DCE38F16C7CEB1F",
        "version": "1.4.0",
        "versionNumber": 140
    },
    "groups": [],
    "healthState": "Normal",
    "healthStateKey": "Normal",
    "issues": [],
    "lastInventorySyncDate": null,
    "lastSyncTimestamp": null,
    "name": "vRO",
    "type": "VMware vRealize Operations Manager",
    "_links": {
        "rel": "self",
        "uri": "/api/v1/connector/managers/b17c3accec1e2a94e28b108ed757a6705c77066d"
    }
}
```

PATCH /api/v1/connector/managers/*{id}*

Use this method to modify authentication and connection settings for a resource manager.

Attention: This REST API will be deprecated in a future release.

Note: This REST API requires Lenovo XClarity Orchestrator v1.2 or later.

Authentication

Authentication with username and password is required.

Resource URI

PATCH `https://`*{orchestrator_server_IP}*`/api/v1/connector/managers/`*{id}*

where *{id}* is the ID of the resource manager. To obtain the resource manager IDs, use GET /api/v1/ connector/managers.

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
op	Required	String	Action to take. This can be the following value. • **replace**. Replaces the entire attribute value with the specified value.
path	Required	String	Name of the attribute to be modified. This can be one of the following values. • **authentication**. Modifies authentication settings. • **connection**. Modifies connection settings. • **options.enableDriveAnalyticsData**. Enables or disables drive analytics-data collection for resource managers.
value	Required	String	Attribute value, depending on the data type

The following example modifies the authentication and connection settings for an XClarity Administrator resource manager.

```
[
   { "op": "replace", "path": "authentication", "value": { "username": "USERID",
                                                           "password": "CME44len",
                                                           "type": "basic"}
   },
   { "op": "replace", "path": "connection", "value": { "hostname": "10.241.54.113",
                                                       "port": 443 }
   },
   { "op": "replace", "path": "options.enableDriveAnalyticsData", "value": 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	The resource cannot be found. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

DELETE /api/v1/connector/managers/*{id}*

Use this method to disconnect (remove) a specific resource manager.

Attention: This REST API will be deprecated in a future release. Use DELETE /api/v1/managers-management/managers/*{id}* instead.

An asynchronous job is created to complete this request. The response header returns the job URI and job ID.

A successful response code indicates that the job was successfully transmitted and accepted by the hub. 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.

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

Authentication
Authentication with username and password is required.

Resource URI
DELETE `https://{orchestrator_server_IP}/api/v1/connector/managers/{id}`

where *{id}* is the ID of the resource manager. To obtain the resource manager IDs, use GET /api/v1/connector/managers.

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	The resource cannot be found. 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** and **JobID** fields respectively.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

/api/v1/connector/vrealizeAuthSources

Use this REST API to return a list of authorization sources for a specific VMware vRealize Operations Manager resource manager.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

HTTP methods
GET

GET /api/v1/connector/vrealizeAuthSources

Use this method to return a list of authorization sources for a specific VMware vRealize Operations Manager resource manager.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/connector/vrealizeAuthSources

Query parameters

Parameters	Re-quired / Optional	Description
ipAddress=*{ipAddress}*	Required	IP address of the vRealize Operations Manager resource manager

The following example returns the authorization sources for a specific vRealize Operations Manager resource manager.

GET https://192.0.2.0/api/v1/connector/vrealizeAuthSources?ipAddress=192.0.2.0

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. 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).

Attributes	Type	Description
authSources	Array of strings	List of names of authorization sources
_links	Object	Resource URI (see Links)

The following example is returned if the request is successful.

```
{
   "authSources": ["All vCenter Servers", "vcenter-1975"],
   "_links": {
      "rel": "self",
      "uri": "/api/v1/connector/vrealizeAuthSources
   }
}
```

/api/v1/data/deviceInfo

Use this REST API to return general information about a specific device.

HTTP methods

GET

GET /api/v1/data/deviceInfo?deviceID=*{id}*

Use this method to return general information about a specific device.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/data/deviceInfo?deviceID={id}`

Query parameters

Parameters	Re-quired / Optional	Description
deviceID=*{id}*	Required	Returns general information about a device, specified by the ID To obtain the device IDs, use GET /api/v1/data/devices

The following example returns general information about a specific device.
```
GET https://192.0.2.0/api/v1/data/deviceInfo?deviceID=
3015DE7E2B6011E881940A94EF5F5B65-C7199530FEDE4FE09540DFC3D75FC56C
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a query parameter is specified and the value of that parameter has no matches, the response body returns default values.
400	Bad Request	A query parameter 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	The resource cannot be found. 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).

Attributes	Type	Description
domainName	String	Domain name
entitleSerialNumber	String	Entitled serial number

Attributes	Type	Description
groupNames	Array of strings	List of names of the groups to which the device belongs
healthStatus	String	Health state of the device (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
healthStatusKey	String	Health state key. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
hostname	String	Hostname
ipv4Addresses	Array of strings	List of IPv4 addresses
ipv6Addresses	Array of strings	List of IPv6 addresses
location	Object	Information about the location of the device
location	String	Location description
lowestRackUnit	String	Lowest rack unit
rack	String	Rack name
room	String	Room name
machineType	String	Device machine type
manager	Object	Information about the resource manager that manages this device
domainName	String	Fully qualified domain name
fqdn	String	Full-qualified domain name
hostname	String	Host name
inContextHref	String	In context URI
ipv4Addresses	Array of strings	IPv4 addresses
ipv6Addresses	Array of strings	IPv6 addresses
model	String	Device model
patternComplianceStatus	String	Sever-configuration pattern compliance status (translated). This can be one of the following values. • **Compliant** • **Failed Deployment** • **No Pattern Assigned** • **Not Compliant** • **Pending Compliance Check** • **Pending Deployment** • **Pending Restart**

Attributes	Type	Description
patternComplianceStatusKey	String	Sever-configuration pattern compliance status key. This can be one of the following values. • **Compliant** • **FailedDeployment** • **NoPatternAssigned** • **NotCompliant** • **PpendingComplianceCheck** • **PendingDeployment** • **PendingRestart**
patternID	String	Sever-configuration pattern ID
patternName	String	Sever-configuration pattern name If a pattern is not assigned, this value is **No Assignment**.
powerStatus	String	Power status (translated). This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
powerStatusKey	String	Power status key. This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
productName	String	Device product name
serialNumber	String	Device serial number
userDefinedName	String	User-defined name for the device
uuid	String	Device UUID
_links	Object	Device URI (see Links)

The following example is returned if the request is successful.

```
{
    "domainName": "labs.lenovo.com",
    "entitleSerialNumber": null,
    "groupNames": [],
    "healthStatus": "Warning",
    "healthStatusKey": "Warning",
    "hostname": "XCC-7Y02-0123456789",
    "ipv4Addresses": ["10.243.0.235","169.254.95.118"],
    "ipv6Addresses": ["fd55:faaf:e1ab:2021:a94:efff:fe4f:5635","fe80::a94:efff:fe4f:5635"],
    "location": {
        "location": "elephante",
        "lowestRackUnit": 33,
        "rack": "Snufflaluffagus",
        "room": "pacaderm"
    },
    "machineType": "7Y02",
    "manager": {
        "domainName": "",
        "fqdn": null,
        "hostname": "localhost",
        "inContextHref": "/ui/index.html#/compDetails/Rack-Tower Server/8151C5148B4411E791329DD935F1CD89/",
        "ipv4Addresses": ["10.243.17.164"],
        "ipv6Addresses": ["0::0","fe80:0:0:0:215:5dff:fe0c:d156"]
```

```
  },
  "model": "RCZ000",
  "patternComplianceStatus": "No Pattern Assigned",
  "patternComplianceStatusKey": "NoPatternAssigned",
  "patternID": null,
  "patternName": "No Assignment",
  "powerStatus": "On",
  "powerStatusKey": "On",
  "productName": "ThinkSystem SR570",
  "serialNumber": "0123456789",
  "userDefinedName": "",
  "uuid": "8151C5148B4411E791329DD935F1CD89",
  "_links": {
      "rel": "self",
      "uri": "/api/v1/data/devices/C7199530FEDE4FE09540DFC3D75FC56C"
  }
}
```

/api/v1/data/devices

Use this REST API to return a list of all managed devices.

HTTP methods

GET

GET /api/v1/data/devices

Use this method to return a list of all managed devices.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/data/devices

Query parameters

This REST API supports query parameters for paginating, scoping, filtering, sorting, including data, and excluding data in the response. For more information about these common query parameters, see Paginating, scoping, filtering, sorting, including data, and excluding data in responses. For a list of supported attributes, see GET /api/v1/data/devices/*{id}*.

The following example returns a list of all managed devices.
GET https://192.0.2.0/api/v1/data/devices

The following example returns a list of all devices that are managed by a specific resource manager.
GET https://192.0.2.0/api/v1/data/devices
?filterEquals[][attributes]=lxcaUUID&filterEquals[][values]=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

The following example returns a list of all managed IBM servers and includes the manufacturer in the response.
GET https://192.0.2.0/api/v1/data/devices
?filterContains[0][attributes]=typeKey&filterContains[0][values]=server
&filterEquals[1][attributes]=manufacturer&filterEquals[1][values]=IBM
&includeAttributes=id,deviceName,ipv4Addresses,ipv6Addresses,lxcaUUID,productName,manufacturer

The following example returns a list of all managed servers.

```
GET https://192.0.2.0/api/v1/data/devices
?filterContains[0][attributes]=typeKey&filterContains[0][values]=server
```

The following example returns a list of all managed ThinkSystem servers.
```
GET https://192.0.2.0/api/v1/data/devices
?filterContains[0][attributes]=typeKey&filterContains[0][values]=server
&filterContains[1][attributes]=productName&filterContains[1][values]=ThinkSystem
```

The following example returns a list of all managed chassis.
```
GET https://192.0.2.0/api/v1/data/devices
?filterContains[][attributes]=typeKey&filterContains[][values]=chassis
```

The following example returns a list of all managed storage devices.
```
GET https://192.0.2.0/api/v1/data/devices
?filterContains[][attributes]=typeKey&filterContains[][values]=storage
```

The following example returns a list of all managed switches.
```
GET https://192.0.2.0/api/v1/data/devices
?filterContains[][attributes]=typeKey&filterContains[][values]=switch
```

The following example returns warranty information for all devices in a specific group with expired warranties.
```
GET https://192.0.2.0/api/v1/data/devices
?filterContains[1][attributes]=statusKey&filterContains[1][values]=Expired
&groupIDs=G_136FAA46D0754FE5B5A493F454EC5551
&includeAttributes=id,name,machineType,model,serialNumber,warranty
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.
206	Partial Content	Partial content was returned for a multi-part response. The response header includes a content-range header field indicating the range that is included in the response body for each part.
400	Bad Request	A query parameter 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.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes		Type	Description
results		Array of objects	Information about each managed device
	id	String	Device ID **Tip:** The device ID includes the UUID of the device and the UUID of the resource manager that manages the device, separated by a dash (*deviceUUID–managerUUID*).
	deviceName	String	Name that is displayed in the user interface for this device
	ipv4Addresses	Array of strings	List of IPv4 addresses
	ipv6Addresses	Array of strings	List of IPV6 addresses
	lxcaUUID	String	Resource manager UUID
	name	String	Device name
	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**
	powerStatus	String	Power status. This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
	productName	String	Product name
	_links	String	Device URI (see Links)
_metadata		Object	Request metadata (see Metadata)

The following example is returned if the request is successful.

```
{
    "results": [{
        "id": "00632D78DE644E23B712E200FE449787-7AF5D198CECF431AAEC674C7CA5A29B5",
        "deviceName": "Kong-SB",
        "ipv4Addresses": ["10.243.0.165"],
        "ipv6Addresses": ["fe80::e61f:13ff:fed9:367d"],
        "lxcaUUID": "7AF5D198CECF431AAEC674C7CA5A29B5",
        "name": "Kong-SB",
        "overallHealthState": "Normal",
        "powerStatus": "On",
        "productName": "System x3750 M4",
        "_links": {
            "rel": "self",
            "uri": "/api/v1/data/devices/00632D78DE644E23B712E200FE449787-7AF5D198CECF431AAEC674C7CA5A29B5"
        }
    }],
    "_metadata": {...}
}
```

/api/v1/data/devices/*{id}*

Use this REST API to return information about a specific managed device.

HTTP methods

GET

GET /api/v1/data/devices/*{id}*

Use this method to return information about a specific managed device.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/data/devices/{id}`

where *{id}* is the UUID or ID of the device. To obtain the device UUID and IDs, use GET /api/v1/data/devices.

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	The resource cannot be found. 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.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes	Type	Description
id	String	Device ID **Tip:** The device ID is made up of the UUID of the device and the UUID of the resource manager that manages the device, separated by a dash.
accessState	String	Access state of the device (translated). This can be one of the following values. • **Online** • **Offline** • **Offline Managed** • **Partial** • **Pending** • **Unknown**
accessStateKey	String	Access state of the server key. This can be one of the following values. • **Online** • **Offline** • **Offline Managed** • **Partial** • **Pending** • **Unknown**
accessStateRecords	Array of objects	Information about access state records
health	String	
ipAddress	String	
messageBundle	String	
messageDisplay	String	
messageID	String	
messageParameter	String	
protocol	String	
username	String	
timestamp	Long	
trusted	Boolean	
accountLockoutPeriod	Integer	
accurateHealth	Boolean	Indicates whether the health status is accurate. This can be one of the following values. • **true**. The **accessState** is Offline Managed, Online, or partial. • **false**. The **acccessState** is Offline, Pending, or Unknown.
activationKeys	Array of objects	List of installed Feature On Demand (FoD) keys
description	String	FoD key description
keyExpirationDate	String	Date when the FoD key expires
keyFeatureType	Integer	FoD feature type
keyIdentiferList	Array of objects	FoD associative identifier list

Attributes			Type	Description
	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 add-in cards **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.
	class		String	Class
	firmware		Array of objects	Information about add-in card firmware
		build	String	Firmware build
		classifications	Array of integers	Firmware type codes
		date	String	Firmware date
		deviceTypeKey	String	
		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

Attributes				Type	Description
fodUniqueID				String	FoD unique ID
FRU				String	Add-in card FRU part number
fruSerialNumber				String	
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 the physical port
		logicalPorts		Array of objects	List of associated logical ports
			addresses	Array of Strings	Assigned addresses
			logicalPortIndex	Integer	Number of logical ports

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**
				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
			portType		String	Physical port type. This can be one of the following values. • **ATM** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **OTHER** • **TOKENRING** • **UNKNOWN**
		speed			String	
		status			String	
	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	Slot number for the add-in card
agentVersion					String	(ThinkEdge Client devices only) Version of the UDC agent that is running on the device If set to null, the UDC agent agent is not installed.

Attributes	Type	Description
arch	String	Architecture. This can be one of the following values. • **ia64** • **ppc** • **ppc64** • **x86** • **x86_64** • **Unknown**
assetTag	String	(ThinkSystem rack servers only) Name or Tag that represents the server or other physical enclosure
attachedNodes	Array of objects	(Switches only)
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
bmuParamObject	String	
canisters	Array of objects	(Storage devices only) Information about each canister in the device
id	String	Canister ID
cmmDisplayName	String	(Chassis only) Chassis name
cmmHealthState	String	(Chassis only) Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
cmms	Array of objects	(Chassis only) Information about each CMM

Attributes	Type	Description
accessState	String	Access state (translated) of the chassis. This can be one of the following values. • **Online** • **Offline** • **Offline Managed** • **Partial** • **Pending** • **Unknown**
accessStateKey	String	Access state key of the chassis. This can be one of the following values. • **Online** • **Offline** • **Offline Managed** • **Partial** • **Pending** • **Unknown**
accurateHealth	Boolean	Indicates whether the health status is accurate. This can be one of the following values. • **true**. The **accessState** is Offline Managed, Online, or partial. • **false**. The **accessState** is Offline, Pending, or 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.
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** • **Warning** • **Critical** • **Unknown**
dataHandle	Long	Time stamp of the last status update
description	String	Description that was provided by the CMM
deviceTypeKey	String	
domainName	String	User-defined domain name
dnsHostnames	Array of strings	
errorFields	Array of objects	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** • **Warning** • **Critical** • **Unknown**

Attributes		Type	Description
firmware		Array of objects	Information about CMM firmware
	build	String	Firmware build
	classifications	Array of integers	Firmware type codes
	date	String	Firmware date
	name	String	Firmware name
	deviceTypeKey	String	
	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	Strin-Boo-leang	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	CMM FRU part number
fruSerialNumber		String	CMM FRU serial number
hostConfig		Array of objects	Information about host configuration
	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

Attributes			Type	Description
ipInterfaces			Array of objects	Information about each IP interface
	IPv4assignments		Array of objects	Information about each IPv4 assignment
		id	Integer	IPv4 assignment ID
		address	String	IPv4 address
		deviceTypeKey	String	
		gateway	String	IPv4 gateway
		subnet	String	IPv4 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**
	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 assignment
		id	Integer	IPv6 assignment ID
		address	String	IPv6 address
		gateway	String	IPv6 gateway
		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**

Attributes			Type	Description
		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
leds			Array of objects	Information about server 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**

Attributes	Type	Description
macAddresses	Array of strings	List of MAC addresses
machineType	String	Server machine type
manufacturer	String	Manufacturer
manufacturerId	String	Manufacturer ID
mgmtProcIPaddress	String	IP address used by XClarity Orchestrator to manage this resource
model	String	CMM model
name	String	Name that is displayed in the user interface for this device
overallHealthState	String	Highest severity of all alerts. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
overallHealthStateKey	String	Highest severity key. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
parent	Object	Information about the parent device
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
powerStatus	String	
powerStatusKey	String	
productId	String	CMM product ID
role	String	Role of the CMM. This can be one of the following values. • **primary** • **backup**
serialNumber	String	CMM serial number
slots	Array of integers	CMM primary slot
type	String	Resource type. This value is always **CMM**.
userDefinedName	String	User-defined name for the device
userDescription	String	Description that was defined by the user
uri	String	CMM URI
uuid	String	CMM UUID

Attributes	Type	Description
configCompliance	Array of objects	Information about the server-configuration compliance
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.
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
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.
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.
templateId	String	ID of the server pattern that was used to create the profile
type	String	Internal use only
contact	String	Contact (assigned in Lenovo XClarity Administrator)
contacts	Object	Information about support contacts for this device (assigned in XClarity Orchestrator)
primary	Object	Information about the primary contact
id	String	Contact ID
fullName	String	Contact name
companyName	String	Company name
contactEmail	String	Email address
contactPhone	String	Phone number
streetAddress	String	Street address
city	String	City
stateProvince	String	State or province
postalCode	String	Country or region
country	String	Postal code

Attributes			Type	Description
		preferredContactMethod	String	Preferred contact method. This can be one of the following values. • **any** • **phone** • **email**
		uri	String	Contact URI
	secondary		Array of strings	Information about each secondary contact
		id	String	Contact ID
		fullName	String	Contact name
		companyName	String	Company name
		contactEmail	String	Email address
		contactPhone	String	Phone number
		streetAddress	String	Street address
		city	String	City
		stateProvince	String	State or province
		postalCode	String	Country or region
		country	String	Postal code
		preferredContactMethod	String	Preferred contact method. This can be one of the following values. • **any** • **phone** • **email**
		uri	String	Contact URI
dataHandle			Long	Time stamp of the last status update
description			String	
deviceDrivers			Array of objects	Information about the device drivers
	displayName		String	Display name
	driverClass		String	Class
	driverClassId		String	Class ID
	driverFiles		Array of objects	Information about the device-driver files
		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

Attributes	Type	Description
releaseDate	String	Release date
version	String	Version
deviceInfo	Object	Information about the device
domainName	String	Domain name
entitleSerialNumber	String	Entitled serial number
groupNames	Array of strings	List of names for groups that include this device
healthStatus	String	Highest severity of all alerts (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
healthStatusKey	String	Severity key of highest severity of all alerts. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
hostname	String	Hostname
ipv4Addresses	Array of strings	List of IPv4 addresses
ipv6Addresses	Array of strings	List of IPV6 addresses
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
machineType	String	Machine type
manager	Object	Information about the resource manager that manages this device
id	String	Resource manager ID
domainName	String	Domain name
fqdn	String	Fully qualified domain name
hostname	String	Host name
inContextHref	String	In context URI
ipv4Addresses	Array of strings	IPv4 addresses
ipv6Addresses	Array of strings	IPv6 addresses

Attributes	Type	Description
model	String	Device model
powerStatus	String	Power status (translated). This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
powerStatusKey	String	Power status key. This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
productName	String	Product name
serialNumber	String	Device serial number
userDefinedName	String	User-defined name for the device
uuid	String	Device UUID
deviceName	String	Device name
deviceType	String	Device type (translated). This can be one of the following values. • **Chassis** • **Server** • **Storage** • **Switch**
deviceTypeKey	String	Device type key. This can be one of the following values. • **chassis** • **server** • **storage** • **switch**
discoveryTimestamp	String	Timestamp when the device was discovered 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.
diskDriveSensorInfo	Array of strings	List of hard-driver sensor names
dnsHostnames	Array of string	
domainName	String	Domain name
driveBays	Integer	Number of drive bays
drives	Array of objects	Drive details
bay	Integer	Drive bay
blockSize	Integer	Block size
capacity	Long	Drive capacity
description	String	Description
diskState	String	Disk-drive state

Attributes	Type	Description
encryptionStatus	String	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	Information about add-in card firmware
build	String	Firmware build
classifications	Array of integers	Firmware type codes
date	String	Firmware date
deviceTypeKey	String	Device type key
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	Health state (translated) that corresponds to the highest event severity of all disk drives in the device. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
healthStateKey	String	Health state key that corresponds to the highest event severity of all disk drives in the device. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
hotSpareType	String	Type of hot spare drive. This can be one of the following values. • **Global** • **None**
interfaceType	String	(ThinkServer servers only) Drive 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	Integer	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	String	Device temperature
uuid	String	Storage device UUID
drivesInstalled	Integer	(Storage devices only) Number of installed drives
encapsulation	Object	Information about encapsulation
encapsulationMode	String	Encapsulation (firewall settings) mode. This can be one of the following values. • **NOT_SUPPORTED**. Encapsulation is not supported for this device. • **NORMAL**. Encapsulation is disabled for this device.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. • **ENCAPSULATION_LIGHT**. Encapsulation is enabled for this device.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.
excludedHealthState	String	Highest severity alert with exclusions. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
expansionCards	Array of objects	Information about expansion cards
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 the physical ports
logicalPorts	Array of objects	List of associated logical ports
addresses	Array of Strings	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.
physicalPortIndex	Integer	Number of physical ports
portType	String	Physical port type. This can be one of the following values. • **ATM** • **ETHERNET** • **FC** • **FDDI** • **FRAMERELAY** • **IB** • **OTHER** • **TOKENRING** • **UNKNOWN**

Attributes			Type	Description
		portNumber	Integer	Number of the physical port
		peerBay	Integer	Peer I/O module bay
	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**
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**
fans			Array of objects	Information about each fan in the device
	description		String	Fan description
	healthState		String	Fan health state (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
	healthStateKey		String	Fan health state key. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
	name		String	Fan name
	slot		Integer	Fan slot
	slots		Integer	Fan slot
	speed		Integer	Fan speed
	status		String	Fan status
featuresOnDemand			Array of objects	Information about features on demand (FOD)
	features		Array of string	List of active features on demand

Attributes	Type	Description
tierLevel	Integer	(ThinkSystem only) Tier level of the Lenovo XClarity Controller feature key that is installed. This can be one of the following values. • **0**. • **1**. Lenovo XClarity Controller Standard • **2**. Lenovo XClarity Controller Advanced • **3**. Lenovo XClarity Controller Enterprise
firmware	Array of objects	Information about each firmware
build	String	Firmware build
classifications	Array	Firmware type codes
date	String	Firmware date
deviceTypeKey	String	
firmwareActivationStatus	String	
firmwareActivationStatusKey	String	
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**
type	String	Firmware type, such as UEFI, MP, or DSA
version	String	Firmware version
firmwareCompliance	Object	Information about the firmware compliance
status	String	Compliance status. This can be one of the following values. • **compliant**. The device is compliant with their server profile. • **notCompliant**. The device is not compliant with their server profile. • **noPolicyAssigned**. The device is not assigned a server profile. • **unsupportedCompliance**. Configuration is not supported for the device.
flashStorage	Array of objects	Information about flash storage
defaultBlockSize	Long	Flash storage device block size
description	String	Flash storage description
serialNumber	String	Flash storage serial number
firmware	Array of objects	Flash storage firmware properties
build	String	Firmware build

Attributes			Type	Description
		classifications	Array of integers	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 identifier
		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	
fruSerialNumber			String	
groups			Array of objects	Information about each group in which this device is a member
	id		String	Group ID
	name		String	Group name
	type		String	Group type. This value is always "DeviceGroup."
	uri		String	Group URI
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
hostname			String	Hostname
inProcessing			String	
ipInterfaces			Array of objects	Information about each IP interface

Attributes		Type	Description
IPv4assignments		Array of objects	Information about each IPv4 assignment
	id	Integer	IPv4 assignment ID
	address	String	IPv4 address
	deviceTypeKey	String	
	gateway	String	IPv4 gateway
	subnet	String	IPv4 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**
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 assignment
	id	Integer	IPv6 assignment ID
	address	String	IPv6 address
	deviceTypeKey	String	
	gateway	String	IPv6 gateway
	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**

Attributes	Type	Description
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
isEmbedded	Boolean	
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 not a compute node.
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	Indicates whether this is a scalable device. This can be one of the following values. • **true** • **false**
isITME	Boolean	Indicates whether this device is a compute node in a chassis. 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	Ethernet-over-USB port forwarding mode
deviceTypeKey	String	
externalIPAddress	String	IP address of the port

Attributes	Type	Description
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**
lastSyncTimestamp	String	Timestamp when this data was last refreshed from the resource manager 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.
lastUpdateTimestamp	String	Timestamp when this data was last updates from the resource manager 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.
leds	Array of objects	Information about server 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 location of the server or Flex System storage device
location	String	Location
lowestRackUnit	Integer	Lowest rack unit
rack	String	Rack
room	String	Room

Attributes	Type	Description
lxcaOverallHealthState	String	Resource manager health state. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
lxcaUUID	String	Resource manager UUID
m2Presence	Boolean	Indicates whether the device 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.
macAddresses	Array of strings	List of MAC addresses
machineType	String	Server machine type
manager	Object	Information about the resource manager that manages this device
id	String	Resource manager ID
domainName	String	Domain name
fqdn	String	Fully qualified domain name
groups	Array of objects	Information about groups in which the manager is a member
id	String	Group ID
name	String	Group name
type	String	Group type. This value is always **ManagerGroup**.
uri	String	Group URI
hostname	String	Host name
inContextHref	String	In context URI
ipv4Addresses	Array of strings	IPv4 addresses
ipv6Addresses	Array of strings	IPv6 addresses
uri	Array of strings	Resource manager URI
manufacturer	String	Manufacturer
manufacturerID	String	Manufacturer ID
memoryModules	Array of objects	Information about memory modules
capacity	Long	Capacity
deviceTypeKey	String	Device type key
displayName	String	Display name
fruPartNumber	String	FRU part number

Attributes	Type	Description
healthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
healthStateKey	String	Health state key. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
manufacturer	String	Manufacturer
metrics	Object	Information about memory metric data
alarmTrips	Object	Information about alarm trips
model	String	Model
operatingMemoryMode	Array of strings	
partNumber	String	Part number
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
mgmtProcIPaddress	String	IP address used by XClarity Orchestrator to manage this resource
mgmtProcType	String	Type of management controller. This can be one of the following values. • **FSP** • **IMM2** • **XCC** • **XCC2** • **XCC3** • **UNKNOWN**
model	String	Server model
mtm	String	Machine type and model, separate by a forward slash (for example, 8387/AC1)
name	String	Name that is displayed in the user interface for this device
onboardPciDevices	Array of objects	Information about onboard PCI device
class	String	Class
firmware	Array of objects	Information about add-in card firmware

Attributes		Type	Description
	build	String	Firmware build
	classifications	Array of integers	Firmware type codes
	date	String	Firmware date
	deviceTypeKey	String	
	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
	version	String	Firmware version
fodUniqueID		String	FoD unique ID
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.
name		String	Add-in card description
pciBusNumber		String	PCI bus number
pciDeviceNumber		String	PCI device number
pciFunctionNumber		String	PCI function number
pciRevision		String	PCI revision number
pciSegmentNumber		String	PCI segment number
pciSubID		String	PCI subsystem ID
pciSubVendorID		String	PCI subsystem ID
portInfo		Object	Information about the port

Attributes				Type	Description
	physicalPorts			Array of objects	Information about 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**
		portNumber		Integer	Number of the physical port
		logicalPorts		Array of objects	List of associated logical ports
			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
			addresses	Array of strings	Assigned addresses
			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
	posID			String	Device ID
	vpdID			String	VPD ID
osInfo				Object	Information about the operating system that is installed on the device
	description			String	Operating system name and version
	hostname			String	Hostname or IP address of the operating system
	os_country			String	(ThinkEdge Client devices only) Country where the operating system is installed
	os_language			String	(ThinkEdge Client devices only) Operating system language

Attributes	Type	Description
os_name	String	(ThinkEdge Client devices only) Operating system name
os_version	String	(ThinkEdge Client devices only) Operating system version
storedCredential	String	URI of the stored-credential account that is used to access the operating system (for example, storedCredentials/2653)
osProfiles	Object	Information about the operating-system profile for the server
applicableStatus	String	Profile status (translated). This can be one of the following values. • **Assigned**. An OS profile is assigned to this device. • **No Profile Assigned**. An OS profile is not assigned to this device.
applicableStatusKey	String	Profile status key. This can be one of the following values. • **assigned**. An OS profile is assigned to this device. • **noProfileAssigned**. An OS profile is not assigned to this device.
assigned	Object	Information about the assigned profile
id	String	Profile ID
name	String	Profile name
uri	String	Profile URI
deployStatus	String	OS profile deployment status (translated). This can be one of the following values.
deployStatusKey	String	OS profile deployment status key. This can be one of the following values.
overallHealthState	String	Highest severity of all events (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
overallHealthStateKey	String	Highest severity key. This can be one of the following values. • **normal** • **warning** • **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
partNumber	String	Part number
patterns	Object	Information about the sever-configuration pattern that is assigned to this device
assigned	Object	Information about the assigned pattern
id	String	Pattern ID
name	String	Pattern name

Attributes	Type	Description
complianceStatus	String	Compliance status (translated). This can be one of the following values. • **Compliant** • **Failed Deployment** • **No Pattern Assigned** • **Not Compliant** • **Pending Compliance Check** • **Pending Deployment** • **Pending Restart**
complianceStatusKey	String	Compliance status key. This can be one of the following values. • **Compliant** • **FailedDeployment** • **NoPatternAssigned** • **NotCompliant** • **PpendingComplianceCheck** • **PendingDeployment** • **PendingRestart**
pciDevices	Array of objects	Information about PCI devices
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	Flash storage firmware properties
build	String	Firmware build
classifications	Array of integers	Firmware type codes
date	String	Firmware date
deviceTypeKey	String	Device type key
name	String	Firmware name

Attributes			Type	Description
	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
fodUniqueID			String	FoD unique ID
FRU			String	Add-in card FRU part number
fruSerialNumber			String	Add-in card 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
pciSubID			String	PCI subsystem ID
pciSubVendorID			String	PCI sub-vendor ID
portInfo			Object	Information about the ports
	physicalPorts		Array of objects	Information about the physical ports
		logicalPorts	Array of objects	List of associated logical ports

Attributes					Type	Description
				addresses	Array of Strings	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
			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	Product name
	slotName				String	Slot name
	slotNumber				String	Slot number
	slotSupportsHotPlug				String	Indicates whether the slot is hot pluggable. This can be one of the following values. • **true** • **false**
	vpdID				String	VPD ID

Attributes	Type	Description
ports	Array of objects	Port information
ioModuleBay	Integer	Attached IO module bay number
portNumber	Integer	Port number
posID	String	Device 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
maximumPowerCappingHotPlugLevel	Long	Maximum power capping hot plug level
maxPowerCap	Long	Maximum power capping level
minimumHardCapLevel	Long	Minimum hard capping level
minimumPowerCappingHotPlugLevel	Long	Minimum power capping hot plug level
minPowerCap	Long	Minimum power capping level
powerCappingAllocUnit	String	Power capping allocation unit
powerStatus	String	Power status (translated). This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
powerStatusKey	String	Power status key. This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
powerSupplies	Array of objects	(Rack servers only) Information about power supplies
cmmDisplayName	String	Assigned component name
cmmHealthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**

Attributes		Type	Description
dataHandle		Long	Time stamp of the last status update
description		String	Assigned component description
deviceTypeKey		String	Device type key
excludedHealthState		String	Highest severity alert with exclusions. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
firmware		Array of objects	Information about firmware
	build	String	Firmware build
	classifications	Array of integers	Firmware type codes
	date	String	Firmware date
	deviceTypeKey	String	Device type key
	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
fruSerialNumber		String	FRU serial number
hardwareRevision		String	Hardware revision
healthState		String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**

Attributes	Type	Description
healthStateKey	String	Health state key. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
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 power-supply 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
manufactureDate	String	Manufacture date
manufacturer	String	Manufacturer name
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

Attributes	Type	Description
overallHealthState		Highest severity of all power supplies(translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
overallHealthStateKey		Highest severity key. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
parent	Object	Information about the parent device, if applicable
uri	String	Parent URI
uuid	String	Parent UUID
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**
powerStatus	String	Power status (translated). This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
powerStatusKey	String	Power status key. This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
productId	String	Product ID
productName	String	Product name
serialNumber	String	Serial number
slots	Array	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
primary	Boolean	
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
processors		Information about processors
cores	Integer	Number of cores
displayName	String	Display name
family	String	Family
healthState	String	Health state (translated)
healthStateKey	String	Health state key
manufacturer	String	Manufacturer
maxSpeedMHZ	Integer	Maximum processor speed
partNumber	String	Part number
present	Boolean	
productVersion	String	Product version
serialNumber	String	Serial number
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	
processorSlots	Integer	Number of processor slots
productId	String	Product ID
productName	String	Product name
protectedMode	String	
raidSettings	Array	Information about RAID devices
batteryData	Array	
description	String	RAID devices description
diskDrives	Array of objects	Information about disk drives
bay	Integer	Bay or slot number
blockSize	Long	Block size

Attributes			Type	Description
	capacity		Integer	(M.2 drives only) Storage capacity, in KB
	description		String	Description
	diskState		String	Disk-drive state
	encryptionStatus		String	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 firmware
		build	String	Firmware build.
		classifications	Array of integers	Firmware type codes
		date	String	Firmware date.
		deviceTypeKey	String	
		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	Health state (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
	healthStateKey		String	Health state key. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
	hotSpareType		String	Type of hot spare drive. This can be one of the following values. • **Global** • **None**
	interfaceType		String	Interface type

Attributes			Type	Description
		largestAvailableSize	Integer	Largest available size
		m2Location	String	(M.2 drives only) Location of M.2 drive and bay
		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**. Percent of remaining life • **-1**. Unknown (default) • **-2**. Information is not available • **-3**. Drive is not an SSD
		serialNumber	String	Serial number
		temperature	Integer	Device temperature
		uuid	String	UUID
	firmware		Array of objects	Information about firmware
		build	String	Firmware build
		classifications	Array of integers	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		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
	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	Model
	name		String	RAID devices name

Attributes				Type	Description
pciFirmware				Array of objects	
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	Storage array ID
	arrayStatus			String	Storage array status
	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	Bay
		blockSize		Integer	Block size
		capacity		Long	Storage capacity
		description		String	Drive description
		diskState		String	Drive state
		firmware		Array of objects	Information about disk-drive firmware
			build	String	Firmware build
			classifications	Array of integers	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**

Attributes					Type	Description
				type	String	Firmware type, such as UEFI, MP, or DSA
				version	String	Firmware version
		FRU			String	Drive FRU
		healthState			String	Drive health status. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
		interfaceType			String	Drive interface type
		largestAvailableSize			Integer	Largest available size
		m2Location			String	M.2 location
		manufacturer			String	Drive manufacturer
		mediaType			String	Media type
		model			String	Drive model
		name			String	Drive name
		numberOfBlocks			Long	Number of blocks
		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**. Percent of remaining life • **-1**. Unknown (default) • **-2**. Information is not available • **-3**. Drive is not an SSD
		partNumber			String	Drive part number
		serialNumber			String	Drive serial number
		uuid			String	Drive UUID
	description				String	Storage description
	name				String	Storage name
	raidLevel				Integer	RAID level
	remainingSpace				Integer	Remaining space
	totalManagedSpace				Long	
storageVolumes					Array of objects	Information about each storage volume
	accessPermission				String	
	blockSize				Integer	
	bootable				Boolean	
	description				String	
	driveIndex				Integer	
	health				String	
	isSDRAID				String	

Attributes			Type	Description
	LUN		Integer	
	name		String	
	numberOfBlocks		Long	
	primaryPartition		Integer	
	removable		Boolean	
	stripeSize		Integer	
	targetType		String	
	volumeID		String	
	volumeStatus		String	
	volumeType		String	
	volumeOwner		String	
	volumeUID		String	
	uuid		String	RAID device UUID
releaseName			String	Release name
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.
	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		object	Information about the stored credential that is associated with this device, if applicable

Attributes	Type	Description
id	String	Description of the stored credential
description	String	ID of the stored credential
userName	String	Name of the stored credential
uri	String	URI of the device
securityMode	String	Security Mode. This can be one of the following values. • **NIST SP 800-131A** • **Compatibility Security** • **Standard Security** • **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	Device serial number
slots	Array of integers	List of occupied slots
ssdWearThreshold	Integer	
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.
subSlots	String	Information about management status
systemBoard	Object	Information about the system board
machineType	String	Device machine type
model	String	Device model
productName	String	Product name
serialNumber	String	Device serial number
uuid	String	Device UUID
techTipsCount	Integer	Number of tech tips that are associated with this device For information about each tech tip, use GET /api/v1/data/ techTips.
thinkServerFru	Array of Strings	(ThinkServer servers only)
type	String	Resource type (translated). This can be one of the following values. • **chassis** • **server** • **storage** • **switch**
typeKey	String	Resource type key. This can be one of the following values. • **chassis** • **server** • **storage** • **switch**

Attributes	Type	Description
updates	Object	(XClarity Administrator only) Information about the update history for the resource manager
identifier	String	Update ID
components	Array of objects	Information about each update component
componentID	String	Component ID
cveDetails	Object	Information about available CVEs for this component
availableFixes	Integer	Total number of CVEs available for this component
cveList	Array of strings	List of CVEs that are available for the component
id	String	
fixedVersion	Object	
identifier	String	
number	String	
releaseTimestamp	String	
name	String	CVE name
publishDate	String	Timestamp when the CVE was published
severity	String	Highest severity (translated) of all CVEs for the component. This can be one of the following values. • **Critical**. Devices with one or more critical CVEs • **Noncritical**. Devices with one or more high, medium, and low CVEs • **Protected**. Devices with no CVEs
_link	Object	CVE link (see Links)
fixedVersion	Object	
identifier	String	
number	String	
releaseTimestamp	String	
severity	String	Highest severity (translated) of all CVEs for the component. This can be one of the following values. • **Critical**. Devices with one or more critical CVEs • **Noncritical**. Devices with one or more high, medium, and low CVEs • **Protected**. Devices with no CVEs
severityKey	String	Highest severity key of all CVEs for the component. This can be one of the following values. • **critical**. Devices with one or more critical CVEs • **noncritical**. Devices with one or more high, medium, and low CVEs • **protected**. Devices with no CVEs
_severity	Object	Information about the severity weight

Attributes				Type	Description
			name	String	Highest severity key of all CVEs for the component. This can be one of the following values. • **critical**. Devices with one or more critical CVEs • **noncritical**. Devices with one or more high, medium, and low CVEs • **protected**. Devices with no CVEs
			weight	Integer	Weight of the severity
		firmwareActivationStatus		String	
		firmwareActivationStatusKey		String	
		mainComponentName		String	Main component name
		name		String	Component name
		policyState		String	Policy state (translated). This can be one of the following values. • **No Policy Assigned** • **Policy Assigned**
		policyStateKey		String	Policy state key. This can be one of the following values. • **NoPolicyAssigned** • **PolicyAssigned**
		targetVersion		Object	Information about the target update for the component based on the assigned policy If a policy is not assigned, this value is null.
			identifier	String	Version ID
			number	String	Version number
			releaseTimestamp	String	Timestamp when the version was released 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.
		upgradeable		Boolean	Indicates whether the component can be updated. This can be one of the following values. • **true**. The component can be updated. • **false**. The component cannot be updated.
		version		Object	Information about the update that is currently installed for the component
			identifier	String	Version ID
			number	String	Version number
			releaseTimestamp	String	Timestamp when the version was released 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.
	cveDetails			Object	Information about available CVEs for the update
		availableFixes		Integer	Total number of CVEs available for the update
		severity		String	Highest severity (translated) of all CVEs in the the update. This can be one of the following values. • **Critical**. Devices with one or more critical CVEs • **Noncritical**. Devices with one or more high, medium, and low CVEs • **Protected**. Devices with no CVEs

Attributes	Type	Description
severityKey	String	Highest severity key of all CVEs in the the update. This can be one of the following values. • **Critical**. Devices with one or more critical CVEs • **Noncritical**. Devices with one or more high, medium, and low CVEs • **Protected**. Devices with no CVEs
policy	Object	Information about the update-compliance policy that is assigned to this device If a policy is not assigned, this value is null.
id	String	Policy ID
name	String	Policy name
policyState	String	Policy state (translated). This can be one of the following values. • **No Policy Assigned** • **Policy Assigned**
policyStateKey	String	Policy state key. This can be one of the following values. • **NoPolicyAssigned** • **PolicyAssigned**
userDefinedName	String	User-defined name for the device
userDescription	String	User description
uuid	String	UUID
vnicMode	String	VNIC mode. This can be one of the following values. • **enabled** • **disabled**
vpdID	String	VPD ID
warranty	Object	Information about the warranty for this device
endTimestamp	String	Warranty expiration date 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.
number	String	Warranty number. This can be one of the following values. • **3PL** • **3XL**
startTimestamp	String	Warranty start date 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.
status	String	Warranty status key (translated). This can be one of the following values. • **Active** • **Expired** • **Retrieving Data** • **null**
statusKey	String	Warranty status key. This can be one of the following values. • **Active** • **Expired** • **RetrievingData** • **null**

Attributes	Type	Description
_links	Object	Device URI (see Links)
_rawType	String	

The following example is returned if the request is successful.

```
{
    "id": "198B27F09DE84EFA808FD670B9D1F71F-B2950AF32CA74EF79A9D62DCBAAC6B01",
    "accessState": "Online",
    "accessStateKey": "Online",
    "accurateHealth": true,
    "activationKeys": [{
        "description": "Lenovo XClarity Controller 2 Platinum Upgrade",
        "keyExpirationDate": "",
        "keyFeatureType": 74,
        "keyIdentiferList": [{
            "keyIdentifier": "7D9D1234567890",
            "keyIdentifierType": "MT"
        }],
        "keyStatus": "VALID",
        "keyUseCount": 0,
        "keyUseLimit": 0,
        "uuid": ""
    }],
    "addinCards": [{
        "class": "Network controller",
        "firmware": [ {
            "build": "0",
            "classifications": [ 13 ],
            "date": "",
            "deviceTypeKey": "software bundle",
            "name": "Firmware Bundle",
            "revision": "0",
            "role": "",
            "softwareID": "17AA4104",
            "status": "Active",
            "type": "Software Bundle",
            "version": "227.0.3.1"
        }],
        "fodUniqueID": "",
        "FRU": "01PE761",
        "fruSerialNumber": "01PE761",
        "isAddOnCard": true,
        "isAgentless": false,
        "isPLDMUpdateSupported": false,
        "manufacturer": "Broadcom Limited",
        "name": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
        "partNumber": "SN37A28309",
        "pciBusNumber": "65",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "0",
        "pciRevision": "0x0001",
        "pciSegmentNumber": "0",
        "pciSubID": "0x4104",
        "pciSubVendorID": "0x17aa",
        "portInfo": {
            "physicalPorts": [{
                "logicalPorts": [{
                    "addresses": "e4:3d:1a:63:e6:ec",
                    "logicalPortIndex": 1,
```

```
                    "portNumber": 1,
                    "portType": "ETHERNET",
                    "vnicMode": false
                }],
                "peerBay": 0,
                "physicalPortIndex": 1,
                "portType": "ETHERNET",
                "portNumber": 1,
                "speed": "N/A",
                "status": "Down"
            }]
        },
        "posID": "0x1657",
        "productName": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
        "slotName": "PCIe 6",
        "slotNumber": "6",
        "slotSupportsHotPlug": "false",
        "vpdID": "0x14e4"
    },
    ...,
    {
        "class": "Network controller",
        "firmware": [{
                "build": "0",
                "classifications": [13],
                "date": "",
                "deviceTypeKey": "software bundle",
                "name": "Firmware Bundle",
                "revision": "0",
                "role": "",
                "softwareID": "17AA4104",
                "status": "Active",
                "type": "Software Bundle",
                "version": "227.0.3.1"
            }],
        "fodUniqueID": "",
        "FRU": "01PE761",
        "fruSerialNumber": "01PE761",
        "isAddOnCard": true,
        "isAgentless": false,
        "isPLDMUpdateSupported": false,
        "manufacturer": "Broadcom Limited",
        "name": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
        "partNumber": "SN37A28309",
        "pciBusNumber": "65",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "3",
        "pciRevision": "0x0001",
        "pciSegmentNumber": "0",
        "pciSubID": "0x4104",
        "pciSubVendorID": "0x17aa",
        "portInfo": {
            "physicalPorts": [{
                "logicalPorts": [{
                    "addresses": "e4:3d:1a:63:e6:ef",
                    "logicalPortIndex": 1,
                    "portNumber": 1,
                    "portType": "ETHERNET",
                    "vnicMode": false
                }],
                "peerBay": 0,
```

```
                    "physicalPortIndex": 4,
                    "portType": "ETHERNET",
                    "portNumber": 4,
                    "speed": 1,
                    "status": "Up"
                }]
        },
    "posID": "0x1657",
    "productName": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
    "slotName": "PCIe 6",
    "slotNumber": "6",
    "slotSupportsHotPlug": "false",
    "vpdID": "0x14e4"
}],
"assetTag": "",
"description": "This resource is used to represent a chassis or other physical
                enclosure for a Redfish implementation.",
"deviceInfo": {
    "domainName": null,
    "entitleSerialNumber": null,
    "groupNames": [],
    "healthStatus": "Warning",
    "healthStatusKey": "Warning",
    "hostname": "XCC-MTM-SN",
    "ipv4Addresses": [ "10.240.193.125" ],
    "ipv6Addresses": [ "2002:97b:c2bb:830:922e:16ff:fe0a:1597", "fe80::922e:16ff:fe0a:1597",
                        "fe80::922e:16ff:fe0a:1598" ],
    "location": {
        "location": "",
        "lowestRackUnit": 1,
        "rack": "",
        "room": ""
    },
    "machineType": "7D9D",
    "manager": {
        "id": "B2950AF32CA74EF79A9D62DCBAAC6B01",
        "domainName": "",
        "fqdn": null,
        "hostname": "xc1h",
        "inContextHref": "/ui/index.html#/compDetails/Rack-Tower Server/198B27F09DE84EFA808FD670B9D1F71F/",
        "ipv4Addresses": [ "10.240.197.128" ],
        "ipv6Addresses": []
    },
    "model": "MT110D",
    "powerStatus": "On",
    "powerStatusKey": "On",
    "productName": "ThinkSystem SR645 V3 MB,Genoa,DDR5,Oahu,1U",
    "serialNumber": "1234567890",
    "userDefinedName": "Oahu",
    "uuid": "198B27F09DE84EFA808FD670B9D1F71F",
},
"deviceName": "Oahu",
"deviceType": "Server",
"deviceTypeKey": "server",
"discoveryTimestamp": "2024-05-16T05:01:49.303Z",
"drives": [],
"encapsulation": {
    "encapsulationMode": "normal"
},
"fans": [{
    "description": "Fan Fan 1 Front Tach",
```

```
            "healthState": "Normal",
            "healthStateKey": "Normal",
            "name": "Fan 1 Front Tach",
            "slot": "1",
            "slots": 1,
            "speed": 7552,
            "status": "OK"
        },
        ...,
        {
            "description": "Fan Fan 8 Rear Tach",
            "healthState": "Normal",
            "healthStateKey": "Normal",
            "name": "Fan 8 Rear Tach",
            "slot": "8",
            "slots": 8,
            "speed": 6264,
            "status": "OK"
        }],
        "featuresOnDemand": {
            "features": [ "RDOC", "REMOTE CONTROL 6 USERS", "REMOTE MEDIA" ],
            "tierLevel": 3
        },
        "firmware": [{
            "build": "KAX319G",
            "classifications": [ "10" ],
            "date": "2023-11-02T00:00:00Z",
            "deviceTypeKey": "xcc",
            "firmwareActivationStatus": "Active",
            "firmwareActivationStatusKey": "Active",
            "name": "XClarity Controller",
            "revision": "2.62",
            "role": "Primary",
            "status": "Active",
            "type": "XCC",
            "version": "2.62"
        },
        ...,
        {
            "build": "Unknown",
            "classifications": [],
            "date": "",
            "deviceTypeKey": "lxum",
            "firmwareActivationStatus": "Inactive",
            "firmwareActivationStatusKey": "Inactive",
            "name": "Lenovo XClarity Update Manager",
            "revision": "Unknown",
            "role": "Primary",
            "status": "Inactive",
            "type": "LXUM",
            "version": "Unknown"
        }],
        "groups": [],
        "height": 1,
        "hostname": "XCC-MTM-SN",
        "ipInterfaces": [{
            "IPv4assignments": [{
                "id": 0,
                "address": "10.240.193.125",
                "deviceTypeKey": "inuse",
                "gateway": "10.240.193.1",
```

```
            "subnet": "255.255.255.0",
            "type": "INUSE"
        }],
        "IPv4DHCPmode": "STATIC_ONLY",
        "IPv4enabled": true,
        "IPv6assignments": [{
            "id": 0,
            "address": "2002:97b:c2bb:830:922e:16ff:fe0a:1597",
            "deviceTypeKey": "inuse",
            "gateway": "0:0:0:0:0:0:0:0",
            "prefix": 64,
            "scope": "Global",
            "source": "Stateless",
            "type": "INUSE",
        },
        ...,
        {
            "id": 0,
            "address": "fe80:0:0:0:922e:16ff:fe0a:1598",
            "deviceTypeKey": "inuse",
            "gateway": "0:0:0:0:0:0:0:0",
            "prefix": 64,
            "scope": "LinkLocal",
            "source": "Other",
            "type": "INUSE"
        }],
        "IPv6DHCPenabled": false,
        "IPv6enabled": true,
        "IPv6statelessEnabled": true,
        "IPv6staticEnabled": false,
        "label": "unknown",
        "name": "Manager Ethernet Interface"
    }],
    "ipv4Addresses": [ "10.240.193.125" ],
    "ipv6Addresses": [ "2002:97b:c2bb:830:922e:16ff:fe0a:1597", "fe80::922e:16ff:fe0a:1597",
                     "fe80::922e:16ff:fe0a:1598" ],
    "isEmbedded": false,
    "lanOverUsb": "disabled",
    "lanOverUsbPortForwardingModes": [{
        "deviceTypeKey": "osdeploy",
        "externalIPAddress": "",
        "state": "disabled",
        "type": "OSDeploy"
    }],
    "lastSyncTimestamp": "2024-05-17T06:47:31.428Z",
    "lastUpdateTimestamp": "2024-05-17T06:47:31.365Z",
    "leds": [{
        "color": "Green",
        "location": "Planar",
        "name": "BMC Heartbeat",
        "state": "Blinking"
    },
    ...,
    {
        "color": "Amber",
        "location": "Planar",
        "name": "CPU2",
        "state": "Off"
    }],
    "location": {
        "location": "",
```

```
        "lowestRackUnit": 1,
        "rack": "",
        "room": ""
    },
    "lxcaOverallHealthState": "Warning",
    "lxcaUUID": "B2950AF32CA74EF79A9D62DCBAAC6B01",
    "machineType": "7D9D",
    "manager": {
        "id": "B2950AF32CA74EF79A9D62DCBAAC6B01",
        "domainName": "",
        "fqdn": null,
        "groups": [],
        "hostname": "xc1h",
        "inContextHref": "/ui/index.html#/compDetails/Rack-Tower Server/198B27F09DE84EFA808FD670B9D1F71F/",
        "ipv4Addresses": [ "10.240.197.128" ],
        "ipv6Addresses": [],
        "uri": "/api/v1/connector/managers/B2950AF32CA74EF79A9D62DCBAAC6B01"
    },
    "manufacturer": "Lenovo",
    "manufacturerId": "Lenovo",
    "memoryModules": [{
        "capacity": 16,
        "deviceTypeKey": "ddr5",
        "displayName": "DIMM 7",
        "fruPartNumber": "",
        "healthState": "NA",
        "healthStateKey": "NA",
        "manufacturer": "Samsung",
        "metrics": {
            "alarmTrips": {}
        },
        "model": "DDR5",
        "operatingMemoryMode": [ "Volatile" ],
        "partNumber": "M321R2GA3BB6-CQKMG",
        "present": false,
        "serialNumber": "80CE012210029FBA98",
        "slot": 7,
        "speed": 4800,
        "type": "DDR5",
    }],
    "mgmtProcIPaddress": "10.240.193.125",
    "mgmtProcType": "XCC2",
    "model": "MT110D",
    "mtm": "7D9D/MT110D",
    "name": "Oahu",
    "onboardPciDevices": [{
        "class": "Display controller",
        "firmware": [],
        "fodUniqueID": "",
        "isAddOnCard": false,
        "isAgentless": false,
        "isPLDMUpdateSupported": false,
        "name": "Onboard VGA",
        "pciBusNumber": "197",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "0",
        "pciRevision": "0x0052",
        "pciSegmentNumber": "0",
        "pciSubID": "0x2000",
        "pciSubVendorID": "0x1a03",
        "portInfo": {},
```

```
            "posID": "0x2000",
            "vpdID": "0x1a03"
        },
        ...,
        {
            "class": "Mass storage controller",
            "firmware": [],
            "fodUniqueID": "",
            "isAddOnCard": false,
            "isAgentless": false,
            "isPLDMUpdateSupported": false,
            "name": "Onboard SATA Controller",
            "pciBusNumber": "199",
            "pciDeviceNumber": "0",
            "pciFunctionNumber": "1",
            "pciRevision": "0x0091",
            "pciSegmentNumber": "0",
            "pciSubID": "0x7901",
            "pciSubVendorID": "0x1022",
            "portInfo": {},
            "posID": "0x7901",
            "vpdID": "0x1022"
        }],
    "osProfiles": {
        "applicableStatus": "No Profile Assigned",
        "applicableStatusKey": "NoProfileAssigned",
        "assigned": {
            "id": null,
            "name": "No Assignment",
            "uri": null
        },
        "deployStatus": "Ready",
        "deployStatusKey": "ready"
    },
    "overallHealthState": "Warning",
    "overallHealthStateKey": "Warning",
    "patterns": {
        "assigned": {
            "id": null,
            "name": "No Assignment"
        },
        "complianceStatus": "No Pattern Assigned",
        "complianceStatusKey": "NoPatternAssigned"
    },
    "partNumber": "STA7B07502",
    "pciDevices": [{
        "class": "Display controller",
        "firmware": [],
        "fodUniqueID": "",
        "isAddOnCard": false,
        "isAgentless": false,
        "isPLDMUpdateSupported": false,
        "name": "Onboard VGA",
        "pciBusNumber": "197",
        "pciDeviceNumber": "0",
        "pciFunctionNumber": "0",
        "pciRevision": "0x0052",
        "pciSegmentNumber": "0",
        "pciSubID": "0x2000",
        "pciSubVendorID": "0x1a03",
        "portInfo": {},
```

```
            "posID": "0x2000",
            "vpdID": "0x1a03"
        },
        ...,
        {
            "class": "Network controller",
            "firmware": [{
                "build": "0",
                "classifications": [ 13 ],
                "date": "",
                "deviceTypeKey": "software bundle",
                "name": "Firmware Bundle",
                "revision": "0",
                "role": "",
                "softwareID": "17AA4104"
                "status": "Active",
                "type": "Software Bundle",
                "version": "227.0.3.1",
            }],
            "fodUniqueID": "",
            "FRU": "01PE761",
            "fruSerialNumber": "01PE761",
            "isAddOnCard": true,
            "isAgentless": false,
            "isPLDMUpdateSupported": false,
            "manufacturer": "Broadcom Limited",
            "name": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
            "partNumber": "SN37A28309",
            "pciBusNumber": "65",
            "pciDeviceNumber": "0",
            "pciFunctionNumber": "0",
            "pciRevision": "0x0001",
            "pciSegmentNumber": "0",
            "pciSubID": "0x4104",
            "pciSubVendorID": "0x17aa",
            "portInfo": {
                "physicalPorts": [{
                    "logicalPorts": [{
                        "addresses": "e4:3d:1a:63:e6:ec",
                        "logicalPortIndex": 1,
                        "portNumber": 1,
                        "portType": "ETHERNET",
                        "vnicMode": false
                    }],
                    "peerBay": 0,
                    "physicalPortIndex": 1,
                    "portType": "ETHERNET",
                    "portNumber": 1,
                    "speed": "N/A",
                    "status": "Down"
                }]
            },
            "posID": "0x1657",
            "productName": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
            "slotName": "PCIe 6",
            "slotNumber": "6",
            "slotSupportsHotPlug": "false",
            "vpdID": "0x14e4"
        }],
        "powerAllocation": {
            "maximumAllocatedPower": 1800,
```

```
        "minimumAllocatedPower": 0
    },
    "powerCappingPolicy": {
        "cappingACorDCMode": "AC",
        "cappingPolicy": "Unknown",
        "currentPowerCap": 0,
        "maximumPowerCappingHotPlugLevel": -1,
        "maxPowerCap": 1800000,
        "minimumHardCapLevel": 0,
        "minimumPowerCappingHotPlugLevel": -1,
        "minPowerCap": 0,
        "powerCappingAllocUnit": "watts*10^-3"
    },
    "powerStatus": "On",
    "powerStatusKey": "On",
    "powerSupplies": [{
        "cmmDisplayName": "Power Supply 1",
        "cmmHealthState": "Unknown",
        "dataHandle": 0,
        "description": "Power Supply 1",
        "deviceTypeKey": "powersupply"
        "excludedHealthState": "Normal",
        "firmware": [{
            "build": null,
            "classifications": [ 10 ],
            "date": "",
            "deviceTypeKey": "firmware",
            "name": "PSU1",
            "role": "OK",
            "status": "OK",
            "softwareID": "PSUARTE7100",
            "type": "Firmware",
            "version": "6.52"
        }],
        "FRU": "",
        "fruSerialNumber": "",
        "hardwareRevision": "",
        "healthState": "Normal",
        "healthStateKey": "Normal",
        "inputVoltageIsAC": true,
        "inputVoltageMax": -1,
        "inputVoltageMin": -1,
        "leds": [],
        "machineType": "",
        "manufactureDate": "",
        "manufacturer": "ARTE",
        "manufacturerId": "",
        "model": "",
        "name": "Power Supply 1",
        "overallHealthState": "Normal",
        "overallHealthStateKey": "Normal",
        "parent": {
            "uri": "chassis/",
            "uuid": ""
        },
        "partNumber": "SP57A96595",
        "posID": "",
        "powerAllocation": {
            "totalInputPower": 0,
            "totalOutputPower": 1800
        },
```

```
            "powerState": "Unknown",
            "productId": "",
            "productName": "",
            "serialNumber": "P2ZS26G0216",
            "slots": [1],
            "type": "PowerSupply",
            "uri": "powerSupply/",
            "userDescription": "",
            "uuid": "",
            "vpdID": ""
      }],
      "processors": [{
            "cores": 96,
            "displayName": "AMD Eng Sample: 100-000000894-04",
            "family": "AMD_ZEN_PROCESSOR_FAMILY",
            "healthState": "GOOD",
            "healthStateKey": "GOOD",
            "manufacturer": "Advanced Micro Devices, Inc.",
            "maxSpeedMHZ": 3700,
            "partNumber": "Unknown",
            "present": false,
            "productVersion": "AMD Eng Sample: 100-000000894-04",
            "serialNumber": "0x02B60EB2C4ED0031",
            "slot": 1,
            "socket": "CPU 1",
            "speed": 2.15,
            "tdpWatts": 360
      }],
      "productId": "664A00",
      "productName": "ThinkSystem SR645 V3 MB,Genoa,DDR5,Oahu,1U",
      "raidSettings": [],
      "securityMode": "Compatibility Security",
      "serialNumber": "1234567890",
      "ssdWearThreshold": 8,
      "ssoEnabled": false,
      "systemBoard": {
            "machineType": "7D9D",
            "model": "MT110D",
            "productName": "ThinkSystem SR645 V3 MB,Genoa,DDR5,Oahu,1U",
            "serialNumber": "1234567890",
            "uuid": "198B27F09DE84EFA808FD670B9D1F71F"
      },
      "type": "server",
      "updates": {
            "identifier": "7D9D",
            "components": [{
                  "componentID": "XCC",
                  "cveDetails": {
                        "availableFixes": 0,
                        "cveList": [],
                        "fixedVersion": null,
                        "severity": "Protected",
                        "severityKey": "protected",
                        "_severity": {
                              "name": "protected",
                              "weight": 0
                        }
                  },
                  "firmwareActivationStatus": "Active",
                  "firmwareActivationStatusKey": "Active",
                  "mainComponentName": "XClarity Controller",
```

```json
            "name": "XClarity Controller",
            "policyState": "No Policy Assigned",
            "policyStateKey": "NoPolicyAssigned",
            "targetVersion": null,
            "upgradeable": true,
            "version": {
                "identifier": "KAX319G",
                "number": "2.62",
                "releaseDate": "2023-11-02T00:00:00Z"
            }
        },
        ...,
        {
            "componentID": "UEFI",
            "cveDetails": {
                "severity": "Protected",
                "severityKey": "protected",
                "availableFixes": 0,
                "fixedVersion": null,
                "cveList": [],
                "_severity": {
                    "name": "protected",
                    "weight": 0
                }
            },
            "firmwareActivationStatus": "Active",
            "firmwareActivationStatusKey": "Active",
            "mainComponentName": "Unified Extensible Firmware Interface",
            "name": "Unified Extensible Firmware Interface",
            "policyState": "No Policy Assigned",
            "policyStateKey": "NoPolicyAssigned",
            "targetVersion": null,
            "upgradeable": true,
            "version": {
                "identifier": "KAE119A",
                "number": "4.20",
                "releaseDate": "2024-04-10T00:00:00Z"
            }
        }]
        "cveDetails": {
            "availableFixes": 0,
            "severity": "Protected",
            "severityKey": "protected"
        }
        "policy": {
            "name": "No Assignment",
            "id": null
        },
        "policyState": "No Policy Assigned",
        "policyStateKey": "NoPolicyAssigned"
    },
    "userDefinedName": "Oahu",
    "uuid": "198B27F09DE84EFA808FD670B9D1F71F",
    "warranty": {
        "endTimestamp": "2019-12-10T00:00:00.000Z",
        "number": "TC0",
        "startTimestamp": "2019-10-30T00:00:00.000Z",
        "status": "Expired",
        "statusKey": "Expired"
    },
    "_links": {
```

```
      "rel": "self",
      "uri": "/api/v1/data/devices/198B27F09DE84EFA808FD670B9D1F71F-B2950AF32CA74EF79A9D62DCBAAC6B01"
   },
   "_rawType": "server"
}
```

/api/v1/data/devices/*{id}*/fans

Use this REST API to returnfan information for a specific device.

HTTP methods

GET

GET /api/v1/data/devices/*{id}*/fans

Use this method to return fan information for a specific device.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/data/devices/{id}/fans`

where *{id}* is the ID of the device. To obtain the device IDs, use GET /api/v1/data/devices.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. 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).

Attributes	Type	Description
fans	Array of objects	Information about each fan in the device

	description	String	Fan description
	healthState	String	Fan health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
	healthStateKey	String	Fan health state key. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
	name	String	Fan name
	slots	Integer	Fan slot
	speed	Integer	Fan speed
	status	String	Fan status
_links		Object	Device URI (see Links)

The following example is returned if the request is successful.

```
{
   "fans": [{
      "description": "Logical Device for fan / cooling device 1",
      "healthState": "Normal",
      "healthStateKey": "Normal",
      "name": "Fan 1",
      "slots": 1,
      "speed": 0,
      "status": "OK"
   },
   ...,
   {
      "description": "Logical Device for fan / cooling device 7",
      "healthState": "Normal",
      "healthStateKey": "Normal",
      "name": "Fan 7",
      "slots": 7,
      "speed": 0,
      "status": "OK"
   }],
   "_links": {
      "rel": "self",
      "uri": "/api/v1/data/devices/C7199530FEDE4FE09540DFC3D75FC56C/fans"
   }
}
```

/api/v1/data/devices/*{id}*/memoryModules

Use this REST API to returnmemory information about a specific device.

HTTP methods

GET

GET /api/v1/data/devices/*{id}*/memoryModules

Use this method to return memory-module information about a specific device.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/data/devices/{id}/memoryModules`

where *{id}* is the ID of the device. To obtain the device IDs, use GET /api/v1/data/devices.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. 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).

Attributes		Type	Description
memoryModules		Array of objects	Information about each memory module in the device
	capacity	Integer	Capacity
	deviceTypeKey	String	Device type key
	displayName	String	Display name
	fruPartNumber	String	FRU part number
	healthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
	healthStateKey	String	Health state key. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**

Attributes		Type	Description
manufacturer		String	Manufacturer
metrics		Object	Information about memory metric data
	alarmTrips	Object	Information about alarm trips
model		String	Model
partNumber		String	Part number
present		Boolean	
serialNumber		String	Serial number
slot		Integer	Slot
speed		Integer	Number of data-transfer operations that occur in each second, in MT/s (megatransfers per second)
type		String	Type
_links		Object	Device URI (see Links)

The following example is returned if the request is successful.

```
{
   "memoryModules": [{
      "capacity": 2,
      "deviceTypeKey": "ddr3",
      "displayName": "DIMM 21",
      "fruPartNumber": "",
      "healthState": "NA",
      "healthStateKey": "NA",
      "manufacturer": "Micron Technology",
      "metrics": { "alarmTrips": {} },
      "model": "DDR3",
      "operatingMemoryMode": [ "Volatile" ],
      "partNumber": "9KSF25672PZ-1G4M1",
      "present": false,
      "serialNumber": "377B770D",
      "slot": 21,
      "speed": 1333,
      "type": "DDR3"
   },
   ...,
   {
      "capacity": 16,
      "deviceTypeKey": "ddr5",
      "displayName": "DIMM 7",
      "fruPartNumber": "",
      "healthState": "NA",
      "healthStateKey": "NA",
      "manufacturer": "Samsung",
      "metrics": { "alarmTrips": {} },
      "model": "DDR5",
      "operatingMemoryMode": [ "Volatile" ],
      "partNumber": "M321R2GA3BB0-CQKMG",
      "present": false,
      "serialNumber": "80CE01214102186E41",
      "slot": 7,
      "speed": 4800,
      "type": "DDR5"
```

```
    }],
    "_links": {
        "rel": "self",
        "uri": "/api/v1/data/devices/C7199530FEDE4FE09540DFC3D75FC56C/memoryModules"
    }
}
```

/api/v1/data/devices/*{id}*/pciDevices

Use this REST API to returnPCI-device information for a specific device.

HTTP methods

GET

GET /api/v1/data/devices/*{id}*/pciDevices

Use this method to return PCI-device information for a specific device.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/data/devices/{id}/pciDevices`

where *{id}* is the ID of the device. To obtain the device IDs, use GET /api/v1/data/devices.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. 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).

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**
	firmware		Array of objects	Flash storage firmware properties
		build	String	Firmware build
		classifications	Array of integers	Firmware type codes
		date	String	Firmware date
		deviceTypeKey	String	Device type key
		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
	fodUniqueID		String	FoD unique ID

Attributes	Type	Description
FRU	String	Add-in card FRU part number
fruSerialNumber	String	Add-in card 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
pciSubID	String	PCI subsystem ID
pciSubVendorID	String	PCI sub-vendor ID
portInfo	Object	Information about the ports
physicalPorts	Array of objects	Information about the physical ports
logicalPorts	Array of objects	List of associated logical ports
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	Product name
		slotName		String	Slot name
		slotNumber		String	Slot number
		slotSupportsHotPlug		String	Indicates whether the slot is hot pluggable. This can be one of the following values. • **true** • **false**
		vpdID		String	VPD ID
_links				Object	Device URI (see Links)

The following example is returned if the request is successful.

```
{
   "pciDevices": [{
      "class": "Display controller",
      "firmware": [],
      "fodUniqueID": "",
      "isAddOnCard": false,
      "isAgentless": false,
      "isPLDMUpdateSupported": false,
      "name": "Onboard VGA",
      "pciBusNumber": "198",
      "pciDeviceNumber": "0",
      "pciFunctionNumber": "0",
      "pciRevision": "0x0052",
      "pciSegmentNumber": "0",
      "pciSubID": "0x2000",
      "pciSubVendorID": "0x1a03",
```

```
            "portInfo": {},
            "posID": "0x2000",
            "vpdID": "0x1a03",
        },
        ...,
        {
            "class": "Network controller",
            "firmware": [{
                "build": "0",
                "classifications": [ 13 ],
                "date": "",
                "deviceTypeKey": "software bundle",
                "name": "Firmware Bundle",
                "revision": "0",
                "role": "",
                "softwareID": "17AA4104",
                "status": "Active",
                "type": "Software Bundle",
                "version": "222.0.2.1"
            }],
            "FRU": "01PE761"
            "fruSerialNumber": "01PE761",
            "fodUniqueID": "",
            "isAddOnCard": true,
            "isAgentless": false,
            "isPLDMUpdateSupported": false,
            "manufacturer": "Broadcom Limited",
            "name": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
            "partNumber": "SN37A28309",
            "pciBusNumber": "2",
            "pciDeviceNumber": "0",
            "pciFunctionNumber": "0",
            "pciRevision": "0x0001",
            "pciSegmentNumber": "0",
            "pciSubID": "0x4104",
            "pciSubVendorID": "0x17aa",
            "portInfo": {
                "physicalPorts": [{
                    "logicalPorts": [{
                        "addresses": "84:16:0c:ae:15:f2",
                        "logicalPortIndex": 1,
                        "portNumber": 1,
                        "portType": "ETHERNET",
                        "vnicMode": false
                    }],
                    "physicalPortIndex": 1,
                    "peerBay": 0,
                    "portType": "ETHERNET",
                    "portNumber": 1,
                    "speed": -1,
                    "status": "Down"
                }]
            },
            "posID": "0x1657",
            "productName": "Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter",
            "slotName": "PCIe 13",
            "slotNumber": "13",
            "slotSupportsHotPlug": "false",
            "vpdID": "0x14e4"
        }],
        "_links": {
```

```
        "rel": "self",
        "uri": "/api/v1/data/devices/91C6C497643711ED9D3BA31E8F6751A9-B65EC401D9B741F49736CFC9380791F4/pciDevices"
    }
}
```

/api/v1/data/devices/*{id}*/processors

Use this REST API to returnprocessor information for a specific device.

HTTP methods

GET

GET /api/v1/data/devices/*{id}*/processors

Use this method to return processor information for a specific device.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/data/devices/{id}/processors`

where *{id}* is the ID of the device. To obtain the device IDs, use GET /api/v1/data/devices.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. 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).

Attributes	Type	Description
processors	Array of objects	Information about each processor in the device
cores	Integer	Number of cores
displayName	String	Display name
family	String	Family
healthState	String	Health state (translated)
healthStateKey	String	Health state key

Attributes		Type	Description
	manufacturer	String	Manufacturer
	maxSpeedMHZ	Integer	Maximum processor speed
	partNumber	String	Part number
	present	Boolean	
	productVersion	String	Product version
	serialNumber	String	Serial number
	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	String	Speed
	tdpWatts	Integer	
_links		Object	Device URI (see Links)

The following example is returned if the request is successful.

```
{
    "processors": [{
        "cores": 24,
        "displayName": "AMD EPYC 9274F 24-Core Processor",
        "family": "AMD_ZEN_PROCESSOR_FAMILY",
        "healthState": "GOOD",
        "healthStateKey": "GOOD",
        "manufacturer": "Advanced Micro Devices, Inc.",
        "maxSpeedMHZ": 4300,
        "partNumber": "Unknown",
        "present": false,
        "productVersion": "AMD EPYC 9274F 24-Core Processor",
        "serialNumber": "0x472391C8E4723800",
        "slot": 1,
        "socket": "CPU 1",
        "speed": 4.05,
        "tdpWatts": 320,
    }],
    "_links": {
        "rel": "self",
        "uri": "/api/v1/data/devices/2E9F10E5641511ED97CBB040AD2C7996-B65EC401D9B741F49736CFC9380791F4/processors"
    }
}
```

/api/v1/data/devices/{id}/powerSupplies

Use this REST API to returnpower-supply information about a specific device.

HTTP methods

GET

GET /api/v1/data/devices/{id}/powerSupplies

Use this method to return power-supply information about a specific device.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/data/devices/{id}/powerSupplies`

where *{id}* is the ID of the device. To obtain the device IDs, use GET /api/v1/data/devices.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. 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).

Attributes			Type	Description
powerSupplies			Array of objects	(Rack servers only) Information about power supplies
	cmmDisplayName		String	Assigned component name
	cmmHealthState		String	Health state (translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
	dataHandle		Long	Time stamp of the last status update
	description		String	Assigned component description
	deviceTypeKey		String	Device type key
	excludedHealthState		String	Excluded health state. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
	firmware		Array of objects	Power-supply firmware details
		build	String	Firmware build
		classifications	Array of integers	Firmware type codes

Attributes		Type	Description
	date	String	Firmware date
	deviceTypeKey	String	Device type key
	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
fruSerialNumber		String	FRU serial number
hardwareRevision		String	Hardware revision
healthState		String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
healthStateKey		String	Health state key. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
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

Attributes			Type	Description
		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
	manufacturer		String	Manufacture name
	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	Highest severity of all power supplies(translated). This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
	overallHealthStateKey		String	Highest severity key. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
	parent		Object	Information about the parent device
		uri	String	Parent URI
		uuid	String	Parent UUID
	posID		String	Position ID
	powerAllocation		Object	Information about power allocation
		totalInputPower	Long	Total input power

Attributes			Type	Description
		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**
	powerStatus		String	Power status (translated). This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
	powerStatusKey		String	Power status key. This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
	productId		String	Product ID
	productName		String	Product name
	serialNumber		String	Serial number
	slots		Integer	Power-supply primary slot
	type		String	Resource type. This value is always **PowerSupplies**.
	uri		String	Power supply URI
	userDescription		String	User description
	uuid		String	UUID
	vpdID		String	VPD ID
_links			Object	Device URI (see Links)

The following example is returned if the request is successful.

```
{
    "powerSupplies": [{
        "cmmDisplayName": "Power Supply 1",
        "cmmHealthState": "Unknown",
        "dataHandle": 0,
        "description": "Power Supply 1",
        "deviceTypeKey": "powersupply",
        "excludedHealthState": "Normal",
        "firmware": [{
            "build": null,
            "classifications": [ 10 ],
            "date": "",
            "deviceTypeKey": "firmware",
            "name": "PSU1",
            "role": "OK",
            "softwareID": "PSUDETA6d00",
            "status": "OK",
            "type": "Firmware",
            "version": "3.50"
```

```
        }],
        "FRU": "",
        "fruSerialNumber": "",
        "hardwareRevision": "",
        "healthState": "Normal",
        "healthStateKey": "Normal",
        "inputVoltageIsAC": true,
        "inputVoltageMax": -1,
        "inputVoltageMin": -1,
        "leds": [],
        "machineType": "",
        "manufactureDate": "",
        "manufacturer": "DETA",
        "manufacturerId": "",
        "model": "",
        "name": "Power Supply 1",
        "overallHealthState": "Normal",
        "overallHealthStateKey": "Normal",
        "parent": {
            "uri": "chassis/",
            "uuid": ""
        },
        "partNumber": "SP57A14695",
        "posID": "",
        "powerAllocation": {
            "totalInputPower": 0,
            "totalOutputPower": 750
        },
        "powerState": "Unknown",
        "powerStatus": "Unknown",
        "powerStatusKey": "Unknown"
        "productId": "",
        "productName": "",
        "serialNumber": "D1DG01B0043",
        "slots": [ 1 ],
        "type": "PowerSupply",
        "uri": "powerSupply/",
        "userDescription": "",
        "uuid": "",
        "vpdID": ""
    }],
    "_links": {
        "rel": "self",
        "uri": "/api/v1/data/devices/91C6C497643711ED9D3BA31E8F6751A9-B65EC401D9B741F49736CFC9380791F4/powerSupplies"
    }
}
```

/api/v1/data/devices/{id}/storage

Use this REST API to storage information for a specific device.

HTTP methods

GET

GET /api/v1/data/devices/{id}/storage

Use this method to return storage information for a specific device.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/data/devices/{id}/storage`

where *{id}* is the ID of the device. To obtain the device IDs, use GET /api/v1/data/devices.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. 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).

Attributes		Type	Description
bay		String	Bay or slot number
blockSize		Integer	Block size
capacity		Integer	(M.2 drives only) Storage capacity, in KB
description		String	Description
diskState		String	Disk-drive state
encryptionStatus		String	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	Information about add-in card firmware
	build	String	Firmware build
	classifications	Array of integers	Firmware type codes
	date	String	Firmware date
	deviceTypeKey	String	Device type key
	name	String	Firmware name
	revision	String	Firmware revision

Attributes	Type	Description
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
FRU	String	FRU
healthState	String	Health state (translated) that corresponds to the highest event severity of all disk drives in the device. This can be one of the following values. • **Normal** • **Warning** • **Critical** • **Unknown**
healthStateKey	String	Health state key that corresponds to the highest event severity of all disk drives in the device. This can be one of the following values. • **normal** • **warning** • **critical** • **unknown**
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
manufacturer	String	Manufacturer
mediaType	String	Media type
model	String	Model
name	String	Drive name
numberOfBlocks	Integer	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

Attributes	Type	Description
uuid	String	Storage device UUID
_links	Object	Device URI (see Links)

The following example is returned if the request is successful.

```
[
    {
        "bay": 0,
        "blockSize": 512,
        "capacity": 1200243695616,
        "description": "1.20TB 10K 12Gbps SAS 2.5 HDD",
        "diskState": "Online",
        "encryptionStatus": "Unencrypted",
        "firmware": [{
            "build": "0",
            "classifications": [ 10 ],
            "date": "",
            "deviceTypeKey": "firmware",
            "name": "ST1200MM0009",
            "revision": "0",
            "role": "",
            "softwareID": "01GV140",
            "status": "Inactive",
            "type": "Firmware",
            "version": "L1BD"
        }],
        "FRU": "00FC615",
        "healthState": "OK",
        "healthStateKey": "OK",
        "hotSpareType": "None",
        "interfaceType": "SAS",
        "largestAvailableSize": 512,
        "m2Location": "",
        "manufacturer": "Seagate",
        "mediaType": "HDD",
        "model": "ST1200MM0009",
        "name": "Disk.0",
        "numberOfBlocks": 2344225968,
        "partNumber": "00FC615",
        "remainingLife": null,
        "serialNumber": "WFKBX0F4",
        "temperature": 22,
        "uuid": ""
    },
    ...,
    {
        "bay": 7,
        "blockSize": 512,
        "capacity": 300000000000,
        "description": "300GB 10K 12Gbps SAS 2.5 HDD",
        "diskState": "JBOD",
        "encryptionStatus": "Unencrypted",
        "firmware": [{
            "build": "0",
            "classifications": [ 10 ],
            "date": "",
            "deviceTypeKey": "firmware",
            "name": "ST300MM0008",
            "revision": "0",
```

```
        "role": "",
        "softwareID": "00KJ441",
        "status": "Inactive",
        "type": "Firmware",
        "version": "L58D"
    }],
    "FRU": "00FC612",
    "healthState": "OK",
    "healthStateKey": "OK",
    "hotSpareType": "None",
    "interfaceType": "SAS",
    "largestAvailableSize": 512,
    "m2Location": "",
    "manufacturer": "Seagate",
    "mediaType": "HDD",
    "model": "ST300MM0008",
    "name": "Disk.7",
    "numberOfBlocks": 585937500,
    "partNumber": "SH20J31903",
    "remainingLife": null,
    "serialNumber": "S4209Y1Y",
    "temperature": 21,
    "uuid": ""
  }
]
```

/api/v1/data/devices/*{id}*/systemBoard

Use this REST API to returnsystem-board information for a specific device.

HTTP methods

GET

GET /api/v1/data/devices/*{id}*/systemBoard

Use this method to return system-board information for a specific device.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/data/devices/*{id}*/systemBoard

where *{id}* is the ID of the device. To obtain the device IDs, use GET /api/v1/data/devices.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. 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).

Attributes	Type	Description
machineType	String	Device machine type
model	String	Device model
productName	String	Device product name
serialNumber	String	Device serial number
uuid	String	Device UUID
_links	Object	Device URI (see Links)

The following example is returned if the request is successful.

```
{
   "machineType": "8737",
   "model": "AC1",
   "productName": "Flex System x240 Compute Node with embedded 10Gb Virtual Fabric",
   "serialNumber": "00008X7162",
   "uuid": "8E9768E2A8143660A24E01542802FEE7",
   "_links": {
      "rel": "self",
      "uri": "/api/v1/data/devices/C7199530FEDE4FE09540DFC3D75FC56C/systemBoard"
   }
}
```

/api/v1/data/deviceStatus

Use this REST API to returnstatus information for a specific device.

HTTP methods

GET

GET /api/v1/data/deviceStatus?deviceID=*{id}*

Use this method to return status information for a specific device.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/data/deviceStatus?deviceID=*{id}*

Query parameters

Parameters	Re-quired / Optional	Description
deviceID=*{id}*	Required	Returns status for a device, specified by the ID To obtain the device IDs, use GET /api/v1/data/devices

The following example returns status information for a specific device.
```
GET https://192.0.2.0/api/v1/data/deviceStatus?deviceID=
3015DE7E2B6011E881940A94EF5F5B65-C7199530FEDE4FE09540DFC3D75FC56C
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a query parameter is specified and the value of that parameter has no matches, the response body returns default values.
400	Bad Request	A query parameter 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	The resource cannot be found. 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).

Attributes	Type	Description
criticalAlerts	Integer	Number of critical alerts
faultLedStatus	String	Number of informational alerts
identityLedStatus	String	Fault LED status. This can be one of the following values. • **Off**. The LED is off. • **On**. The LED is on.
informationalAlerts	Integer	Identity LED status. This can be one of the following values. • **Off**. The LED is off. • **On**. The LED is on.
powerStatus	String	Power status. This can be one of the following values. • **Off** • **On** • **Standby** • **Unknown**
warningAlerts	Integer	Number of warning alerts
_links	Object	Device URI (see Links)

The following example is returned if the request is successful.
```
{
    "criticalAlerts": 0,
    "faultLedStatus": "Off",
```

```
    "identityLedStatus": "Off",
    "informationalAlerts": 0,
    "powerStatus": "Off",
    "warningAlerts": 1,
    "_links": {
        "rel": "self",
        "uri": "/api/v1/data/devices/C7199530FEDE4FE09540DFC3D75FC56C"
    }
}
```

/api/v1/data/techTips

Use this REST API to return a list of tech tips that are associated with a specific device.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

HTTP methods

GET

GET /api/v1/data/techTips

Use this method to return a list of technical tips that are associated with a specific device.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/data/techTips

Query parameters

Parameters	Re- quired / Optional	Description
deviceUUID=*{uuid}*	Required	Device UUID To obtain the device UUIDs, use GET /api/v1/data/devices.

The following example return a list of technical tips that are associated with a specific device.
GET https://192.0.2.0/api/v1/data/techTips?deviceUUID=00632D78DE644E23B712E200FE449787

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	The resource cannot be found. 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).

Attributes		Type	Description
results		Array of objects	Information about each tech tip
	abstract	String	Tech tip abstract
	timestamp	String	Timestamp when the tech tip 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.
	tipID	String	Technical tip ID You can get detailed information for this tech tip from the web using the following URL: `https://datacentersupport.lenovo.com/solutions/` *{techTipID}*
_links		Object	Request metadata (see Links)

The following example is returned if the request is successful.

```
{
    "results": [{
        "abstract": "System will hang at 'UEFI DXE INIT' when deploying iSCSI BOFM with QL45262
                    adapter - Lenovo ThinkSystem",
        "timestamp": "2021-01-22T00:00:00.000Z",
        "tipID": "HT510220"
    },
    {
        "abstract": "'An Uncorrectable Error has occurred on CPUs' when memory in closed page mode
                    - Lenovo ThinkAgile and Lenovo ThinkSystem",
        "timestamp": "2021-01-22T00:00:00.000Z",
        "tipID": "ht510558"
    }],
    "_links": {
        "rel": "self",
        "uri": "/api/v1/techTips/07389DD8C45D11E793557ED30AE53667-155B46F6F9064C25ACE5177C69F5E07F"
    }
}
```

/api/v1/managers-management/managers

Use this REST API to return a list of all resource managers or to connect a resource manager.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

HTTP methods

GET, POST

GET /api/v1/managers-management/managers

Use this method to return a list of all resource managers.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET `https://{orchestrator_server_IP}/api/v1/managers-management/managers`

Query parameters

This REST API supports query parameters for paginating, filtering, sorting, including data, and excluding data in the response. For more information about these common query parameters, see Paginating, scoping, filtering, sorting, including data, and excluding data in responses. For a list of supported attributes, see GET /api/v1/managers-management/managers/{id}.

The following example returns a list of all resource managers.
GET `https://192.0.2.0/api/v1/managers-management/managers`

The following example returns a list of all unhealthy resource managers.
GET `https://192.0.2.0/api/v1/managers-management/managers`
`?filterNotEquals[][attributes]=healthState&filterNotEquals[][values]=Normal`

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.
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).

Attributes		Type	Description
results		Array of objects	Information about each resource manager
	id	String	Manager ID
	connectTimestamp	String	Timestamp when the resource manager was registered with the orchestrator server 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.

Attributes		Type	Description
healthState		String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
name		String	Resource manager name
type		String	Type of resource manager. This can be the following value. • **XClarity Management Hub 2.0** • **XClarity Management Hub** • **XClarity Administrator** • **XClarity Orchestrator** • **Schneider EcoStruxure IT** • **VMware vRealize Operations Manager**
_links		Object	Resource URI (see Links)
_ui		Object	Information about UI-specific attributes
	healthStateKey	String	Health state key. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
_metadata		Object	Request metadata (see Metadata)

The following example is returned if the request is successful.

```
{
    "results": [{
        "id": "53788A673607458DA14766162020FDAD",
        "connectTimestamp": "2022-08-02T03:21:20.079Z",
        "healthState": "Normal",
        "name": "10.241.54.10",
        "type": "XClarity Administrator",
        "_links": {
            "rel": "self",
            "uri": "/api/v1/managers-management/managers/53788A673607458DA14766162020FDAD"
        },
        "_ui": {
            "healthStateKey": "Normal"
        }
    },
    ...,
    {
        "type": "XClarity Orchestrator",
        "healthState": "Normal",
        "id": "00000000000000000000000000000000",
        "name": "XClarity Orchestrator",
        "_links": {
            "rel": "self",
```

```
            "uri": "/api/v1/managers-management/managers/00000000000000000000000000000000"
        },
        "_ui": {
            "healthStateKey": "Normal"
        }
    }],
    "_metadata": {...}
}
```

POST /api/v1/managers-management/managers

Use this method to connect (register) one XClarity Management Hub 2.0 or XClarity Management Hub management hubs, or connect one or more Schneider Electric EcoStruxure IT Expert, VMware vRealize Operations Manager, and Lenovo XClarity Administrator resource managers.

When connecting multiple managers, a job is created to complete this request. The response header returns the URI for the job in the **Location** field.

When connecting multiple managers, a successful response code indicates that the job was successfully transmitted and accepted by the orchestrator. 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 Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{orchestrator_server_IP}*/api/v1/managers-management/managers

Query parameters

None

Request body

Table 10. XClarity Management Hub 2.0 or XClarity Management Hub management hub

Attributes	Re-quired / Optional	Type	Description
registrationRequest	Required	String	Registration key that is generated by the management hub

Table 11. EcoStruxure IT Expert resource managers

Attributes	Re-quired / Optional	Type	Description
managers		Required	Array of objects	Information about each resource manager
	authentication		Required	Object	Information about authentication settings
		token	Required	String	Token value
		type	Required	String	Authentication type. This is always **token**.

Table 11. EcoStruxure IT Expert resource managers (continued)

Attributes			Re-quired / Optional	Type	Description
connection			Optional	Object	Information about connection settings
	url		Optional	String	Resource manager URL
name			Required	String	Resource manager name
type			Required	String	Type of resource manager. This is always **Schneider EcoStruxure IT**.

Table 12. vRealize Operations Manager resource managers

Attributes			Re-quired / Optional	Type	Description
managers			Required	Array of objects	Information about each resource manager
	authentication		Required	Object	Information about authentication settings
		authSource	Optional	String	Name of the authentication source for users and groups To obtain a list of available authorization sources, use GET /api/v1/connector/vrealizeAuthSources.
		password	Required	String	Password to use for basic authentication
		type	Required	String	Authentication type. This is always **basic**.
		username	Required	String	username to use for basic authentication
	connection		Required	Object	Information about connection settings
		hostname	Required	String	Resource manager host name
		port	Required	Integer	Resource manager port
	hubID		Required	String	ID of the XClarity Management Hub used to manage this manager
	type		Required	String	Type of resource manager. This is always **vRealize Operations Manager**

Table 13. XClarity Administrator resource managers

Attributes			Re-quired / Optional	Type	Description
managers			Required	Array of objects	Information about each resource manager
	authentication		Required	Object	Information about authentication settings
		password	Required	String	Password to use for basic authentication
		type	Required	String	Authentication type. This is always **basic**.
		username	Required	String	Username to use for basic authentication
	connection		Required	Object	Information about connection settings

Table 13. XClarity Administrator resource managers (continued)

Attributes			Re-quired / Optional	Type	Description
		hostname	Required	String	Resource manager host name
		port	Required	Integer	Resource manager port
	options		Required	Object	Information about options
		enableDriveAnalyticsData	Required	Boolean	Indicates whether drive analytics data collection is enabled. This can be one of the following values. • **true**. Drive analytics data collection is enabled. • **false**. Drive analytics data collection is disabled. **Note:** This attribute is supported by XClarity Administrator v3.3 and later.
	type		Required	String	Type of resource manager. This is always **XClarity Administrator**.

The following example connects to a management hub.

```
{
   "registrationRequest": "eyJzZWxmSW5mbyI6eyJ1dWlkIjoiMjNjODdmMGEtMmNiNiOOOTEwLTk3NDgtOTE5MzQON2E
                           2NTVjIiwiaG9zdG5hbWUiOiJ4aG1jMTkOIiwiZG9tYWluIjoibGFicy5sZW5vdm8uY29tIi
                           wiZnFkbiI6InhobWMxOTQubGFicy5sZW5vdm8uY29tIiwiaXBBZGRyZXNzZXMiOlsiMTAuM
                           jQzLjIuMTA3Il0sInZlcnNpb24iOiIzLjYuMCIsImJ1aWxkIjoiNDEiLCJodWJJWZXJzaW9u
                           IjoiMS4wLjAifSwiY3NyIjoiLSOtLS1CRUdJTiBDRVJUSUZQOFURSBSRVFVRVNULSOtLS1
                           cbk1JSUVOekNDQXA4QOFRQXdjVMTUFrOExVVUCaE1DVlZeEN6QUpCZO5WQkFnTUFFrNU
                           RNUkF3RGdZRFZRUUhcbkRBZFNZV3hsYVdkkO1ROHdEUVlEVlFSORBWk1aVzV2Zm84eEREQ
                           UtCZO5WQkFzTUEwbFFSSekVsTUNNROExVUVCbkF3d2NUMjRnYOhKbGJHaphaUOJuWVhSbGdQ
                           RjVJSFJ2SUhAdmNuVmhRRENDQWlJd0RRWUpLb1pJaHZjTkFRUUN
                           nb0NNnZ0lCUQ1kSO1UcFNzRFRuVlVlSloxa1JLc1ZCCUhhHNktGYkRlYmhVSU5akgxWFRcbl
                           htMWhncEQyTDVuaO5sVUN1ejdMSTJOOVBLYkxWOEV1T2kxcUl1L3diR3dQMzArcU1qUjl1U
                           EorLOFUcXNUVUWNcbkFFY1lFSOkOcWM4YnlKaOZYN25qa3hpbkbDBQMEp6cDBzTjh3WUJTUlNE
                           SnBFOTd4dGtZZcHNIaEFFYRFNpYTlPamVcbit3cERRnTDBBRemR5TGg5djIwaVMrS21rQzE2Szc
                           yZzZmMFgwROp1Zk1YZE5hR25zK1Q4TXNVZ3YwUUo1MTY5L3dcblY2TnVTbXVvVTM4QlY4Rn
                           lwUWxTYXQwaGt5M1lEMldhY3pnaU5tUUUyd0JaQWpqQUtTL3pIYm1LVnnQ4a3kvUlpcbmtza
                           ktsS2V4UUcvUnl6ZGVyaTREV2dzMVhkZWtJaNVFYNjYwcStwYmkwUVhtND VNSGFqMnAvOVN2
                           Q2FBRlBhTUtcbk5qTkRCWWkhYdOoORTNpdlFXK3NTVkRqajJCbVY3bXZadTVOWkdpDKzEydy9
                           xU2tVMW4VbDFObHhUTStvV3pqRjBBclBSZGlwbC1SZlgwWVZCbklSeUdaMGdpeL1BHTUVtVlVZRmY2Y1
                           BIQWhlMmlOZVVxTWxxZEZnVVS2xVeGUyMOhDaUZlbL2ZOL2tcblh3N2NyVVVgrL1daTnRRdXZUUa
                           3hwUHovMVBiL3k0cWQ3YThGeWVWTnNUYWxhbOVrb1lIc3AOZ1d5d2dGbFMOYXRcbjF5Sno3
                           bzNiUmVZZcnNKRzlQeFY3V2O4b1hiSCtZTFlyY1FkM1hsbWg3OWtySOkOSElWRXo4SHNIOWY
                           zbWptTnlcbmlZZlMvRFVOVkdtdD2t4aENVVd0hKRDJ6cER66eS9qYkQzbVJnRnZ6RzlNR2p5eF
                           NlREhVVM1M2NGUyaWw5TE5RQzVcbkFnTUJBQUdnQURBTkJna3Foa2lHOXcwQkFRc0ZBQU9DAQ
                           WdFQUYxYmowwS3libUJyR2VzWjRxYTFFFXODlkYkh6QVRcbnFGGVRacVpkkdFoxYlluU2c29HUmFG
                           YXgzc0tUTWJuZmgyaaEtnQm1KMUUZ3ZUx0elFSQ3hqZEJJQOQzZU5zSOJhUUNcbjRMQmxxYWGp
                           tSmYyMDBzRkgyN3htL1NvSnlFRE1UQ1Y5jdkFZUUCswZUlRUEJDd2ZpVmFIYWpJK1l3ZlNTYW
                           lNelZcbnJyMzU1ZHlxMFJMOEljNzU5S2VoTWZpTWhiTlF4UOkOOUJPejNSMW9RQ2xlblMzW
                           llYS1FCcFE1dnRibHHpKZEhcbnNOcHU4ZEs0YnY2Tm5iUU8vT3U2Mm99SR3h5d1B6SUhRRWpQ
                           SFkrOHMwNXBqcnBibGRRONlljQUlwZEMxdW1PS1VcbjFQWCctoY2lLNnI0YzRnN2JicW91MEt
                           VNmdDUUxwMGJiZ0xDUlldIYOo1Vk92T1VrbO44UWthb09QaO5aa1Jyck9cbllFSmExQXB5YT
                           Uwb0oreUlTcO5ENGtsdjFhSOxvWTlDalV6K0pLYXVoNOO4VVRmaFFuSFFkYO9XNVF4dWlCY
                           U5cbmxxjVOVONOxTMVIvUjk4ekdqOXY4WEoxNnNNKYUc1ajdaZUc3OG1DDazNERTRNdGJUZUpW
                           K2VwVSt8BaytWbWp6WWp6WDRcbmcg1c1FDaGxjRm96NWVlLOMvQWFoakJLL2tHQ1h1h1T1k2S3dvU1B
                           OK0xLQTFFOMFRrNnlend3SEJIRHI4dkVVCMjJjbkddzOVFqcjJZaVJGZjVwYnc2YVZVWVFpXOE
                           1MdUpuRHRSSXWwdzhzdmp3dmFxenFzVVXsNnNRRZDVlVjjdzdmWTRcbnlPRjNEV21qK25na
                           mZtTOhaS1hEckFFTUXF4dDlZNTF2RnViMmlUTjlxSORZU2cxQWpJS2wySXVnNDRQdjB1aXFc
                           blNwNWo4dGJJcXB0ck5OND1cbi0tLS0tRU5EIENFUlRJRklDQVRFIFJFUVVFU1QtLSOtLVx
                           uIiwicHVibGljS2V5IjoiLSOtLS1CRUdJTiBQVUJMSUMgS0VZLSOtLS1cbk1JSUNJakFOQm
```

```
                    drcWhraUc5dzBCQVFFRkFBTONBZzhBTUlJQONnSONBZOVBeHhGbONsVWpkMFJLLOFmSXhpR
                    Stcbk9CNmdsdGhBZ1JCNzFWS3FnWElPWWY5UEtVYmVlZjAzdWtDU2hTWjFtZOdXSmorUXll
                    cXNSZDBVZHRjNCs5dmdcbkFSbW4ramZOaHFGbjVmMFpNZUNNbHcrcGh4SOh1ZHlvQUEyTCt
                    IMHBlenhzWVZDUkpWeHduTzVGQXVqU3hieVJcbmNtVWt6eWRxTjQOOEdZUXdnYkRDMDBjb1
                    BBRGxsYXdrODV6MmIwK2NmZG1VbGU4VUd3dzh3L21zWmNUbFBqVkFcbk1FWGZodHFKYUhia
                    2pDZlh5eml6RnZtanJYdDRBbitwb1lmSGYvdGlWWmQ1STBXaTBpNXR4d3pPWkxVYTZvWHhc
                    bmxhSmtpMFN3bmlmUVIyWE9pVCttV1hTRWlTQ3pZMWtwbDg5RnorQUdYMExhTjJkNFFuWFJ
                    xclVmTmFhTlNpbVBcblFzUDFxdGpQQVDRxcjdWSHlMQ1drQjIOWjlOVzFHNGROVWVZMDJwaO
                    dJVXVwbmlwemR6UU1tOGZ5UHBFQTlNQVFcblc2SEN5RWdwdzR2eDJESWNKWE84ZDhRWWUxL
                    OgxTzU1ZOdYSGZ2Z1F1ekJUdEgOcU9uTWZ1WmxGQ3N4eStQbVZcbmNYUDRyWWU4cVBJRzdw
                    MjFCWEgydFhiNHkxZVpPUmZqa1E3TGw5ZmRudkFRYVgvMW8vQVRSNlpveFBTZEE5WXZcbnc
                    3UkpzeElIWmg1RUFzT1RadXJppczkyVORjZ1kwTnJSRFFJUkNNYUOxzZGVSUOxzSTF6ZWRVbm
                    NpNWtYKONIU1pcbmJHdVBBNWhPK3BEdnhQOUQ4UkRSNWpJWDNTb21KOXNoNVpYaONnakdmQ
                    WE4eU55a3k4dGdlN3hYUVJOSSs5aUhcbml5U2FJMHpyb1Bjb1V1cEx5TkxKRkpzQOF3RUFB
                    UTO9XG4tLSOtLUVORCBQVUJMSUMgSOVZLSOtLS1cbiJ9",
```
}

The following example connects to a EcoStruxure IT Expert, vRealize Operations Manager, and XClarity
Administrator resource manager.
```
{
    "managers": [{
        "authentication": {
            "token": "AK1/2sixskmmcO6wj/1i6v3epcz5c25rc29jv1tOOhce1pjahyobux63 ",
            "type": "token"
        },
        "connection": {
            "url": "https://api.ecostruxureit.com/rest/v1/organizations"
        },
        "name": "Croco 1",
        "type": "Schneider EcoStruxure IT"
    },
    {
        "authentication": {
          "authSource": "All vCenter Servers",
          "password": "*********",
          "type": "basic",
          "username": "USERID"
        },
        "connection": {
          "hostname": "10.241.54.100",
          "port": 443
        },
        "hubID": "B7DE58431234C23839398F3AD4873923",
        "type": "vRealize Operations Manager"
    },
    {
        "authentication": {
            "password": "CME44len",
            "type": "basic",
            "username": "USERID"
        },
        "connection": {
            "hostname": "10.241.54.102",
            "port": 443
        },
        "options": {
            "enableDriveAnalyticsData": true
        },
        "type": "XClarity Administrator"
    }]
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. A descriptive error message is returned in the response body.

Response header

When connecting multiple managers, the URI and ID of the root job are returned in the **Location** and **JobID** fields respectively.

Response body

For XClarity Management Hub resource managers, when the request is successful, the following attribute is returned. If the request fails, standard message attributes are returned. For all other resource managers, standard message attributes are always returned (see Status messages).

Attributes	Type	Description
registrationKey	String	Registration key that is generated by Lenovo XClarity Orchestrator to complete the connection to the management hub To complete the connection, import the registration key in the XClarity Management Hub by clicking **Administration → Hub Configuration**, and clicking **Install Registration Key**, entering the registration key, and then clicking **Submit**.

The following example is returned if the request is successful.

```
{
   "registrationKey": "0DF4-0110-E231",
}
```

/api/v1/managers-management/managers/*{id}*

Use this REST API to return information about a specific resource manager or to delete a specific resource manager.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

HTTP methods

GET, DELETE

GET /api/v1/managers-management/managers/*{id}*

Use this method to return information about a specific resource manager.

Note: This REST API requires Lenovo XClarity Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/i/v1/managers-management/managers/*{id}*

where *{id}* is the ID of the resource manager. To obtain the manager IDs, use GET /api/v1/managers-management/managers.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. 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).

Attributes		Type	Description
id		String	Resource-manager ID
authenticationKey		String	(Lenovo XClarity Management Hub and Lenovo XClarity Administrator only) Authentication key
authSource		String	(vRealize Operations Manager only) Name of the authentication source for users and groups To obtain a list of available authorization sources, use GET /api/v1/connector/vrealizeAuthSources.
connectTimestamp		String	Timestamp when the manager was registered with the orchestrator server 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.
connection		Object	Information about connection settings
	hostname	String	Manager host name
	port	Integer	Manager port number
	url	Integer	(EcoStruxure IT Expert) Manager port number
groups		Array of objects	Information about each group in which this manager is a member
	id	String	Group ID
	name	String	Group name
	type	String	Group type. This value is always **ManagerGroup**.

Attributes	Type	Description
healthState	String	Health state (translated). This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**
hubID	String	(vRealize Operations Manager only) Management Hub ID to use to connect the resource manager
issues	Array of strings	Reason for an unhealthy status If **healthState** is **Normal**, this attribute is set to an empty array. If **healthState** is not Normal, this attribute can be one or more of the following values. • **InvalidCredentials** • **ConnectionProblems**
lastInventorySyncTimestamp	String	Timestamp when the portal last refreshed the inventory for the manager 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.
lastSyncTimestamp	String	Timestamp when portal last refreshed the information about the manager 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.
name	String	Resource manager name to use for basic authentication
options	Object	(Lenovo XClarity Management Hub and XClarity Administrator only) Information about applicable options
enableDriveAnalyticsData	Boolean	Indicates whether drive analytics-data collection is enabled. This can be one of the following values. • **true**. The component can be updated. • **false**. The component cannot be updated.
properties	Object	Information about the resource manager properties
build	Integer	Manager build number
buildNumber	Integer	Manager build number
forwarderID	String	(Lenovo XClarity Management Hub and XClarity Administrator only) ID of the event forwarder in XClarity Administrator that pushes events to this XClarity Orchestrator instance
metricsSubscriptionID	String	(Lenovo XClarity Management Hub and XClarity Administrator only) ID of the metrics subscription in XClarity Administrator that pushes metrics to this XClarity Orchestrator instance
networkSettings	Object	(Lenovo XClarity Management Hub and XClarity Administrator only) Manager network settings
domainName	String	Manager domain name
hostname	String	Manager host number

Attributes			Type	Description
	ipv4Addresses		Array of strings	List of IPv4 addresses for the manager
	ipv6Addresses		Array of strings	List of IPv6 addresses for the manager
	uuid		String	Manager UUID
	version		String	Manager version number
	versionNumber		Integer	Manager version number
type			String	Type of manager. This can be one of the following values. • **XClarity Management Hub 2.0** • **XClarity Management Hub** • **XClarity Administrator** • **Schneider EcoStruxure IT** • **VMware vRealize Operations Manager**
updates			Object	(Lenovo XClarity Management Hub and XClarity Administrator only) Information about current software updates
	components		Array of objects	Information about updates on each component
		componentID	String	Component ID
		name	String	Component name
		targetVersion	Object	Information about the target update for the component based on the assigned policy If a policy is not assigned, this value is null.
		identifier	String	Version identifier
		number	String	Version number
		releaseTimestamp	String	Timestamp when the update was released 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.
		upgradeable	Boolean	Indicates whether the component can be updated. This can be one of the following values. • **true**. The component can be updated. • **false**. The component cannot be updated.
		version	Object	Information about current version
		identifier	String	Version identifier
		number	String	Version number
		releaseTimestamp	String	Timestamp when the update was released 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.
	identifier		String	Update identifier
	policy		Object	Information about the assigned update policy
		id	String	Policy ID If a policy is not assigned to the manager, this value is null.

Attributes		Type	Description
	name	String	Policy name If a policy is not assigned to the manager, this value is **No Assignment**.
	policyState	String	Update policy state (translated) • **No Policy Assigned** • **Policy Assigned**
	policyStateKey	String	Update policy state key • **NoPolicyAssigned** • **PolicyAssigned**
_links		Object	Resource URI (see Links)
_ui		Object	Information about UI-specific attributes
	healthStateKey	String	Health state key. This can be one of the following values. • **Normal** • **Non-Critical** • **Warning** • **Minor-Failure** • **Major-Failure** • **Non-Recoverable** • **Critical** • **Unknown**

The following example is returned if the request is successful for a Lenovo XClarity Management Hub resource manager.

```
{
   "id": "53788A673607458DA14766162020FDAD",
   "authenticationKey": "53788A673607458DA14766162020FDAD",
   "connectTimestamp": "2022-08-02T03:21:20.079Z",
   "connection": {
      "hostname": "10.241.54.10",
      "port": 443
   },
   "groups": [],
   "healthState": "Normal",
   "issues": [],
   "lastInventorySyncTimestamp": "2022-08-02T17:53:35.322Z",
   "lastSyncTimestamp": "2022-08-02T03:21:20.079Z",
   "name": "10.241.54.10",
   "options": {
      "enableDriveAnalyticsData": false
   },
   "properties": {
      "build": "108",
      "buildNumber": 108,
      "forwarderID": "1659410478081",
      "metricsSubscriptionID": "62e8982fcdd22d416d86f82e",
      "networkSettings": {
         "domainName": "",
         "hostname": "localhost",
         "ipv4Addresses": ["10.241.54.10"],
         "ipv6Addresses": ["fd64:30d9:58db:5bbc:0:0:0:1e10","fe80:0:0:0:250:56ff:fe8b:2320"]
      },
      "uuid": "53788A673607458DA14766162020FDAD",
      "version": "1.0.0",
      "versionNumber": 100
   },
```

```
    "type": "Lenovo XClarity Management Hub",
    "updates": {
        "components": [{
            "componentID": "lxca",
            "name": "Lenovo XClarity Management Hub 1.0.0",
            "targetVersion": null,
            "upgradeable": true,
            "version": {
                "identifier": "108",
                "number": "1.0.0",
                "releaseTimestamp": null
            },
        }],
        "identifier": "lxca",
        "policy": {
            "id": null,
            "name": "No Assignment"
        },
        "policyState": "No Policy Assigned",
        "policyStateKey": "NoPolicyAssigned"
    },
    "_links": {
        "rel": "self",
        "uri": "/api/v1/managers-management/managers/53788A673607458DA14766162020FDAD"
    },
    "_ui": {
        "healthStateKey": "Normal"
    }
}
```

The following example is returned if the request is successful for a EcoStruxure IT Expert resource manager.

```
{
    "id": "b17c3accec1e2a94e28b108ed757a6705c77066d",
    "connectTimestamp": "2021-02-16T12:36:40.809Z",
    "connection": {
        "url": "https://api.ecostruxureit.com/rest/v1/organizations"
    },
    "details": {
        "build": null,
        "uuid": null,
        "version": null,
        "versionNumber": null
    },
    "groups": [],
    "healthState": "Normal",
    "healthStateKey": "Normal",
    "issues": [],
    "lastInventorySyncTimestamp": null,
    "lastSyncTimestamp": "2021-02-16T12:36:40.809Z",
    "name": "Demo Ecox manager1",
    "type": "Schneider EcoStruxure IT",
    "updates": null,
    "_links": {
        "rel": "self",
        "uri": "/api/v1/connector/managers/b17c3accec1e2a94e28b108ed757a6705c77066d"
    }
}
```

The following example is returned if the request is successful for a vRealize Operations Manager resource manager.

```json
{
    "id": "b17c3accec1e2a94e28b108ed757a6705c77066d",
    "authSource": "",
    "connectTimestamp": null,
    "connection": {
        "hostname": "10.241.54.100",
        "port": 443
    },
    "groups": [],
    "healthState": "Normal",
    "hubID": "1234",
    "issues": [],
    "lastInventorySyncDate": null,
    "lastSyncTimestamp": null,
    "name": "vRealize Operations Manager",
    "properties": {
        "uuid": "21A727A22EECA0B85DCE38F16C7CEB1F",
        "build": "41",
        "buildNumber": 41,
        "version": "1.4.0",
        "versionNumber": 140
    },
    "type": "vRealize Operations Manager",
    "_links": {
        "rel": "self",
        "uri": "/api/v1/managers-management/managers/b17c3accec1e2a94e28b108ed757a6705c77066d"
    },
    "_ui": {
        "healthStateKey": "Normal"
    }
}
```

DELETE /api/v1/managers-management/managers/*{id}*

Use this method to delete a specific resource manager.

An asynchronous job is created to complete this request. The response header returns the job URI and job ID.

A successful response code indicates that the job was successfully transmitted and accepted by the hub. 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 Orchestrator v2.0 or later.

Authentication

Authentication with username and password is required.

Resource URI

DELETE https://*{orchestrator_server_IP}*/api/v1/managers-management/managers/*{id}*

where *{id}* is the ID of the resource manager. To obtain the manager IDs, use GET /api/v1/managers-management/managers.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
404	Not found	The resource cannot be found. A descriptive error message is returned in the response body.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

Chapter 6.   Jobs

The following REST APIs are available for managing jobs.

/api/v1/jobs-management/schedules

Use this REST API to return a list of all scheduled jobs or to create a scheduled job.

Note: This REST API requires Lenovo XClarity Orchestrator v2.1 or later.

HTTP methods

GET, POST

GET /api/v1/jobs-management/schedules

Use this method to return a list of all scheduled jobs.

Note: This REST API requires Lenovo XClarity Orchestrator v2.1 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/jobs-management/schedules

Query parameters

This REST API supports query parameters for paginating, filtering, sorting, including data, and excluding data in the response. For more information about these common query parameters, see Paginating, scoping, filtering, sorting, including data, and excluding data in responses. For a list of supported attributes, see GET /api/v1/jobs-management/schedules/*{id}*.

The following example returns all scheduled firmware-update jobs.
```
GET https://192.0.2.0/jobs-management/schedules
?filterEquals[0][attributes]=metadata.method&filterEquals[0][values]=POST
&filterContains[1][attributes]=method.path&filterContains[1][values]=updates
```

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. The request completed successfully. If a query parameter is specified and the value of that parameter has no matches, the response body returns default values. The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.
400	Bad Request	A query parameter 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

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes			Type	Description
results			Array of objects	Information about each scheduled job
	id		String	Scheduled job ID
	createdBy		String	Name of the user that created the schedule
	creationTimestamp		String	Timestamp when the scheduled job 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.
	jobID		String	Job ID
	launchedTimestamp		String	Timestamp when the scheduled job ran 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.
	metadata		Object	Information about the operation to be performed for this job
		body	Object	Request body of the operation
		method	String	Method. This value is always **POST**.
		path	String	URI of the operation, including query parameters
	status		String	Job status (translated). For a job with subtasks, this is most severe status of all subtsaks. This can be one of the following values. • **Cancelled**. The schedule was canceled. • **Error**. An error prevented the job from running on schedule.. • **Launched**. The job ran on schedule. • **Pending**. The job is scheduled for a later time.
	statusKey		String	Job status key. For a job with subtasks, this is most severe status of all subtsaks. This can be one of the following values. • **cancelled**. The schedule was canceled. • **error**. An error prevented the job from running on schedule.. • **launched**. The job ran on schedule. • **pending**. The job is scheduled for a later time.

Attributes		Type	Description
	scheduleTimestamp	String	Timestamp when the scheduled job is to run 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.
	title	String	Scheduled job title
	_links	Object	Resource URI (see Links)
_metadata		Object	Request metadata (see Metadata)

```
{
    "results": {
        "id": "c3047feb4ad44ba2b956950c812ce36e",
        "createdBy": "user1",
        "creationTimestamp": "2024-01-29T17:41:03.429Z",
        "jobID": "156",
        "launchedTimestamp": "2024-01-29T17:41:08.355Z",
        "metadata": {
            "method": "POST",
          "path": "/api/v1/updates-management/updates",
            "body": {
                "activationRule": "ImmediateActivation",
                "forceUpdate": false,
                "groupIDs": [],
                "installPrerequisiteFirmware": false,
                "resourceIDs": [ "CFEC7691C59F3613A1D47ABA0113C99C-5B421B48D19F46FBAD1A20F620D670D2" ],
                "updateRule": "ContinueOnError"
            }
        },
        "scheduleTimestamp": "2024-01-10T13:00:00.000Z",
        "status": "Launched",
        "statusKey": "launched",
        "title": "test",
        "_links": {
            "rel": "self",
            "uri": "/api/v1/jobs-management/schedules/c3047feb4ad44ba2b956950c812ce36e"
        },
    "_metadata": {}
}
```

POST /api/v1/jobs-management/schedules

Use this method to create a scheduled job.

Note: This REST API requires Lenovo XClarity Orchestrator v2.1 or later.

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{orchestrator_server_IP}*/api/v1/jobs-management/schedules

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
metadata	Required	Object	Information about the operation to be performed for this job
body	Required	Object	Request body of the operation
method	Required	String	Method. This value is always **POST**.
path	Required	String	URI of the operation, including query parameters
scheduleTimestamp	Required	String	Timestamp when the scheduled job is to run 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.
title	Required	String	Scheduled job title

The following example creates a scheduled firmware-update job.

```
{
    "metadata": {
        "body": {
            "activationRule": "ImmediateActivation",
            "forceUpdate": false,
            "groupIDs": [],
            "installPrerequisiteFirmware": false,
            "resourceIDs": ["CFEC7691C59F3613A1D47ABA0113C99C-5B421B48D19F46FBAD1A20F620D670D2"],
            "updateRule": "ContinueOnError"
        },
        "method": "POST",
        "path": "/api/v1/updates-management/updates"
    },
    "scheduleTimestamp": "2024-01-10T13:00:00.000Z",
    "title": "test"
}
```

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.
500	Internal Server Error	An internal error occurred. A descriptive error message is returned in the response body.

Response header

The URL of the scheduled job is returned in the "Location" field.

Response body

Attributes	Type	Description
{message_attributes}	varies	Status messages (see Status messages)

/api/v1/jobs-management/schedules/*{id}*

Use this REST API to return information about or cancel a specific schedule job.

Note: This REST API requires Lenovo XClarity Orchestrator v2.1 or later.

HTTP methods

GET, DELETE

GET /api/v1/jobs-management/schedules/*{id}*

Use this method to return information about a specific schedule job.

Note: This REST API requires Lenovo XClarity Orchestrator v2.1 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/api/v1/jobs-management/schedules/*{id}*

where *{id}* is the ID of the scheduled job. To obtain the scheduled job ID, use GET /api/v1/jobs-management/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.
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).

Attribute	Type	Description
id	String	Scheduled job ID
createdBy	String	Name of the user that created the schedule
creationTimestamp	String	Timestamp when the scheduled job 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.

Attribute	Type	Description
jobID	String	Job ID
launchedTimestamp	String	Timestamp when the scheduled job ran 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.
metadata	Object	Information about the operation to be performed for this job
body	Object	Request body of the operation
method	String	Method. This value is always **POST**.
path	String	URI of the operation, including query parameters
status	String	Job status (translated). For a job with subtasks, this is most severe status of all subtsaks. This can be one of the following values. • **Cancelled**. The schedule was canceled. • **Error**. An error prevented the job from running on schedule.. • **Launched**. The job ran on schedule. • **Pending**. The job is scheduled for a later time.
statusKey	String	Job status key. For a job with subtasks, this is most severe status of all subtsaks. This can be one of the following values. • **cancelled**. The schedule was canceled. • **error**. An error prevented the job from running on schedule.. • **launched**. The job ran on schedule. • **pending**. The job is scheduled for a later time.
scheduleTimestamp	String	Timestamp when the scheduled job is to run 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.
title	String	Scheduled job title
_links	Object	Resource URI (see Links)

```
{
    "id": "c3047feb4ad44ba2b956950c812ce36e",
    "createdBy": "user1",
    "creationTimestamp": "2024-01-29T17:41:03.429Z",
    "jobID": "156",
    "launchedTimestamp": "2024-01-29T17:41:08.355Z",
    "metadata": {
        "method": "POST",
        "path": "/api/v1/updates-management/updates",
        "body": {
            "activationRule": "ImmediateActivation",
            "forceUpdate": false,
            "groupIDs": [],
            "installPrerequisiteFirmware": false,
            "resourceIDs": [ "CFEC7691C59F3613A1D47ABA0113C99C-5B421B48D19F46FBAD1A20F620D670D2" ],
            "updateRule": "ContinueOnError"
        }
    },
    "scheduleTimestamp": "2024-01-10T13:00:00.000Z",
    "status": "Launched",
    "statusKey": "launched",
    "title": "test",
    "_links": {
```

```
        "rel": "self",
        "uri": "/api/v1/jobs-management/schedules/c3047feb4ad44ba2b956950c812ce36e"
    }
}
```

DELETE /api/v1/jobs-management/schedules/*{id}*

Use this method to cancel a scheduled job that is in the Pending state.

Note: This REST API requires Lenovo XClarity Orchestrator v2.1 or later.

Authentication

Authentication with username and password is required.

Resource URI

DELETE https://*{orchestrator_server_IP}*/api/v1/jobs-management/schedules/*{id}*

where *{id}* is the ID of the scheduled job. To obtain the scheduled job ID, use GET /api/v1/jobs-management/schedules.

Query parameters

Done

Request body

Done

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter 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	The 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_attributes}	*varies*	Status messages (see Status messages)

Chapter 7. Resource management

The following REST APIs are available for managing resources, such as power-on operations, remote control, and offline management.

/api/v1/knowledge/devices/*{id}*

Use this REST API to unmanage a specific device that is managed offline.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

HTTP methods

GET

DELETE /api/v1/knowledge/devices/*{id}*

Use this method to unmanage a specific device that is managed offline.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

DELETE https://*{orchestrator_server_IP}*/api/v1/knowledge/devices/*{id}*

where *{id}* is the UUID or ID of the device. To obtain the device UUID and IDs, use GET /api/v1/data/devices.

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	The resource cannot be found. 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.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

Chapter 8. Analytics

The following REST APIs are available for analyzing data metrics.

/api/v1/customAlerts/metrics

Use this REST API to return a list of metrics that can be used in custom alert rules.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

HTTP methods

GET

GET /customAlerts/metrics

Use this method to return a list of metrics that can be used in custom alert rules.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{orchestrator_server_IP}*/customAlerts/metrics

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Attributes		Type	Description
results		Array of objects	Information about each metric
	metric	String	Metric name
	sampleRate	Integer	Rate, in seconds, at which the metrics values are recorded
_links		Object	Resource URI (see Links)

The following example is returned if the request is successful.

```
{
    "results": [{
        "metric": "cpu_temp",
        "sampleRate": "60"
    },
    {
        "metric": "cpu_utilization",
        "sampleRate": "30"
    }],
    "_links": {
        "rel": "self",
        "uri": "/api/v1/customAlerts/metrics"
    }
}
```

/api/v1/customAlerts/rules

Use this REST API to return a list of all custom alert rules or to create a custom alert rule.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

HTTP methods

GET, POST

GET /api/v1/customAlerts/rules

Use this method to return a list of all custom alert rules.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://*{management_server_IP>*/api/v1/customAlerts/rules

Query parameters

This REST API supports query parameters for paginating, filtering, sorting, including data, and excluding data in the response. For more information about these common query parameters, see Paginating, scoping, filtering, sorting, including data, and excluding data in responses. For a list of supported attributes, see GET /api/v1/customAlerts/rules/*{id}*.

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully. If a single query parameter is specified and the value of that parameter has no matches, the response body returns default values. If a list of query parameters is specified and the value of at least one parameter has no matches, the response body returns only what matches.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Table 14. Event-based alert rules

Attributes		Type	Description
results		Array of objects	Information about each custom analytics alert
	id	String	Rule ID
	alertDescription	String	Additional information to clarify the reason for the alert
	alertMsg	String	Message string for the alert
	alertUserAction	String	User actions that can be taken to recover from the alert
	eventCode	String	Four-digit number that uniquely identifies the alert and event When an alert is raised based on a custom alert rule, an event is also raised. The same event code is used for both the active alert and the event using the format FQXXOCAxxxxc, where *xxxx* is the four-digit unique identifier and *c* is the severity.
	criteria	Object	Criteria for raising an alert
	count	Integer	Number of times that the event must occur in the specified interval before an alert is raised
	eventID	String	ID of the event that triggers an alert
	interval	Integer	Period of time, in minutes, in which the event occurs before an alert is raised
	mode	String	Indicates whether the rule applies to a device or device group. This can be one of the following values. • **device**. Raises an alert when the event occurs on any device. The device name is included in this alert. • **group**. Raises an alert when the event occurs on a device in any device group. The group name is included in the alert.
	description	String	Rule description
	name	String	Rule name
	severity	String	Alert severity (translated). This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
	severityKey	String	Alert severity key. This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
	status	String	Rule status (translated). This can be one of the following values. • **enabled** (default) • **disabled**
	statusKey	String	Rule status key. This can be one of the following values. • **enabled** (default) • **disabled**
	type	String	Rule type (translated). For event-based alert rules, this is always **event**.

Table 14. Event-based alert rules (continued)

Attributes	Type	Description
typeKey	String	Rule type key. For event-based alert rules, this is always **event**.
_links	Object	Rule URI (see Links)
_metadata	Object	Request metadata (see Metadata)

The following example is returned for an event-based rule if the request is successful.

```
{
    "results": [{
        "id": "046b6c7fc0b8ac43b9db35dd6489e6dfffff",
        "alertDescription": "",
        "alertMsg": "",
        "alertUserAction": "",
        "eventCode": "FQXXOCA0001J",
        "criteria": {
            "count": 5,
            "eventID": "FQXHMDIO107G",
            "interval": 1440,
            "mode": "device"
        },
        "description": "Server management fails 5 times in a 24-hour period",
        "enabled": true,
        "name": "Server managment failures",
        "severity": "Warning",
        "severityKey": "Warning",
        "status": "enabled",
        "statusKey": "enabled",
        "type": "event",
        "typeKey": "event",
        "_links": {
            "rel": "self",
            "uri": "/api/v1/customAlerts/rules/046b6c7fc0b8ac43b9db35dd6489e6dfffff"
        }
    }],
    "_metadata": {...}
}
```

Table 15. Metric-based alert rules

Attributes	Type	Description
results	Array of objects	Information about each custom analytics alert
id	String	Rule ID
alertDescription	String	Additional information to clarify the reason for the alert
alertMsg	String	Message string for the alert
alertUserAction	String	User actions that can be taken to recover from the alert
eventCode	String	Four-digit number that uniquely identifies the alert and event. When an alert is raised based on a custom alert rule, an event is also raised. The same event code is used for both the active alert and the event using the format `FQXXOCAxxxxc`, where *xxxx* is the four-digit unique identifier and *c* is the severity.
criteria	Object	Criteria for raising an alert

Table 15. Metric-based alert rules (continued)

Attributes			Type	Description
		operator	String	Comparison operator to use when comparing the value of **metric** against the specified **threshold**. This can be one of the following values. • **gt**. Greater than • **gte**. Greater than or equal to • **lte**. Less than or equal to • **lt**. Less than
		count	Integer	(Count mode only) Minimum amount of time, in seconds, that the limit is breached before an alert is raised
		interval	Integer	(Average and count modes only) Period of time, in seconds, in which the measurement is evaluated
		threshold	Integer	Threshold to be met for raising an alert
		metric	String	Metric for which the value is to be evaluated
		mode	String	Criteria mode. This can be one of the following values. • **average**. Raises an alert when the average value of the metric breaches the threshold (based on the comparator) during a specific interval. For example, you can create a rule to raise an alert when the average CPU Temperature (**metric**) during a 24-hour period (**interval**) is greater than (**operator**) 40 degrees C (**threshold**). • **count**. Raises an alert when the metric breaches the threshold (based on the comparator) a certain number of times during a specific interval. For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**) for 5 times (**count**) in a 24-hour period (**interval**). • **simple**. Raises an alert when the metric breaches the threshold (based on the comparator). For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**).
	description		String	Rule description
	name		String	Rule name
	severity		String	Alert severity (translated). This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
	severityKey		String	Alert severity key. This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
	status		String	Rule status (translated). This can be one of the following values. • **enabled** (default) • **disabled**
	statusKey		String	Rule status key. This can be one of the following values. • **enabled** (default) • **disabled**

Table 15. Metric-based alert rules (continued)

Attributes		Type	Description
	type	String	Rule type (translated). For event-based alert rules, this is always **metric**.
	typeKey	String	Rule type key. For event-based alert rules, this is always **metric**.
	_links	Object	Rule URI (see Links)
_metadata		Object	Request metadata (see Metadata)

The following example is returned for a metric-based rule if the request is successful.

```
{
    "results": [{
        "id": "046b6c7fc0b8ac43b9db35dd6489e6daee91",
        "alertDescription": "",
        "alertMsg": "",
        "alertUserAction": "",
        "eventCode": "FQXX0CA0002J",
        "criteria": {
            "operator": "gt",
            "count": 5,
            "interval": 1440,
            "threshold": 5,
            "metric": "CPUTemp",
            "mode": "count"
        },
        "description": "CPU Temperature greater than 40 C for 5 times in 24-hours",
        "name": "High CPU temperatures",
        "severity": "Warning",
        "severityKey": " Warning ",
        "status": "enabled",
        "statusKey": " enabled ",
        "type": "metric",
        "typeKey": "metric",
        "_links": {
            "rel": "self",
            "uri": "/api/v1/customAlerts/rules/046b6c7fc0b8ac43b9db35dd6489e6daee91"
        }
    }],
    "_metadata": {…}
}
```

POST /api/v1/customAlerts/rules

Use this method to create a custom alert rule for raising custom analytics alerts.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

POST https://*{management_server_IP>*/api/v1/customAlerts/rules

Query parameters

None

Request body

Table 16. Event-based alert rules

Attributes	Re-quired / Optional	Type	Description
alertDescription	Optional	String	Additional information to clarify the reason for the alert
alertMsg	Required	String	Message string for the alert
alertUserAction	Optional	String	User actions that can be taken to recover from the alert
eventCode	Required	String	Event code that uniquely identifies the alert and event When an alert is raised based on a custom alert rule, an event is also raised. The same event code is used for both the active alert and the event using the format `FQXXOCAxxxxc`, where *xxxx* is the unique identifier and *c* is the severity.
criteria	Required	Object	Criteria for raising an alert
count	Required	Integer	Number of times that the event must occur in the specified interval before an alert is raised
eventID	Required	String	ID of the event that triggers an alert To obtain a list of event IDs, see Event and alert messages in the XClarity Orchestrator online documentation.
interval	Required	Integer	Period of time, in minutes, in which the event occurs before an alert is raised
mode	Required	String	Indicates whether the rule applies to a device or device group. This can be one of the following values. • **device**. Raises an alert when the event occurs on any device. The device name is included in this alert. • **group**. Raises an alert when the event occurs on a device in any device group. The group name is included in the alert.
description	Optional	String	Rule description
name	Required	String	Rule name
severityKey	Required	String	Alert severity key. This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
statusKey	Required	String	Rule status key. This can be one of the following values. • **enabled** (default) • **disabled**
typeKey	Required	String	Rule type key. For event-based alert rules, this is always "event".

The following example creates an event-based rule that raises an alert when server management fails 5 times in a 24-hour period.

```
{
    "alertDescription": "",
    "alertMsg": "",
    "alertUserAction": "",
    "eventCode": "FQXXOCA0001J",
```

```
    "criteria": {
        "count": 5,
        "eventID": "FQXHMDI0107G",
        "interval": 1440,
        "mode": "device"
    },
    "description": "Server management fails 5 times in a 24-hour period",
    "enabled": true,
    "name": "Server managment failures",
    "severityKey": "Warning",
    "statusKey": "enabled",
    "typeKey": "event"
}
```

Table 17. Metric-based alert rules

Attributes	Re-quired / Optional	Type	Description
alertDescription	Optional	String	Additional information to clarify the reason for the alert
alertMsg	Required	String	Message string for the alert
alertUserAction	Optional	String	User actions that can be taken to recover from the alert
eventCode	Required	String	Four-digit number that uniquely identifies the alert and event When an alert is raised based on a custom alert rule, an event is also raised. The same event code is used for both the active alert and the event using the format `FQXX0CAxxxxc`, where *xxxx* is the four-digit unique identifier and *c* is the severity.
criteria	Required	Object	Criteria for raising an alert
operator	Required	String	Comparison operator to use when comparing the value of **metric** against the specified **threshold**. This can be one of the following values. • **gt**. Greater than • **gte**. Greater than or equal to • **lte**. Less than or equal to • **lt**. Less than
count	Required when **mode** is "count"	Integer	(Count mode only) Minimum amount of time, in seconds, that the limit is breached before an alert is raised
interval	Required when **mode** is "aver-age" or "count"	Integer	(Average and count modes only) Period of time, in seconds, in which the measurement is evaluated
threshold	Required	Integer	Threshold to be met for raising an alert
metric	Required	String	Metric for which the value is to be evaluated To obtain a list of metrics, use GET /customAlerts/ metrics.

Table 17. Metric-based alert rules (continued)

Attributes	Re-quired / Optional	Type	Description
mode	Required	String	Criteria mode. This can be one of the following values. • **average**. Raises an alert when the average value of the metric breaches the threshold (based on the comparator) during a specific interval. For example, you can create a rule to raise an alert when the average CPU Temperature (**metric**) during a 24-hour period (**interval**) is greater than (**operator**) 40 degrees C (**threshold**). • **count**. Raises an alert when the metric breaches the threshold (based on the comparator) a certain number of times during a specific interval. For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**) for 5 times (**count**) in a 24-hour period (**interval**). • **simple**. Raises an alert when the metric breaches the threshold (based on the comparator). For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**).
description	Optional	String	Rule description
name	Required	String	Rule name
severityKey	Required	String	Severity key. This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
statusKey	Required	String	Rule status key. This can be one of the following values. • **enabled** (default) • **disabled**
typeKey	Required	String	Rule type key. For metric-based alert rules, this is always "metric".

The following example creates a metric-based rule that raises the CPU Temperature of any device exceeds 40 degrees C for 5 times within a 24-hour period.

```
{
    "alertDescription": "",
    "alertMsg": "",
    "alertUserAction": "",
    "id": "046b6c7fc0b8ac43b9db35dd6489e6daee91",
    "eventCode": "FQXXOCA0002J",
    "criteria": {
        "operator": "gt",
        "count": 5,
        "interval": 1440,
        "threshold": 5,
        "metric": "CPUTemp",
        "mode": "count"
```

```
    },
    "description": "CPU Temperature greater than 40 C for 5 times in 24-hours",
    "name": "High CPU temperatures",
    "severityKey": " Warning ",
    "statusKey": " enabled ",
    "typeKey": "metric"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter 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 header

The URL of the custom analytics alert is returned in the "Location" field.

Response body

Attributes	Type	Description
{message_attributes}	varies	Status messages (see Status messages)

/api/v1/customAlerts/rules/{id}

Use this REST API to return information about a specific custom alert rule, or modify a custom alert rule, or enable, disable, or delete one or more custom alert rules.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

HTTP methods

GET, PUT, PATCH, DELETE

GET /api/v1/customAlerts/rules/{id}

Use this method to return information about a specific custom alert rule.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

GET https://{management_server_IP>/api/v1/customAlerts/rules/{id}

where *{id}* is the ID of the custom analytics alert. To obtain the alert ID, use GET /api/v1/customAlerts/rules.

Query parameters

None

Request body

None

Response codes

Code	Description	Comments
200	OK	The request completed successfully.

Response body

When the request is successful, the following attributes are returned. If the request fails, standard message attributes are returned (see Status messages).

Table 18. Event-based alert rules

Attributes	Type	Description
id	String	Rule ID
alertDescription	String	Additional information to clarify the reason for the alert
alertMsg	String	Message string for the alert
alertUserAction	String	User actions that can be taken to recover from the alert
eventCode	String	Four-digit number that uniquely identifies the alert and event When an alert is raised based on a custom alert rule, an event is also raised. The same event code is used for both the active alert and the event using the format FQXXOCA*xxxxc*, where *xxxx* is the four-digit unique identifier and *c* is the severity.
criteria	Object	Criteria for raising an alert
count	Integer	Number of times that the event must occur in the specified interval before an alert is raised
eventID	String	ID of the event that triggers an alert
interval	Integer	Period of time, in minutes, in which the event occurs before an alert is raised
mode	String	Indicates whether the rule applies to a device or device group. This can be one of the following values. • **device**. Raises an alert when the event occurs on any device. The device name is included in this alert. • **group**. Raises an alert when the event occurs on a device in any device group. The group name is included in the alert.
description	String	Rule description
name	String	Rule name
severity	String	Alert severity (translated). This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
severityKey	String	Alert severity key. This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
status	String	Rule status (translated). This can be one of the following values. • **enabled** (default) • **disabled**

Table 18. Event-based alert rules (continued)

Attributes	Type	Description
statusKey	String	Rule status key. This can be one of the following values. • **enabled** (default) • **disabled**
type	String	Rule type (translated). For event-based alert rules, this is always **event**.
typeKey	String	Rule type key. For event-based alert rules, this is always **event**.
_links	Object	Rule URI (see Links)

The following example is returned for an event-based rule if the request is successful.

```
{
   "id": "046b6c7fc0b8ac43b9db35dd6489e6dfffff",
   "alertDescription": "",
   "alertMsg": "",
   "alertUserAction": "",
   "eventCode": "FQXXOCA0001J",
   "criteria": {
      "count": 5,
      "eventID": "FQXHMDIO107G",
      "interval": 1440,
      "mode": "device"
   },
   "description": "Server management fails 5 times in a 24-hour period",
   "enabled": true,
   "name": "Server managment failures",
   "severity": "Warning",
   "severityKey": "Warning",
   "status": "enabled",
   "statusKey": "enabled",
   "type": "event",
   "typeKey": "event",
   "_links": {
      "rel": "self",
      "uri": "/api/v1/customAlerts/rules/046b6c7fc0b8ac43b9db35dd6489e6daee91"
   }
}
```

Table 19. Metric-based alert rules

Attributes	Type	Description
id	String	Rule ID
alertDescription	String	Additional information to clarify the reason for the alert
alertMsg	String	Message string for the alert
alertUserAction	String	User actions that can be taken to recover from the alert
eventCode	String	Four-digit number that uniquely identifies the alert and event When an alert is raised based on a custom alert rule, an event is also raised. The same event code is used for both the active alert and the event using the format FQXXOCA*xxxxc*, where *xxxx* is the four-digit unique identifier and *c* is the severity.
criteria	Object	Criteria for raising an alert

Table 19. Metric-based alert rules (continued)

Attributes	Type	Description
operator	String	Comparison operator to use when comparing the value of **metric** against the specified **threshold**. This can be one of the following values. • **gt**. Greater than • **gte**. Greater than or equal to • **lte**. Less than or equal to • **lt**. Less than
count	Integer	(Count mode only) Minimum amount of time, in seconds, that the limit is breached before an alert is raised
interval	Integer	(Average and count modes only) Period of time, in seconds, in which the measurement is evaluated
threshold	Integer	Threshold to be met for raising an alert
metric	String	Metric for which the value is to be evaluated
mode	String	Criteria mode. This can be one of the following values. • **average**. Raises an alert when the average value of the metric breaches the threshold (based on the comparator) during a specific interval. For example, you can create a rule to raise an alert when the average CPU Temperature (**metric**) during a 24-hour period (**interval**) is greater than (**operator**) 40 degrees C (**threshold**). • **count**. Raises an alert when the metric breaches the threshold (based on the comparator) a certain number of times during a specific interval. For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**) for 5 times (**count**) in a 24-hour period (**interval**). • **simple**. Raises an alert when the metric breaches the threshold (based on the comparator). For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**).
description	String	Rule description
name	String	Rule name
severity	String	Alert severity (translated). This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
severityKey	String	Alert severity key. This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
status	String	Rule status (translated). This can be one of the following values. • **enabled** (default) • **disabled**
statusKey	String	Rule status key. This can be one of the following values. • **enabled** (default) • **disabled**

Table 19. Metric-based alert rules (continued)

Attributes	Type	Description
type	String	Rule type (translated). For event-based alert rules, this is always **metric**.
typeKey	String	Rule type key. For event-based alert rules, this is always **metric**.
_links	Object	Rule URI (see Links)

The following example is returned for a metric-based rule if the request is successful.

```
{
   "id": "046b6c7fc0b8ac43b9db35dd6489e6daee91",
   "alertDescription": "",
   "alertMsg": "",
   "alertUserAction": "",
   "eventCode": "FQXXOCA0002J",
   "criteria": {
      "operator": "gt",
      "count": 5,
      "interval": 1440,
      "threshold": 5,
      "metric": "CPUTemp",
      "mode": "count"
   },
   "description": "CPU Temperature greater than 40 C for 5 times in 24-hours",
   "name": "High CPU temperatures",
   "severity": "Warning",
   "severityKey": " Warning ",
   "status": "enabled",
   "statusKey": " enabled ",
   "type": "metric",
   "typeKey": "metric",
   "_links": {
      "rel": "self",
      "uri": "/api/v1/customAlerts/rules/046b6c7fc0b8ac43b9db35dd6489e6daee91"
   }
}
```

PUT /api/v1/customAlerts/rules/*{id}*

Use this method to modify a specific custom alert rule.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

PUT https://*{management_server_IP>*/api/v1/customAlerts/rules/*{id}*

where *{id}* is the ID of the custom analytics alert. To obtain the alert ID, use GET /api/v1/customAlerts/rules.

Query parameters

None

Request body

This PUT request updates the entire resource. To clear a value, set the attribute to null (if applicable). If an array is specified, the entire array is replaced (unless stated otherwise). If an optional attribute is not specified, that attribute is not changed. If an immutable (unchangeable) attribute is specified, it is ignored.

Table 20. Event-based alert rules

Attributes	Required / Optional	Type	Description
alertDescription	Optional	String	Additional information to clarify the reason for the alert
alertMsg	Required	String	Message string for the alert
alertUserAction	Optional	String	User actions that can be taken to recover from the alert
eventCode	Required	String	Event code that uniquely identifies the alert and event When an alert is raised based on a custom alert rule, an event is also raised. The same event code is used for both the active alert and the event using the format `FQXXOCAxxxxc`, where *xxxx* is the unique identifier and *c* is the severity.
criteria	Required	Object	Criteria for raising an alert
count	Required	Integer	Number of times that the event must occur in the specified interval before an alert is raised
eventID	Required	String	ID of the event that triggers an alert To obtain a list of event IDs, see Event and alert messages in the XClarity Orchestrator online documentation.
interval	Required	Integer	Period of time, in minutes, in which the event occurs before an alert is raised
mode	Required	String	Indicates whether the rule applies to a device or device group. This can be one of the following values. • **device**. Raises an alert when the event occurs on any device. The device name is included in this alert. • **group**. Raises an alert when the event occurs on a device in any device group. The group name is included in the alert.
description	Optional	String	Rule description
name	Required	String	Rule name
severityKey	Required	String	Alert severity key. This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
statusKey	Required	String	Rule status key. This can be one of the following values. • **enabled** (default) • **disabled**
typeKey	Required	String	Rule type key. For event-based alert rules, this is always "event".

The following example creates an event-based rule that raises an alert when server management fails 5 times in a 24-hour period.

```
{
    "alertDescription": "",
    "alertMsg": "",
    "alertUserAction": "",
    "eventCode": "FQXXOCA0001J",
    "criteria": {
        "count": 5,
        "eventID": "FQXHMDIO107G",
        "interval": 1440,
        "mode": "device"
    },
    "description": "Server management fails 5 times in a 24-hour period",
    "enabled": true,
    "name": "Server managment failures",
    "severityKey": "Warning",
    "statusKey": "enabled",
    "typeKey": "event"
}
```

Table 21. Metric-based alert rules

Attributes	Required / Optional	Type	Description
alertDescription	Optional	String	Additional information to clarify the reason for the alert
alertMsg	Required	String	Message string for the alert
alertUserAction	Optional	String	User actions that can be taken to recover from the alert
eventCode	Required	String	Four-digit number that uniquely identifies the alert and event When an alert is raised based on a custom alert rule, an event is also raised. The same event code is used for both the active alert and the event using the format FQXXOCA*xxxxc*, where *xxxx* is the four-digit unique identifier and *c* is the severity.
criteria	Required	Object	Criteria for raising an alert
operator	Required	String	Comparison operator to use when comparing the value of **metric** against the specified **threshold**. This can be one of the following values. • **gt**. Greater than • **gte**. Greater than or equal to • **lte**. Less than or equal to • **lt**. Less than
count	Required when **mode** is "count"	Integer	(Count mode only) Minimum amount of time, in seconds, that the limit is breached before an alert is raised
interval	Required when **mode** is "average" or "count"	Integer	(Average and count modes only) Period of time, in seconds, in which the measurement is evaluated
threshold	Required	Integer	Threshold to be met for raising an alert

Table 21. Metric-based alert rules (continued)

Attributes	Re- quired / Optional	Type	Description
metric	Required	String	Metric for which the value is to be evaluated To obtain a list of metrics, use GET /customAlerts/ metrics.
mode	Required	String	Criteria mode. This can be one of the following values. • **average**. Raises an alert when the average value of the metric breaches the threshold (based on the comparator) during a specific interval. For example, you can create a rule to raise an alert when the average CPU Temperature (**metric**) during a 24-hour period (**interval**) is greater than (**operator**) 40 degrees C (**threshold**). • **count**. Raises an alert when the metric breaches the threshold (based on the comparator) a certain number of times during a specific interval. For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**) for 5 times (**count**) in a 24-hour period (**interval**). • **simple**. Raises an alert when the metric breaches the threshold (based on the comparator). For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**).
description	Optional	String	Rule description
name	Required	String	Rule name
severityKey	Required	String	Severity key. This can be one of the following values. • **Warning**. User can decide if action is needed. • **Critical**. Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
statusKey	Required	String	Rule status key. This can be one of the following values. • **enabled** (default) • **disabled**
typeKey	Required	String	Rule type key. For metric-based alert rules, this is always "metric".

The following example creates a metric-based rule that raises the CPU Temperature of any device exceeds 40 degrees C for 5 times within a 24-hour period.

```
{
    "alertDescription": "",
    "alertMsg": "",
    "alertUserAction": "",
    "id": "046b6c7fc0b8ac43b9db35dd6489e6daee91",
    "eventCode": "FQXXOCA0002J",
    "criteria": {
        "operator": "gt",
        "count": 5,
        "interval": 1440,
```

```
        "threshold": 5,
        "metric": "CPUTemp",
        "mode": "count"
    },
    "description": "CPU Temperature greater than 40 C for 5 times in 24-hours",
    "name": "High CPU temperatures",
    "severityKey": " Warning ",
    "statusKey": " enabled ",
    "typeKey": "metric"
}
```

Response codes

Code	Description	Comments
200	OK	The request completed successfully.
400	Bad Request	A query parameter 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

Attributes	Type	Description
<message_attributes}	*varies*	Status messages (see Status messages)

PATCH /api/v1/customAlerts/rules/*{id_list}*

Use this method to enable or disable one or more custom alert rules.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

PATCH https://*{management_server_IP>*/api/v1/customAlerts/rules/*{id_list}*

where *{id_list}* is a list of custom alert rule IDs, separated by a comma. To obtain the alert rule IDs, use GET /api/v1/customAlerts/rules.

Query parameters

None

Request body

Attributes	Re-quired / Optional	Type	Description
op	Required	String	Action to take. This can be the following value. • **replace**. Replaces the entire attribute value with the specified value.
path	Required	String	Name of the attribute to be modified. This can be one of the following values. • **statusKey**. Enables or disables the custom alert rule. For more information about the attribute, see GET /api/v1/customAlerts/rules/*{id}*.
value	Required	*varies*	Attribute value, depending on the data type

The following example enable the specified custom alert rules.
```
[
   { "op": "replace", "path": "statusKey", "value": "enabled" }
]
```

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.
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.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)

DELETE /api/v1/customAlerts/rules/*{id_list}*

Use this method to delete one or more custom alert rules.

Note: This REST API requires Lenovo XClarity Orchestrator v1.3 or later.

Authentication

Authentication with username and password is required.

Resource URI

DELETE https://*{management_server_IP>*/api/v1/customAlerts/rules/*{id_list}*

where *{id_list}* is a list of custom alert rule IDs, separated by a comma. To obtain the alert rule IDs, use GET /api/v1/customAlerts/rules.

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.
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.

Response body

Attributes	Type	Description
{message_attributes}	*varies*	Status messages (see Status messages)