



Lenovo XClarity Administrator Problem Determination Guide



Version 4.0.0

First Edition (February 2023)

© Copyright Lenovo 2015, 2023.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Contents	i	Reporting XClarity Administrator problems	76
Summary of changes	v	Attaching a service file to an open service ticket	78
Chapter 1. Getting help and technical assistance	1	Viewing service tickets and status.	79
Chapter 2. Viewing alerts, events, and jobs	3	Transferring service files to Lenovo Support.	80
Placing devices in maintenance mode	3	Configuring management-server log settings	81
Working with alerts	4	Re-enabling Call Home on all managed devices	82
Viewing active alerts	4	Sending periodic data to Lenovo	82
Excluding alerts	8	Sample usage data	84
Resolving an alert	9	Sample hardware data	87
Acknowledging alerts.	10	Chapter 4. Managing disk space	103
Working with events	10	Chapter 5. Discovery and management issues	107
Monitoring events in the event log	10	Cannot discover a device	107
Monitoring events in the audit log	12	Cannot manage a device	108
Resolving an event	14	Cannot manage a storage device due to an invalid SSL/TSL certificate	110
Excluding events	14	Cannot manage a switch due to an invalid SSL/TSL certificate	111
Forwarding events	15	Cannot recover connectivity of a managed Flex System chassis after replacing the rear LED card or midplane assembly	111
Working with jobs	47	Cannot recover connectivity of a managed server after replacing the system board	111
Monitoring jobs	47	Encapsulation is not disabled after a server is unmanaged	112
Scheduling jobs	50	Compute node does not display in the user interface after management	112
Adding a resolution and comments to a job	53	Server power state is not correct	112
Chapter 3. Working with service and support.	55	Chapter 6. Installation, removal, update, and data migration issues	113
Getting bulletins from Lenovo	55	Video output does not display when installing XClarity Administrator in Red Hat KVM	113
Viewing warranty information	56	Adapter changes are not recognized	113
Setting up automatic problem notification	57	During initial setup, unable to open the initial setup wizard in a web browser	113
Setting up automatic problem notification to Lenovo Support (Call Home)	57	Lenovo XClarity Administrator deployment unexpectedly fails	113
Setting up automatic problem notification to the Lenovo Upload Facility.	62	Lenovo XClarity Administrator update has failed	114
Setting up automatic problem notification to a preferred service provider	66	Chapter 7. Connectivity issues	115
Changing the service-recovery password	68	Cannot access Lenovo XClarity Administrator	115
Inspecting service files	69	Cannot connect to Lenovo XClarity Administrator using Safari Browser	115
Defining the support contacts for specific devices	69	Cannot log in	115
Collecting and downloading service data for a device	70		
Collecting and downloading Lenovo XClarity Administrator service files	72		
Collecting and downloading service files for an unresponsive Lenovo XClarity Administrator	74		
Submitting a service request for hardware issues to the Lenovo Support Center	75		

Cannot log in to Lenovo XClarity Administrator	115
Password for a local recovery or supervisor user is forgotten	116
Cannot log in to the managed CMM directly	119
Cannot log in directly to the management controller	119
Cannot log in to managed Flex Power System servers	119
Sudden connectivity loss to a device	119

Chapter 8. Lenovo XClarity Administrator configuration issues121

External LDAP setup issues	121
User does not have sufficient authorization to configure servers	121
Features on Demand activation issues	121
VMware warning that VMXNET 3 driver is not supported	121

Chapter 9. Performance issues123

Lenovo XClarity Administrator performance issues	123
Poor or slow network performance	123

Chapter 10. Security issues125

SSL Certificate Cannot Be Trusted	125
Server certification validation fails	125
Samba and Apache vulnerabilities	126

Chapter 11. Troubleshooting backup and restore issues129

Backup process seems to hang during management server restart	129
XClarity Administrator window is blank after refreshing during backup	129

Chapter 12. Event monitoring and forwarding issues131

Events are not forwarded	131
------------------------------------	-----

Chapter 13. Device management issues133

Cannot securely erase drive data on frozen drives	133
Cannot securely erase SATA SDD volumes when connected to Marvel RAID	133
Inventory data is not up to date after adding or replacing cards	133

Chapter 14. Server configuration issues135

When creating a pattern from an existing server, an error is encountered	135
When deploying a pattern to a device, an activation error is encountered	135
An invalid configuration is deployed to a switch	136

Chapter 15. Firmware update and repository issues.137

Failed to connect to the Lenovo repository	137
After successful firmware update, Apply/Activate page does not show updated firmware versions	137
Cannot connect to fix central to download firmware updates	137
Cannot update firmware on a device	137
CMM Firmware Update Hangs	137
Firmware is up to date but fails the compliance check	138
Firmware updates to Flex System switches unexpectedly fail	138
Firmware update to Flex switch failed, indicating an error with the message “Firmware download operation failed.”	139
Firmware update to Flex switch failed, indicating an error with the message “DCSS_RC_CDT_FAIL”	139
Firmware update to Flex switch failed, indicating an error with the message “time out”	139
Firmware update to Flex switch failed, indicating an error with the message “Cannot download the same firmware version. Download another firmware.”	139
Firmware update to Flex switch failed, indicating an error with the message of failed to contact host	140
Firmware update to Flex switch failed, indicating an error with the message “file does not exist”	140
Firmware update to Flex switch failed, indicating an error with the message of “flashing ended with failure”	140
Firmware update to the EN6131 40 Gb Ethernet Switch or the IB6131 InfiniBand Switch fails unexpectedly	140
Firmware update to the Lenovo EN4091 pass-thru module fails	141
Firmware update to Flex System switch failed, indicating an error with the message of “Host Key Authentication failed”	141
When performing an update, the system fails to enter Maintenance Mode	141
Restarting a server from the operating system does not activate maintenance mode	141
Server running Red Hat Enterprise Linux (RHEL) does not restart	142

Chapter 16. OS device-driver update and repository issues.143

- Cannot connect to the Lenovo Support website to download device-driver updates 143
- Cannot update device drivers on a server. 143

Chapter 17. Operating system deployment issues.145

- Status reporting issues during OS deployment. . . 145
- Cannot deploy an operating system 145
- Cannot import a file into the OS-images repository 146
- OS installer cannot find the disk drive on which you want to install 147
- OS installer cannot boot on a ThinkServer server. 147
- VMware ESXi deployment issues 147
 - VMware deployment causes system hang or restart. 148
 - VMware deployment fails with disk errors . . . 148
 - Operating system does not reboot to complete ESXi deployment on a ThinkServer server 149
- Red Hat and SUSE Linux deployment issues . . . 149
 - Redhat 6.x cannot be deployed on rack-based server with static IP 149
 - OS deployment fails due to missing drivers 149
- Microsoft Windows deployment issues. 150
 - OS deployment fails due to existing system partitions on an attached disk drive 150

Chapter 18. Remote control issues151

- Remote-control session does not start 151
- Remote-control session hangs after login. 151

- Cannot connect to a server 152
- Cannot communicate with a Flex System switch after starting a remote-control session 152
- Cannot connect to a server in single-user mode 152
- Remote Control can connect to a server, but no video is available 152
- A server does not appear in the list for adding a new session 153
- State of server in remote-control session does not match state in the Lenovo XClarity Administrator. 153
- A drive or image cannot be mounted to a server. 153
- Storage media option is not shown in the list of remote media devices available for mounting . . . 154
- Power operation cannot be performed 154
- Video not available when connecting to Flex System x280 X6, x480 X6, and x880 X6 servers . . 154

Chapter 19. User interface issues. . .155

- Menu items, toolbar icons, and buttons are disabled (greyed out). 155
- Web browser becomes unresponsive when multiple tabs are open 155
- JSON response failed, parse error, and other unexpected errors 155
- User interface is not in the preferred language . . . 155
- Slow or seeming unresponsive load times, long wait to refresh, improper rendering 155
- Unexpected loss of data 156
- Device location changes are not reflected in the rack view 156
- Notices clvii
 - Trademarks clviii

Summary of changes

Follow-on releases of Lenovo XClarity Administrator management software support new hardware, software enhancements, and fixes.

Refer to the change history file (*.chg) that is provided in the update package for information about fixes.

There are no enhancements for problem determination and resolution in this version.

For information about changes in earlier releases, See [What's new](#) in the XClarity Administrator online documentation.


Chapter 1. Getting help and technical assistance

If you need help, service, or technical assistance for Lenovo XClarity Administrator, you can find a wide variety of sources available from Lenovo to assist you.

Before you begin

For general information about contact numbers, resources, and guidance to help you get the best support possible when and where you need it, see the [Lenovo Support Plan – Software webpage](#).

Procedure

- Submit ideas or provide feedback about XClarity Administrator by clicking the user-actions menu ( ADMIN_USER) on the XClarity Administrator title bar, and then clicking **Submit ideas** or **Submit feedback**.

You can also submit ideas and feedback from the Internet using the following links:


– [Lenovo XClarity Ideation website](#)

- Check the event log, and follow the suggested actions to resolve any event codes (see [Working with events](#)).
- Find solutions to problems that have identifiable symptoms, and follow the suggested actions to resolve any problems. For the latest troubleshooting procedures, see [Troubleshooting](#) in the XClarity Administrator online documentation.
- Check the [Lenovo Data Center Support website](#) for the latest tips and techniques that you can use to solve issues that you might have with XClarity Administrator. These *tech tips* provide procedures to work around issues that are related to the operation of XClarity Administrator.

To find tech tips that are available for your server:

1. Go to the [Lenovo Data Center Support website](#).
2. Enter “XClarity Administrator” in the **Search** field.
3. Either click **View All** in the **Top Articles** section to view all tips, or enter keywords in the **Search** field to find a specific tip.

Tip: You can sort the list by **Relevance**, **Popularity**, or **Newest** tips.

- Ask questions and find answers on the [Lenovo XClarity Community forum website](#) by clicking the user-actions menu ( ADMIN_USER) on the XClarity Administrator title bar, and then clicking **Visit forum**.
- If the problem is a hardware or baseboard management controller issue with a managed device, see the documentation that came with that device for information about problems and suggested actions.
 - For ThinkAgile appliances, see the [ThinkAgile online documentation](#).
 - For ThinkSystem products, including servers and network devices, see the [ThinkSystem online documentation](#).
 - For Converged, System x, and RackSwitch products, including servers and top-of-rack switches, see the [System x online documentation](#).
 - For NeXtScale products, see the [NeXtScale online documentation](#).
 - For Flex System products, including chassis, switches, storage devices, and compute nodes, see the [Lenovo Flex System online documentation](#).
- If the problem is with the XClarity Administrator management server, you can manually submit a service ticket (see [Reporting XClarity Administrator problems](#)).

- If the problem remains, and you are an entitled customer with a support-line contract, maintenance agreements, and/or warranty, submit an online service request.

Note: Lenovo XClarity Pro provides entitlement to service and support and the full-function-enablement license for XClarity Administrator. For information about purchasing Lenovo XClarity Pro, contact your Lenovo representative or authorized business partner.

Submitting a service request starts the process of determining a resolution to your problem by making the pertinent information available to Lenovo Support quickly and efficiently. Lenovo service technicians can start working on your resolution as soon as you have completed and submitted a request.

Note: If Call Home is configured and enabled, XClarity Administrator automatically opens a service ticket and transfers service files to the Lenovo Support Center when a serviceable event occurs on a managed device so that the issue can be addressed. For information about enabling Call Home, see [Setting up automatic problem notification to Lenovo Support \(Call Home\)](#).

If Call Home is not enabled, you can manually submit a service request and send service files (see [Submitting a service request for hardware issues to the Lenovo Support Center](#)).

Note: IBM is Lenovo's preferred service provider for XClarity Administrator. Service requests for some devices are forwarded to IBM for assistance.

- Through the Lenovo Support Line, you can get technical assistance, for a fee, for usage, configuration, and software problems with your Lenovo products.

To find the local and toll-free support phone numbers, see the [Support Phone List website](#). You can dial the number that you find for your geographical area or click **Contact Us** on the webpage to get assistance.

For severity 1 issues, support hours are 24/7. For all other severities, hours of operation and languages are listed on the webpage for your geographical area.

To contact product support in China, see the [Lenovo Services – China website](#). You can also call 400-106-8888 for product support. The call support is available Monday through Friday, from 9 AM - 6 PM.

Chapter 2. Viewing alerts, events, and jobs

Lenovo XClarity Administrator provides several methods that you can use to monitor the status of managed devices.

- The alerts list provides a real-time view of issues that have been identified with XClarity Administrator or any managed devices.
- The audit log and event log provide a historical view of user actions and events actions that have been identified by XClarity Administrator.
- The jobs log provides a list of longer running tasks that were performed against one or more managed devices.

Placing devices in maintenance mode

When a device is in maintenance mode, Lenovo XClarity Administrator excludes all events and alerts for that device from all pages on which events and alerts are displayed. Excluded alerts are still logged but are hidden from view.

About this task

Only events and alerts that were generated for a device while the device is in maintenance mode are excluded. Events and alerts were generated before the device was placed in maintenance mode are displayed.

Placing a managed device in maintenance and then back in service might cause inventory for that device to be out of date. If you see abnormalities, manually refresh the inventory from the device page by selecting the device and clicking **All Actions → Inventory → Refresh Inventory**.

Procedure

Complete one of the following steps to place devices in maintenance mode.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.
- Step 2. Click **Endpoint Actions** in the left navigation to display the Endpoint Actions page.
- Step 3. Select one or more devices to place in maintenance mode.
- Step 4. Click **Actions → Maintenance** to display the Maintenance mode dialog.
- Step 5. Select the date and time for taking the device out of maintenance mode and placing back in service.

Select **Indefinitely** if you do not want the device placed back in service.

- Step 6. Click **Confirm**. The maintenance column in the table changes to Yes for that device.

After you finish

When you are done with maintenance on the device, you can put the device back in service by selecting the device and clicking **Actions → Maintenance**, and then clicking **Turn off maintenance** in the dialog. If you do not manually place the device back in service mode, it is placed in service mode automatically after the specified end date and time expires.

Working with alerts

Alerts are hardware or management conditions that require investigation and user action. Lenovo XClarity Administrator polls the managed devices asynchronously and displays alerts that are received from those devices.

Learn more:  [XClarity Administrator: Monitoring](#)

About this task

Typically, when an alert is received, a corresponding event is stored in the event log. It is possible to have an alert without a corresponding event in the event log (even if the log wraps). For example, events that occur before you manage a chassis are not displayed in the event log. However, the alerts for the chassis are displayed in the alert log because Lenovo XClarity Administrator polls the CMM after the chassis has been managed.

Viewing active alerts

You can view a list of all active hardware and management alerts.

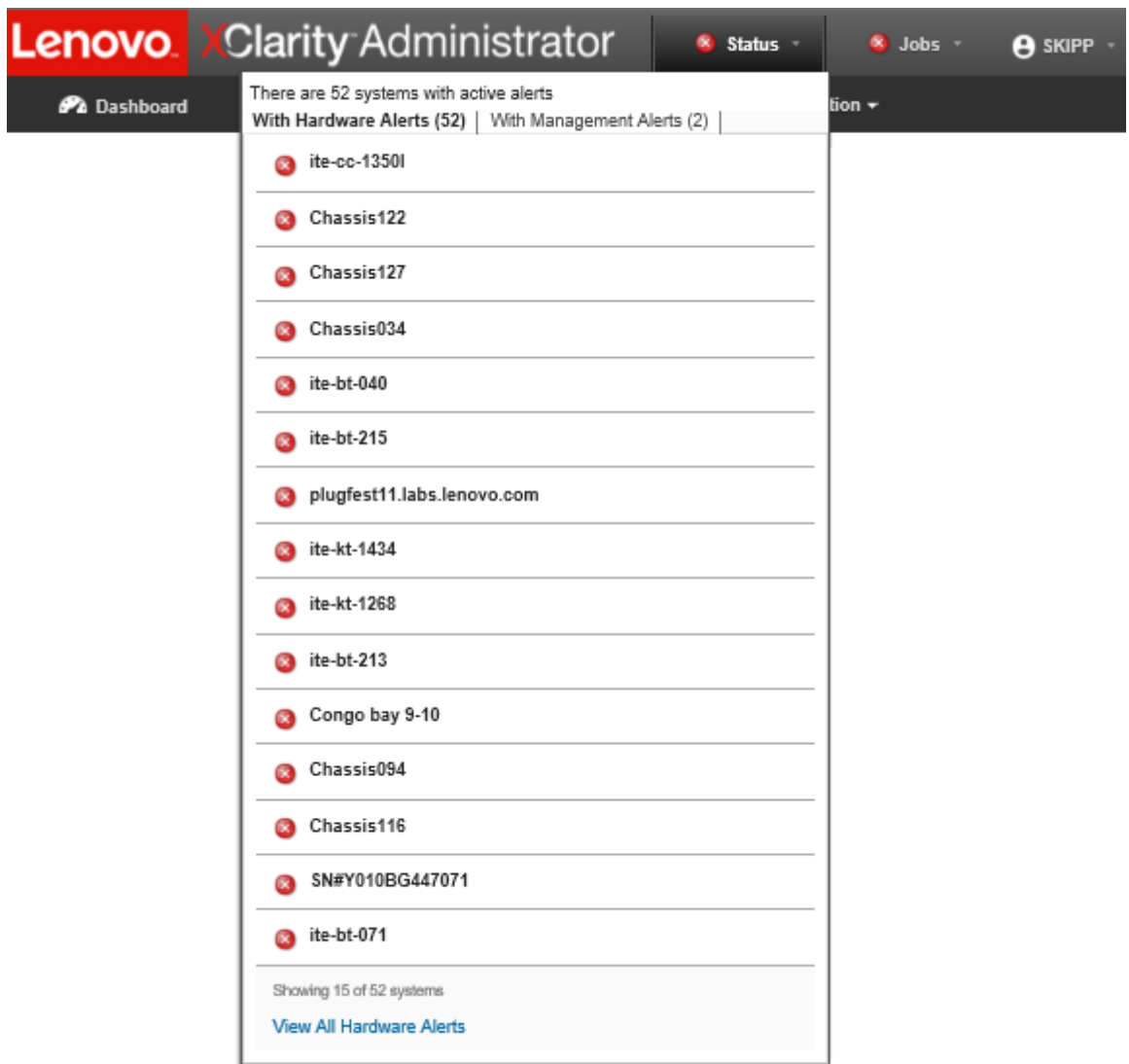
About this task

Note: Alerts for Lenovo Storage devices are presented only in English, even when the locale for Lenovo XClarity Administrator is set to another language. Use an external translation system to translate the messages manually, if needed.

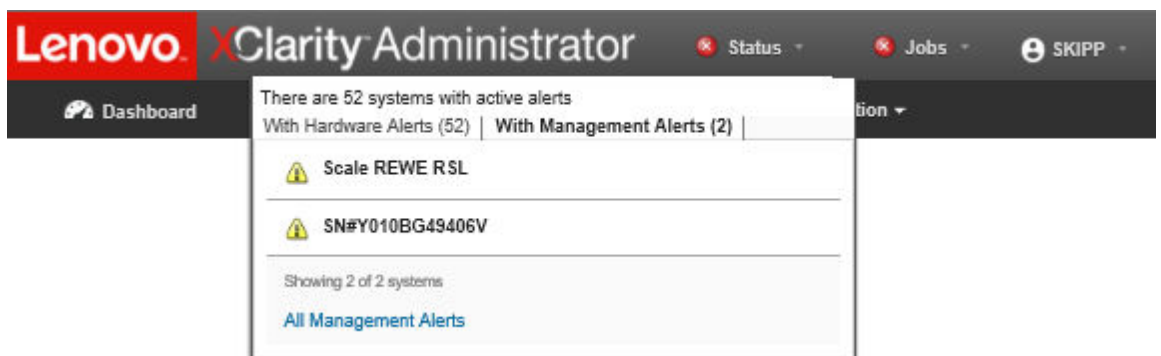
Procedure

Complete one of these procedures to view the active alerts.

- To view only alerts for managed devices (known as *hardware alerts*):
 1. From the XClarity Administrator title bar, click the **Status** pull-down to display a summary of hardware and management alerts.
 2. Click the **With Hardware Alerts** tab to see a summary of alerts for each managed device.



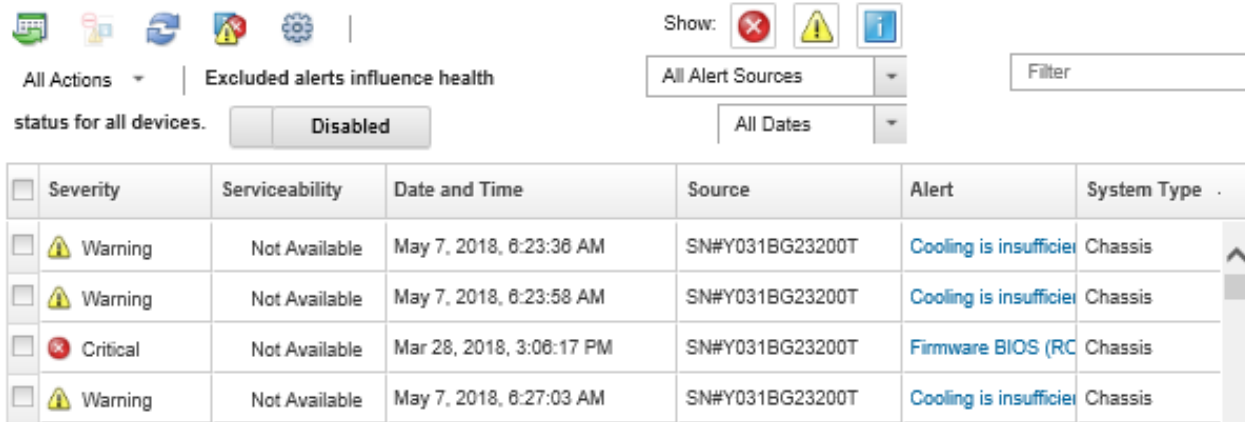
3. Hover the cursor over a device that is listed under that tab to display a list of alerts for that device.
 4. Click the **All Hardware Alerts** link to display the Alerts page with a filtered list of all hardware alerts.
- To view only alerts from XClarity Administrator (known as *management alerts*):
 1. From the XClarity Administrator title bar, click the **Status** pull-down to display a summary of hardware and management alerts.
 2. Click the **With Management Alerts** tab to see a summary of all CMM and XClarity Administrator alerts.







3. Hover the cursor over a device that is listed under that tab to display a list of alerts for that device.
 4. Click the **All Management Alerts** link to display the Alerts page with a filtered list of all CMM and XClarity Administrator alerts.
- To view all alerts in XClarity Administrator, click **Monitoring → Alerts** from the XClarity Administrator menu bar. The Alerts page is displayed with a list of all active alerts.

Alerts

 Alerts indicate hardware or management conditions that need investigation and user action.



<input type="checkbox"/>	Severity	Serviceability	Date and Time	Source	Alert	System Type
<input type="checkbox"/>	 Warning	Not Available	May 7, 2018, 8:23:38 AM	SN#Y031BG23200T	Cooling is insufficient	Chassis
<input type="checkbox"/>	 Warning	Not Available	May 7, 2018, 8:23:58 AM	SN#Y031BG23200T	Cooling is insufficient	Chassis
<input type="checkbox"/>	 Critical	Not Available	Mar 28, 2018, 3:06:17 PM	SN#Y031BG23200T	Firmware BIOS (RC)	Chassis
<input type="checkbox"/>	 Warning	Not Available	May 7, 2018, 8:27:03 AM	SN#Y031BG23200T	Cooling is insufficient	Chassis

- To view alerts for a specific device:
 1. From the XClarity Administrator menu bar, click **Hardware**, and then click a device type. A page is displayed with a tabular view of all managed devices of that type. For example, click **Hardware → Servers** to display the Servers page.
 2. Click a specific device to display the Summary page for the device.
 3. Under Status and Health, click **Alerts** to display a list of all alerts associated with that device.

Notes: The Serviceability column might show “Not Available” if:

- The alert on the device occurred before XClarity Administrator started managing it
- The event log has wrapped, and the event associated with that alert is no longer in the event log.

Chassis > SN#Y010BG49406V > SN#Y010BG49406V Details -

Alerts indicate hardware or management conditions that need investigation and user action.

Show:

All Alert Sources

All Dates

<input type="checkbox"/>	Severity	Serviceability	Date and Time	Alert
<input type="checkbox"/>	Warning	Not Required	Jan 12, 2018, 3...	Minimum SSL/TLS protoc

Results

From the Alerts page, you can perform the following actions:

- Refresh the list of alerts by clicking the **Refresh** icon ().

Tip: If new alerts are detected, the alerts log refreshes automatically every 30 seconds.




- View information about a specific alert (including an explanation and user action) and about the device that is the source of the alert (such as the Universally Unique Identifier) by clicking the link in the **Alert** column. A dialog with information about the alert properties and details is displayed.

Note: If the explanation and recovery actions for an alert are not displayed under the **Details** tab, go to [Lenovo Flex System online documentation](#), and search for the alert ID (for example, FQXHMSE00046). The website always provides the most up-to-date information.

- By default, excluded alerts do not influence the health status of managed devices. You can allow excluded alerts to influence the health status of managed devices from the Alerts page by clicking the toggle to enable **Excluded alerts influence health status for all devices**.
- You can set threshold preferences for raising an alert and event when a certain value, such as the life of an SSD in a ThinkSystem or ThinkServer server, exceeds a warning or critical level (see [Setting threshold preferences for generating alerts and events](#) in the XClarity Administrator online documentation).
- Export the alerts log by clicking the **Export as CSV** icon ().

Note: The timestamps in the exported log use the local time that is specified by the web browser.

- Exclude specific alerts from all pages on which alerts are displayed (see [Excluding alerts](#)).

- Narrow the list of alerts that are displayed on the current page:
 - Show or hide alerts of a specific severity by clicking the following icons:
 - **Critical alerts** icon ()
 - **Warning alerts** icon ()
 - **Informational alerts** icon ()
 - Show only alerts from specific sources. You can choose one of the following options from the drop-down list:
 - All Alert Sources
 - Hardware Events
 - Management Events
 - Service Center Events
 - Customer Serviceable Events
 - Non-serviceable Events
 - Show only alerts with a specific date and time. You can choose one of the following options from the drop-down list:
 - All Dates
 - Previous two hours
 - Previous 24 hours
 - Past Week
 - Past Month
 - List only alerts that contain specific text by entering the text in the **Filter** field.
 - Sort the alerts by column by clicking a column heading.

Excluding alerts

If there are specific alerts that are of no interest to you, you can exclude the alerts from all pages on which alerts are displayed. Excluded alerts are still in the log but are hidden from all pages on which alerts are displayed, including log views and device status.

About this task


Excluded alerts are hidden for all users, not just the user that set the configuration.

You can place devices in maintenance mode, so that all events and alerts for those devices are excluded (see [Placing devices in maintenance mode](#)).

Restriction: Only users with administrative authority can exclude or restore alerts.

Important: If you exclude status alerts, device status on the device summary and detailed pages does not change.

Procedure Complete the following steps to exclude alerts from the alerts log.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring** → **Alerts**. The Alerts page is displayed.
- Step 2. Select the alerts to be excluded, and click the **Exclude alerts** icon (). The Exclude Alerts dialog is displayed.
- Step 3. Select one of the following options:
 - **Exclude selected alerts from all systems.** Excludes the selected alerts from all managed devices.
 - **Exclude alerts only from systems in the scope of the instance selected.** Excludes the selected alerts from managed devices to which the selected alerts apply.

Step 4. Click **Save**.

After you finish

When you exclude alerts, Lenovo XClarity Administrator creates exclusion rules based on information that you provide. You can view a list of exclusion rules and excluded alerts from the Alerts page by clicking the **Show Excluded/Acknowledged Alerts** icon (🚩). In the Excluded/Acknowledged Alerts dialog, click the **Exclusion Rules** tab to view the list of exclusion rules or click the **Excluded Alerts** tab to view the list of excluded alerts.

Excluded Alerts

Exclusion Rules		Excluded Alerts	
🔍 Use the Remove button to remove exclusion rules and restore excluded alerts to the alert list.			
Filter			
<input type="checkbox"/> Alert	System	Alert ID	
<input type="checkbox"/> I/O module IO Module 04 is incompatible with the node configuration.	BlueA_3.16cmm	0EA0C004	
<input type="checkbox"/> Mismatched power supplies in the chassis: PS1 2505W, PS2 2505W, PS3 2104W, PS4 2505W, PS...	All	08216301	

By default, excluded alerts do not influence the health status of managed devices. You can allow excluded alerts to influence the health status of managed devices from the Alerts page by clicking the toggle to enable **Show Excluded/Acknowledged Alerts**.

You can restore alerts that have been excluded in the alerts log by removing the appropriate exclusion rule. To remove an exclusion rule, click the **Show Excluded Alerts** icon (🚩) to display the Excluded Alerts dialog, select the exclusion rules or excluded alert to restore, and click **Remove**.

Resolving an alert

Lenovo XClarity Administrator provides information about the appropriate actions to perform to resolve an alert.

Procedure Complete the following steps to resolve an alert.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Alerts** to display the Alerts page.
- Step 2. Locate the alert in the alerts log.
- Step 3. Click the link in the **Alert** column to view information about the alert (including an explanation and recovery actions) and properties for the device that is the source of the alert (such as the Universally Unique Identifier).
- Step 4. Complete the recovery actions that are listed under the **Details** tab to resolve the alert. The following example illustrates recovery actions for an event.

Change the security policy setting on the referenced managed chassis to match the current security policy on the management server.

To change the security policy on the chassis, open a command-line interface session on the Chassis Management Module (CMM) and run one of the following commands:

- To change the security policy level to `Secure`:

```
security -p secure -T mm[p]
```

- To change the security policy level to Legacy:

```
security -p legacy -T mm[p]
```

Note: If the explanation and recovery actions for an alert are not displayed under the **Details** tab, go to [Lenovo Flex System online documentation](#), and search for the alert ID (for example, FQXHMSE00046). The website always provides the most up-to-date information.


If you follow the recommended actions and the problem persists, contact Lenovo Support.

Acknowledging alerts




When an active alert is acknowledged, the alert is listed on pages on which alerts are displayed but does not affect the severity status for the applicable device.

Procedure

Complete the following steps to acknowledge an alert.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring** → **Alerts**. The Alerts page is displayed.
- Step 2. Select the alerts to be acknowledged.
- Step 3. Click the **Acknowledge alerts** icon ()

After you finish

- You can view a list of acknowledged alerts from the Alerts page by clicking the **Show Excluded/Acknowledged Alerts** icon () to display the Excluded/Acknowledged Alerts dialog, and then clicking the **Acknowledged alerts** tab.
- You can remove the acknowledge for an active alert by clicking the **Show Excluded/Acknowledged Alerts** icon () to display the Excluded/Acknowledged Alerts dialog, clicking the **Acknowledged alerts** tab, select the alerts, and then click the **Remove acknowledgement** icon ()

Working with events

From Lenovo XClarity Administrator, you have access to an event log and an audit log.

Learn more:  [XClarity Administrator: Monitoring](#)

About this task

The *event log* provides a historical list of all hardware and management events.

The *audit log* provides a historical record of user actions, such as logging in to Lenovo XClarity Administrator, creating a new user, and changing a user password. You can use the audit log to track and document authentication and controls in IT systems.

Monitoring events in the event log

The *event log* provides a historical list of all hardware and management events.

About this task

The event log contains informational and non-informational events. The number of each of these events varies until the maximum of 50,000 events is reached in the event log. At that point, there is a maximum of 25,000 informational and 25,000 non-information events. For example, there are 0 events in the event log initially. Assume events are received so that 20,000 informational events and 30,000 non-informational events are received. When the next event is received, the oldest informational event is discarded even if a non-informational event is older. Eventually, the log balances out so that there are 25,000 of each type of event.

Lenovo XClarity Administrator sends an event when the event log reaches 80% of the minimum size and another event when the sum of the event and audit logs reaches 100% of the maximum size.

Tip: You can export the event log to ensure that you have a complete record of all hardware and management events. To export the event log, click the **Export as CSV** icon (📄).

Procedure

To view the event log, click **Monitoring** → **Event Logs** from the Lenovo XClarity Administrator menu bar, and click the **Event Log** tab. The Event Log page is displayed.

Logs

Event Log
Audit Log

? The Event log provides a history of hardware and management conditions that have been detected.

Show:

All Event Sources ▼

Filter

All Actions ▼

All Dates ▼

No groups selected ▼

<input type="checkbox"/>	Severity	Serviceability	Date and Time ▼	Source	Event	System Type
<input type="checkbox"/>	Warning	Not Required	Jun 15, 2018, 9:12:40 AM	Management Server	The device	Management ^
<input type="checkbox"/>	Warning	Not Required	Jun 15, 2018, 9:12:40 AM	Management Server	Minimum SS	Management
<input type="checkbox"/>	Warning	Not Required	Jun 15, 2018, 9:12:39 AM	Management Server	Minimum SS	Management
<input type="checkbox"/>	Warning	Not Required	Jun 15, 2018, 9:10:50 AM	Management Server	The device	Management v

Total: 184 Selected: 0
◀ 1 2 3 ... 19 ▶
10 | 25 | 50 | 100 +

The **Serviceability** column identifies whether the device requires service. This column can contain one of the following values:

- **Not required.** The event is informational and does not require service.
- **User.** Take appropriate recovery action to resolve the issue.


To view information about a specific event, click the link in the **Event** column. A dialog is displayed with information about the properties for the device that sent the event, details about the event, and recovery actions.

- **Support.** If Call Home is enabled on Lenovo XClarity Administrator, the event is typically submitted to Lenovo Support Center unless an open service ticket for the same event ID already exists for the device.


If Call Home is not enabled, it is recommended that you manually open a service ticket to resolve the issue (see [Opening a service ticket](#) in the Lenovo XClarity Administrator online documentation).

Results




From the Event Log page, you can perform the following actions:

- View the source of the event by clicking the link in the **Source** column.
- Refresh the list of events by clicking the **Refresh** icon ().

Tip: The event log refreshes automatically every 30 seconds if new events are detected.

- Clear all events in the event log by selecting **All Actions** → **Clear event log**.
- View details about a specific event by clicking the link in the **Event** column and clicking the **Details** tab.
- Export the event log by clicking the **Export as CSV** icon ().

Note: The timestamps in the exported log use the local time that is specified by the web browser.

- Exclude specific events from all pages on which events are displayed (see [Excluding events](#)).
- Narrow the list of hardware and management events that are displayed on the current page:
 - Show or hide events of a specific severity by clicking the following icons from the drop-down list:
 - **Critical events** icon ()
 - **Warning events** icon ()
 - **Informational events** icon ()
 - Show only events from specific sources. You can choose one of the following options from the drop-down list:
 - All Alert Sources
 - Hardware Events
 - Management Events
 - Serviceable Events
 - Customer Serviceable Events
 - Non-serviceable Events
 - Show only events with a specific date and time. You can choose one of the following options:
 - All Dates
 - Previous 2 hours
 - Previous 24 hours
 - Past Week
 - Past Month
 - Custom

If you select **Custom**, you can filter hardware and management events that were raised between a custom start date and the current date.

- List only events that contain specific text by entering the text in the **Filter** field.
- Sort the events by column by clicking on a column heading.


Monitoring events in the audit log

The *audit log* provides a historical record of user actions, such as logging in to Lenovo XClarity Administrator, creating a new user, and changing a user password. You can use the audit log to track and document authentication and controls in IT systems.

About this task

The audit log can contain a maximum of 50,000 events. When the maximum size is reached, the oldest event in the log is discarded and the new event is added to the log.

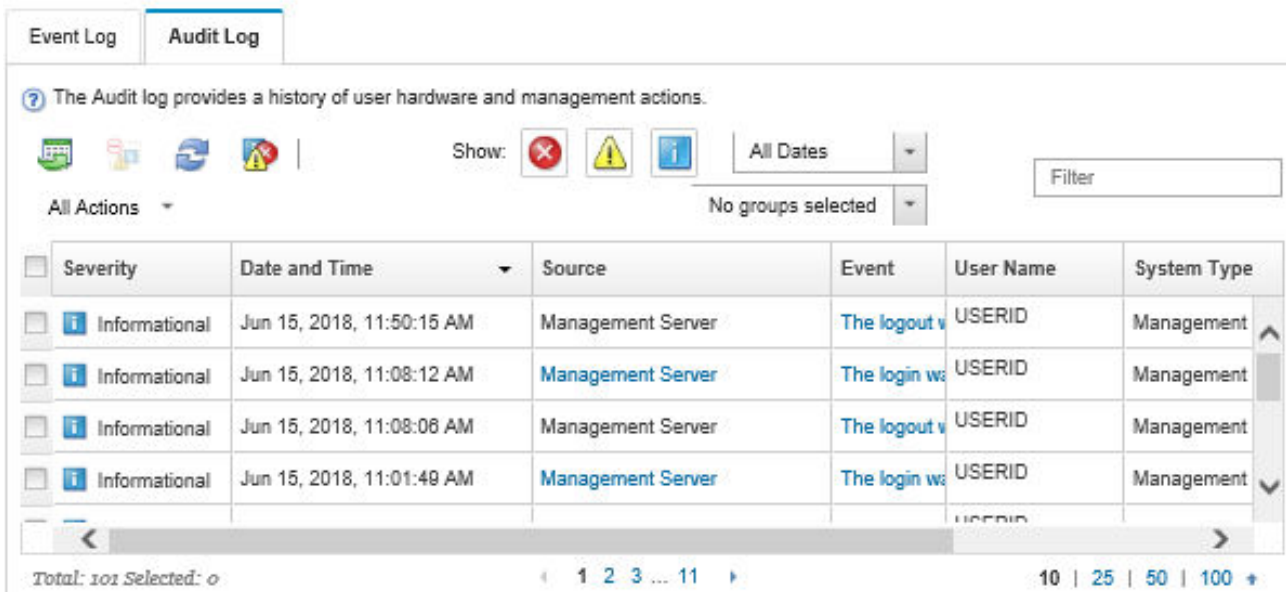
XClarity Administrator sends an event when the audit log reaches 80% of the maximum size and another event when the sum of the event and audit logs reaches 100% of the maximum size.

Tip: You can export the audit log to ensure that you have a complete record of all audit events. To export the audit log, click the **Export as CSV** icon ()

Procedure

To view the audit log, click **Monitoring → Event Logs** from the XClarity Administrator menu bar, and click the **Audit Log** tab. The Audit Log page is displayed.

Logs




The screenshot displays the 'Audit Log' tab in XClarity Administrator. At the top, there are tabs for 'Event Log' and 'Audit Log'. Below the tabs is a help message: 'The Audit log provides a history of user hardware and management actions.' There are several icons for severity levels: All Actions, Error (red X), Warning (yellow triangle), and Info (blue i). A 'Show:' dropdown is set to 'All Dates'. A 'Filter' input field is present. The main area is a table with the following columns: Severity, Date and Time, Source, Event, User Name, and System Type. The table contains four rows of informational events from June 15, 2018. Below the table, there is a pagination bar showing 'Total: 101 Selected: 0' and page numbers 1, 2, 3, ..., 11.

Severity	Date and Time	Source	Event	User Name	System Type
Informational	Jun 15, 2018, 11:50:15 AM	Management Server	The logout v	USERID	Management
Informational	Jun 15, 2018, 11:08:12 AM	Management Server	The login w	USERID	Management
Informational	Jun 15, 2018, 11:08:08 AM	Management Server	The logout v	USERID	Management
Informational	Jun 15, 2018, 11:01:49 AM	Management Server	The login w	USERID	Management


To view information about a specific audit event, click the link in the **Event** column. A dialog is displayed with information about the properties for the device that sent the event, details about the event, and recovery actions.

Results

From this page, you can perform the following actions:




- View the source of the audit event by clicking the link in the **Source** column.
- Refresh the list of audit events by clicking the **Refresh** icon ()

Tip: The event log refreshes automatically every 30 seconds if new events are detected.

- View details about a specific audit event by clicking the link in the **Event** column and then clicking the **Details** tab.
- Export the audit log by clicking the **Export as CSV** icon ()

Note: The timestamps in the exported log use the local time that is specified by the web browser.

- Exclude specific audit events from all pages on which events are displayed (see [Excluding events](#)).
- Narrow the list of audit events that are displayed on the current page:
 - Show or hide events of a specific severity by clicking the following icons:

- **Critical events** icon ()
- **Warning events** icon ()
- **Informational events** icon ()
- Show only events with a specific date and time. You can choose one of the following options from the drop-down list:
 - All Dates
 - Previous 2 hours
 - Previous 24 hours
 - Past Week
 - Past Month
 - Custom

If you select **Custom**, you can filter hardware and management events that were raised between a custom start date and the current date.

- List only events that contain specific text by entering the text in the **Filter** field.
- Sort the events by column by clicking on a column heading.

Resolving an event

Lenovo XClarity Administrator provides information about the appropriate actions to perform to resolve an event.

Procedure

Complete the following steps to resolve an event.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring** → **Event Logs** to display the Logs page.
- Step 2. Click the **Event Log** tab.
- Step 3. Locate the event in the events log.
- Step 4. Click the link in the **Event** column to view information about that event (including an explanation and recovery actions) and about the device that is the source of the event.
- Step 5. Click the **Details** tab.
- Step 6. Complete the recovery actions under the **Details** tab to resolve the event.

Note: If the explanation and recovery action for an event are not displayed, go to [Lenovo Flex System online documentation](#), and search for the event title. The website always provides the most up-to-date information.

If you follow the recommended actions and the problem persists, contact Lenovo Support.

Excluding events

If there are specific events that are of no interest to you, you can exclude the events from all pages on which events are displayed. Excluded events are still in the log but are hidden from all pages on which events are displayed.

About this task


Excluded events are hidden for all users, not just the user that set the configuration.

You can place devices in maintenance mode, so that all events and alerts for those devices are excluded (see [Placing devices in maintenance mode](#)).

Restriction: Only users with administrative authority can exclude or restore events.


Procedure

Complete the following steps to exclude events from the event logs.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring** → **Event Logs**, and click the **Event Log** tab. The Event Logs is displayed.
- Step 2. Select the events to be excluded, and click the **Exclude events** icon (). The Exclude Events dialog is displayed.
- Step 3. Select one of the following options:
 - **Exclude selected events from all systems.** Excludes the selected events from all managed devices.
 - **Exclude events only from systems in the scope of the instance selected.** Excludes the selected events from managed devices to which the selected events apply.
- Step 4. Click **Save**.


After you finish

When you exclude events, Lenovo XClarity Administrator creates exclusion rules based on information that you provide.

- View a list of exclusion rules and excluded events from the Logs page by clicking the **Show Excluded Events** icon (). In the Excluded Events dialog, click the **Exclusion Rules** tab to view the exclusion rules, or click the **Excluded Events** tab to view excluded events.

Excluded Events

Exclusion Rules		Excluded Events	
Event	System	Event ID	Filter
<input type="checkbox"/> Power supply Power Supply 01 power meter is online.	All	00038501	
<input type="checkbox"/> Received Network Time Protocol (NTP) update	All	1.3.6.1.4.1.20301.2.5.7.0.62	
<input type="checkbox"/> The management server launched the job(s) 5655 for job scheduler Collect service data success	All	FQXHMJM0016I	

- Restore events that have been excluded in the event log by removing the appropriate exclusion rule. To remove an exclusion rule, click the **Show Excluded Events** icon () to display the Excluded Events dialog, select the exclusion rules to restore, and click **Remove Exclusions**.
- Prevent serviceable events that are in the list of excluded events from automatically opening problem reports by clicking **Administration** → **Service and Support** from the Lenovo XClarity Administrator menu bar, clicking the **Service Forwarders** tab, and then selecting **No** next to the question **Do you want excluded events to open problem reports?**

Forwarding events

You can configure Lenovo XClarity Administrator to forward events to mobile devices and to connected applications that you have in your environment for aggregating and monitoring hardware status and runtime issues for your hardware environment.

Learn more:  [XClarity Administrator: Monitoring](#)

Forwarding events to syslog, remote SNMP manager, email, and other event services

You can configure Lenovo XClarity Administrator to forward events to connected applications that you have in your environment for aggregating and monitoring hardware status and runtime issues for your hardware environment. You can define the scope of events to be forwarded based on device, event class, event severity, and component.

About this task

Lenovo XClarity Administrator can forward events for one or more devices. For audit events, you can choose to forward all audit events or none. You cannot forward specific audit events. For hardware and management events, you can choose to forward events for one or more severities (critical, warning, and informational) and for one or more components (such as disk drives, processors, and adapters).

Lenovo XClarity Administrator uses event forwarders to forward events. An *event forwarder* includes information about the protocol to use, the recipient, the devices to monitor, and the events to forward. After you create and enable an event forwarder, Lenovo XClarity Administrator starts monitoring for incoming events based on the filter criteria. When a match is found, the associated protocol is used to forward the event.

The following protocols are supported:

- **Azure Log Analytics.** Lenovo XClarity Administrator forwards the monitored events to over the network to Microsoft Azure Log Analytics.
- **Email.** Lenovo XClarity Administrator forwards the monitored events to one or more email addresses using SMTP. The email contains information about the event, the host name of the source device, and links to the Lenovo XClarity Administrator web interface and Lenovo XClarity Mobile app.
- **FTP.** Forwards monitored events over the network to an FTP server.
- **REST.** Lenovo XClarity Administrator forwards the monitored events over the network to a REST Web Service.
- **SNMP.** Lenovo XClarity Administrator forwards the monitored events over the network to a remote SNMP manager. SNMPv1 and SNMPv3 traps are supported.

For information about the management information base (MIB) file that describes the SNMP traps Lenovo XClarity Administrator generates, see [lenovoMgrAlert.mib file](#) in the Lenovo XClarity Administrator online documentation.

- **Syslog.** Lenovo XClarity Administrator forwards the monitored events over the network to a central log server where native tools can be used to monitor the syslog.

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Note: Events are not delivered if, for example, connectivity between Lenovo XClarity Administrator and the event forwarder is down or if the port is blocked.

Setting up event forwarding to Azure Log Analytics

You can configure Lenovo XClarity Administrator to forward specific events to Azure Log Analytics.

About this task


You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for Azure Log Analytics.

- Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.
- Step 2. Click the **Event Forwarder** tab.
- Step 3. Click the **Create** icon (). The **General** tab of New Event Forwarder dialog is displayed.
- Step 4. Select **Azure Log Analytics** as the event-forwarder type, and fill in the protocol-specific information:
 - Enter the name and optional description for the event forwarder.
 - Enter the primary key for the Azure Log Analytics interface.
 - Enter the time-out period (in seconds) for the request. Default is 30 seconds.
 - **Optional:** If authentication is required, select one of the following authentication types:
 - **Basic.** Authenticates to the specified server using the specified user ID and password.
 - **None.** No authentication is used.
- Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarder.

The following example output format is the default format for Azure Log Analytics recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for Azure Log Analytics recipients are listed in the Output Format dialog.

```
{ "Msg": "[EventMessage]", "EventID": "[EventID]", "SerialNum":  
  "[EventSerialNumber]", "SenderUUID": "[EventSenderUUID]", "Flags":  
  "[EventFlags]", "Userid": "[EventUserName]", "LocalLogID":  
  "[EventLocalLogID]", "DeviceName": "[DeviceFullPathName]", "SystemName":  
  "[SystemName]", "Action": "[EventAction]", "FailFRUs":  
  "[EventFailFRUs]", "Severity": "[EventSeverity]", "SourceID":  
  "[EventSourceUUID]", "SourceLogSequence": "[EventSourceLogSequenceNumber]",  
  "FailSNs": "[EventFailSerialNumbers]", "FailFRUUUIDs":  
  "[EventFailFRUUUIDs]", "EventClass": "[EventClass]", "ComponentID":  
  "[EventComponentUUID]", "Mtm": "[EventMachineTypeModel]", "MsgID":  
  "[EventMessageID]", "SequenceNumber": "[EventSequenceID]", "TimeStamp":  
  "[EventTimeStamp]", "Args": "[EventMessageArguments]", "Service":  
  "[EventService]", "CommonEventID": "[CommonEventID]", "EventDate":  
  "[EventDate]", "EventSource": "[EventSource]", "DeviceSerialNumber":  
  "[DeviceSerialNumber]", "DeviceIPAddress": "[DeviceIPAddress]",
```

```
\ "LXCA\ ": \ "[[LXCA_IP]] \ " }
```

You can click **Reset to defaults** to change the output format back to the default fields.

- Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.
- Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.
- Step 8. Click **Next** to display the **Devices** tab.
- Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox. If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

- Step 10. Click **Next** to display the **Events** tab.
- Step 11. Select the filters to use for this event forwarder.

- **Match by event category.**
 1. To forward all audit events regardless of the status level, select **Include All Audit events**.
 2. To forward all warranty events, select **Include Warranty events**.
 3. To forward all health-status-change events, select **Include Status Change events**.
 4. To forward all health-status-update events, select **Include Status Update events**.
 5. Select the event classes and serviceability level that you want to forward.
 6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, FQXHMEM0214I,FQXHMEM0214I).
- **Match by event code.** Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category.**
 1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
 2. To exclude all warranty events, select **Exclude Warranty events**.
 3. To exclude all health-status-change events, select **Exclude Status Change events**.
 4. To exclude all health-status-update events, select **Exclude Status Update events**.
 5. Select the event classes and serviceability level that you want to exclude.
 6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code.** Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

- Step 12. Choose whether to include certain types of events.

- **Include All Audit events.** Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events.** Send notifications about warranties.
- **Include Status Change events.** Sends notifications about changes in status.
- **Include Status Update events.** Sent notifications about new alerts.
- **Include Bulletin events.** Sends notification about new bulletins.

- Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Event Forwarding

<input type="checkbox"/>	Name	Notification Method	Description	Status
<input type="checkbox"/>	x880 Critical events	Syslog		Enabled
<input type="checkbox"/>	SAP ITOA	Syslog		Enabled
<input type="checkbox"/>	Log Insight	Syslog		Enabled

Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate Azure Log Analytics server.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon (.
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon (.
- Suspend event forwarding (see [Suspending event forwarding](#)).

Setting up event forwarding to an email service using SMTP

You can configure Lenovo XClarity Administrator to forward specific events to an email service using SMTP.

Before you begin

To forward email to a web-based email service (such as Gmail, Hotmail, or Yahoo), your SMTP server must support forwarding web mail.

Before setting up an event forwarder to a Gmail web service, review information in [Setting up event forwarding to syslog, remote SNMP manager, or email](#) in the Lenovo XClarity Administrator online documentation.

About this task


You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for email using SMTP.

- Step 1. From the XClarity Administrator menu bar, click **Monitoring** → **Event Forwarding**. The Event Forwarding page is displayed.
- Step 2. Click the **Event Forwarder** tab.
- Step 3. Click the **Create** icon (). The **General** tab of New Event Forwarder dialog is displayed.
- Step 4. Select **Email** as the event-forwarder type, and fill in the protocol-specific information:
 - Enter the name, destination host, and optional description for the event forwarder.
 - Enter the port to use for forwarding events. The default is 25.
 - Enter the time-out period (in seconds) for the request. Default is 30 seconds.
 - Enter the email address for each recipient. Separate multiple email addresses by using a comma.

To send the email to the support contact that is assigned for the device, select **Use Support Contact Email(s)** (see [Defining the support contacts for a device](#) in the XClarity Administrator online documentation).

 - **Optional:** Enter the email address for the sender of the email (for example, john@company.com).

If you do not specify an email address, the sender address is `LXCA.<source_identifier>@<smtp_host>` by default.

If you specify only the sender domain, the format of the sender address is `<LXCA_host_name>@<sender_domain>` (for example, `XClarity1@company.com`).

Notes:

- If you set up your SMTP server to require a hostname to forward emails, and you do not set up a hostname for XClarity Administrator, it is possible that the SMTP server might reject forwarded events. If XClarity Administrator does not have a hostname, the event is forwarded with the IP address. If the IP address cannot be obtained, “localhost” is sent instead, which might cause the SMTP server to reject the event.
- If you specify the sender domain, the source does not identify in the sender address. Instead, information about the source of the event is included in the body of the email, including system name, IP address, type/model, and serial number.
- If the SMTP server accepts only emails that were sent by a registered user, the default sender address (`LXCA.<source_identifier>@<smtp_host>`) is rejected. In this case, you must specify at least a domain name in the **From address** field.
- **Optional:** To establish a secure connection to the SMTP server, select the following connection types:
 - **SSL.** Use the SSL protocol while communicating.
 - **STARTTLS.** Uses TLS to form a secure communication over an unsecure channel.

If one of these connection types is selected, LXCA attempts to download and import the SMTP server’s certificate to its truststore. You are asked to accept adding this certificate to the truststore.

- **Optional:** If authentication is required, select one of the following authentication types:
 - **Regular.** Authenticates to the specified SMTP server using the specified user ID and password.
 - **NTLM.** Uses the NT LAN Manager (NTLM) protocol to authentication to the specified SMTP server using the specified user ID, password, and domain name.
 - **OAUTH2.** Uses the Simple Authentication and Security Layer (SASL) protocol to authenticate to the specified SMTP server using the specified user name and security token. Typically, the user name is your email address.

Attention: The security token expires after a short time. It is your responsibility to refresh the security token.

- **None.** No authentication is used.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded in the email body and the format of the email subject. The information varies for each type of event forwarder.

The following example output format is the default format for email recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for the email recipients are listed in the Output Format dialog.

Email subject

```
[[DeviceName]]-[[EventMessage]]
```

Email body

```
Alert: [[EventDate]] [[EventMessage]]\n\nHardware Information:\nManaged Endpoint : [[DeviceHardwareType]] at [[DeviceIPAddress]]\nDevice name : [[DeviceName]]\nProduct name : [[DeviceProductName]]\n
```

```

Host name          : [[DeviceHostName]]\n
Machine Type      : [[DeviceMachineType]]\n
Machine Model     : [[DeviceMachineModel]]\n
Serial Number     : [[DeviceSerialNumber]]\n
DeviceHealthStatus : [[DeviceHealthStatus]]\n
IPv4 addresses    : [[DeviceIPv4Addresses]]\n
IPv6 addresses    : [[DeviceIPv6Addresses]]\n
Chassis           : [[DeviceChassisName]]\n
DeviceBays        : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
Event ID          : [[EventID]]\n
Common Event ID  : [[CommonEventID]]\n
EventSeverity    : [[EventSeverity]]\n
Event Class      : [[EventClass]]\n
Sequence ID      : [[EventSequenceID]]\n
Event Source ID  : [[EventSourceUUID]]\n
Component ID     : [[EventComponentUUID]]\n
Serial Num       : [[EventSerialNumber]]\n
MTM              : [[EventMachineTypeModel]]\n
EventService     : [[EventService]]\n
Console link     : [[ConsoleLink]]\n
iOS link         : [[iOSLink]]\n
Android link     : [[AndroidLink]]\n
System Name      : [[DeviceFullPathName]]\n

```

You can click **Reset to defaults** to change the output format back to the default fields.

- Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.
- Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.
- Step 8. Click **Next** to display the **Devices** tab.
- Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox. If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

- Step 10. Click **Next** to display the **Events** tab.
- Step 11. Select the filters to use for this event forwarder.

- **Match by event category.**

1. To forward all audit events regardless of the status level, select **Include All Audit events**.
2. To forward all warranty events, select **Include Warranty events**.
3. To forward all health-status-change events, select **Include Status Change events**.
4. To forward all health-status-update events, select **Include Status Update events**.
5. Select the event classes and serviceability level that you want to forward.
6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, FQXMEM0214I,FQXMEM0214I).

- **Match by event code.** Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category.**
 1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
 2. To exclude all warranty events, select **Exclude Warranty events**.
 3. To exclude all health-status-change events, select **Exclude Status Change events**.
 4. To exclude all health-status-update events, select **Exclude Status Update events**.
 5. Select the event classes and serviceability level that you want to exclude.
 6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code.** Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Choose whether to include certain types of events.

- **Include All Audit events.** Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events.** Send notifications about warranties.
- **Include Status Change events.** Sends notifications about changes in status.
- **Include Status Update events.** Sent notifications about new alerts.
- **Include Bulletin events.** Sends notification about new bulletins.

Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.

Event Forwarding

Event Monitors | Push Services | Push Filters

This page is a list of all remote event recipients. You can define up to 20 unique recipients.

| Generate Test Event | All Actions ▾ | Filter

<input type="checkbox"/>	Name ▾	Notification Method	Description	Status
<input type="checkbox"/>	x880 Critical events	Syslog		Enabled ▾
<input type="checkbox"/>	SAP ITOA	Syslog		Enabled ▾
<input type="checkbox"/>	Log Insight	Syslog		Enabled ▾

Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate email service.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ().
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ().
- Suspend event forwarding (see [Suspending event forwarding](#)).

Setting up event forwarding to a Gmail SMTP service

You can setup Lenovo XClarity Administrator to forward monitored events to a web-based email service, such as Gmail.

Use the following configuration examples to help you set up your event forwarder to use the Gmail SMTP service.

Note: Gmail recommends using the OAUTH2 authentication method for the most secure communication. If you choose to use regular authentication, you will receive an email indicating that an application tried to use your account without using the latest security standards. The email includes instructions for configuring your email account to accept these types of applications.

For information about configuring a Gmail SMTP server, see <https://support.google.com/a/answer/176600?hl=en>.

Regular authentication using SSL on port 465

This example communicates with the Gmail SMTP server using the SSL protocol over port 465, and authenticates using a valid Gmail user account and password.

Parameter	Value
Host	smtp.gmail.com
Port	465
SSL	Select
STARTTLS	Clear
Authentication	Regular
User	Valid Gmail email address
Password	Gmail authentication password
From Address	(optional)

Regular authentication using TLS on port 587

This example communicates with the Gmail SMTP server using the TLS protocol over port 587, and authenticates using a valid Gmail user account and password.

Parameter	Value
Host	smtp.gmail.com
Port	587
SSL	Clear
STARTTLS	Select
Authentication	Regular
User	Valid Gmail email address
Password	Gmail authentication password
From Address	(optional)

OAuth2 authentication using TLS on port 587

This example communicates with the Gmail SMTP server using the TLS protocol over port 587, and authenticates using a valid Gmail user account and security token.

Use the following example procedure to obtain the security token.

1. Create a project in the Google Developers Console, and retrieve the client ID and client secret. For more information, see the [Google Sign-In for Websites webpage](#) website.
 - a. From a web browser, open the [Google APIs webpage](#).
 - b. Click **Select a project** → **Create a project** from the menu on that webpage. The New Project dialog is displayed.
 - c. Type a name, select **Yes** to agree to the license agreement, and click **Create**.
 - d. On the **Overview** tab, use the search field to search for “gmail.”
 - e. Click **GMAIL API** in the search results.
 - f. Click on **Enable**.
 - g. Click the **Credentials** tab
 - h. Click **OAuth consent screen**.
 - i. Type a name in the **Product name shown to users** field, and click **Save**.
 - j. Click **Create credentials** → **OAuth client ID**.

- k. Select **Other**, and enter a name.
 - l. Click **Create**. The OAuth client dialog is displayed with your client ID and client secret.
 - m. Record the client ID and client secret for later use.
 - n. Click **OK** to close the dialog.
2. Use the [oauth2.py](#) Python script to generate and authorize a security token by entering the client ID and client secret that was generated when you created the project.

Note: Python 2.7 is required to complete this step. You can download and install Python 2.7 from the [Python website](#)).

- a. From a web browser, open the [gmail-oauth2-tools webpage](#).
- b. Click **Raw**, and then save the content as a file name `oauth2.py` on your local system.
- c. Run the following command a terminal (Linux) or a command line (Windows):

```
py oauth2.py --user=<your_email> --client_id=<client_id>
--client_secret=<client_secret> --generate_oauth2_token
```

For example

```
py oauth2.py --user=jon@gmail.com
--client_id=884243132302-458elfqjbiebpvdmvdackp6elip8kl63.apps.googleusercontent.com
--client_secret=3tnyXgEiBIBT2m00zqnlTszk --generate_oauth2_token
```

This command returns a URL that you must use to authorize the token and retrieve a verification code from the Google website, for example:

To authorize token, visit this url and follow the directions:

```
https://accounts.google.com/o/oauth2/auth?client_id=884243132302
-458elfqjbiebpvdmvdackp6elip8kl63.apps.googleusercontent.com&redirect_uri=
urn%3Aietf%3Awww%3Aoauth%3A2.0%3Aoauth&response_type=code&scope=https%3A%2F%2Fmail.
google.com%2F
```

Enter verification code:

- d. From a web browser, open the URL that was returned in the previous step.
- e. Click **Allow** to agree to this service. A verification code is returned.
- f. Enter the verification code in the `oauth2.py` command.

The command returns the security token and refreshes token, for example:

```
Refresh Token: 1/K8LPGx6UQQajj7tQGyKq8mVG8LVvGIVzHqzxFIMeYEQMEudVrK5jSpOR30zcRFq6
Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600
```

Important: The security token expires after a period of time. You can use the [oauth2.py](#) Python script and the refresh token to generate a new security token. It is your responsibility to generate the new security token and update the event forwarder in Lenovo XClarity Administrator with the new token.

3. From the Lenovo XClarity Administrator web interface, set up event forwarder for email using the following attributes:

Parameter	Value
Host	smtp.gmail.com
Port	587
SSL	Clear
STARTTLS	Select

Parameter	Value
Authentication	OAuth2
User	Valid Gmail email address
Token	Security token
From Address	(optional)

Setting up event forwarding to an FTP server

You can configure Lenovo XClarity Administrator to forward specific events to an FTP server.

About this task


You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for an FTP server.

- Step 1. From the XClarity Administrator menu bar, click **Monitoring** → **Event Forwarding**. The Event Forwarding page is displayed.
- Step 2. Click the **Event Forwarder** tab.
- Step 3. Click the **Create** icon (). The **General** tab of New Event Forwarder dialog is displayed.
- Step 4. Select **FTP** as the event-forwarder type, and fill in the protocol-specific information:
 - Enter the name, destination host, and optional description for the event forwarders.
 - Enter the port to use for forwarding events. The default is 21.
 - Enter the time-out period (in seconds) for the request. Default is 30 seconds.
 - **Optional:** Specify the sequence of characters to be removed from the file content.
 - Enter the file-name format to use for the file that contains the forwarded event. The default format is `event_[[EventSequenceID]].txt`.

Note: Each file contains information for a single event.

 - Enter the path on the remote FTP server where the file is to be uploaded.
 - Choose the character encoding, either **UTF-8** or **Big5**. This is UTF-8 by default.
 - Select the authentication type. This can be one of the following values.
 - **Anonymous.** (default) No authentication is used
 - **Basic.** Authenticates to the FTP server using the specified user ID and password.
- Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarders.

The following example output format is the default format for FTP recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for FTP recipients are listed in the Output Format dialog.

```

Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint   : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name        : [[DeviceName]]\n
Product name       : [[DeviceProductName]]\n
Host name          : [[DeviceHostName]]\n
Machine Type       : [[DeviceMachineType]]\n
Machine Model      : [[DeviceMachineModel]]\n
Serial Number      : [[DeviceSerialNumber]]\n
DeviceHealthStatus : [[DeviceHealthStatus]]\n
IPv4 addresses     : [[DeviceIPv4Addresses]]\n
IPv6 addresses     : [[DeviceIPv6Addresses]]\n
Chassis            : [[DeviceChassisName]]\n
DeviceBays         : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
Event ID           : [[EventID]]\n
Common Event ID   : [[CommonEventID]]\n
EventSeverity      : [[EventSeverity]]\n
Event Class       : [[EventClass]]\n
Sequence ID       : [[EventSequenceID]]\n
Event Source ID   : [[EventSourceUUID]]\n
Component ID      : [[EventComponentUUID]]\n
Serial Num        : [[EventSerialNumber]]\n
MTM               : [[EventMachineTypeModel]]\n
EventService      : [[EventService]]\n
Console link      : [[ConsoleLink]]\n
iOS link          : [[iOSLink]]\n
Android link      : [[AndroidLink]]\n
System Name       : [[DeviceFullPathName]]\n"

```

You can click **Reset to defaults** to change the output format back to the default fields.

- Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.
- Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.
- Step 8. Click **Next** to display the **Devices** tab.
- Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox. If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

- Step 10. Click **Next** to display the **Events** tab.
- Step 11. Select the filters to use for this event forwarder.

- **Match by event category.**
 1. To forward all audit events regardless of the status level, select **Include All Audit events**.
 2. To forward all warranty events, select **Include Warranty events**.
 3. To forward all health-status-change events, select **Include Status Change events**.
 4. To forward all health-status-update events, select **Include Status Update events**.

5. Select the event classes and serviceability level that you want to forward.
 6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, FQXHMEM0214I,FQXHMEM0214I).
- **Match by event code.** Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
 - **Exclude by event category.**
 1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
 2. To exclude all warranty events, select **Exclude Warranty events**.
 3. To exclude all health-status-change events, select **Exclude Status Change events**.
 4. To exclude all health-status-update events, select **Exclude Status Update events**.
 5. Select the event classes and serviceability level that you want to exclude.
 6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
 - **Exclude by event code.** Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Choose whether to include certain types of events.

- **Include All Audit events.** Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events.** Send notifications about warranties.
- **Include Status Change events.** Sends notifications about changes in status.
- **Include Status Update events.** Sent notifications about new alerts.
- **Include Bulletin events.** Sends notification about new bulletins.

Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.

- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Event Forwarding

Name	Notification Method	Description	Status
x880 Critical events	Syslog		Enabled
SAP ITOA	Syslog		Enabled
Log Insight	Syslog		Enabled

Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate FTP server.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon (.
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon (.
- Suspend event forwarding (see [Suspending event forwarding](#)).

Setting up event forwarding to a REST Web Service

You can configure Lenovo XClarity Administrator to forward specific events to a REST Web Service.

About this task


You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for a REST Web Service.

- Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.
- Step 2. Click the **Event Forwarder** tab.
- Step 3. Click the **Create** icon (). The **General** tab of New Event Forwarder dialog is displayed.
- Step 4. Select **REST** as the event-forwarder type, and fill in the protocol-specific information:
 - Enter the resource path on which the forwarder is to post the events (for example, /rest/test).
 - Select the protocol to use for forwarding events. This can be one of the following values.
 - **HTTP**
 - **HTTPS**
 - Select the REST method. This can be one of the following values.
 - **PUT**
 - **POST**
 - Enter the time-out period (in seconds) for the request. Default is 30 seconds.
 - **Optional:** If authentication is required, select one of the following authentication types:
 - **Basic.** Authenticates to the specified server using the specified user ID and password.
 - **None.** No authentication is used.
- Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarder.

The following example output format is the default format for REST Web Service recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for REST Web Service recipients are listed in the Output Format dialog.

```
{\"msg\": \"[[EventMessage]]\", \"eventID\": \"[[EventID]]\", \"serialnum\": \"[[EventSerialNumber]]\", \"senderUUID\": \"[[EventSenderUUID]]\", \"flags\": \"[[EventFlags]]\", \"userid\": \"[[EventUserName]]\", \"localLogID\": \"[[EventLocalLogID]]\", \"systemName\": \"[[DeviceFullPathName]]\", \"action\": \"[[EventActionNumber]]\", \"failFRUNumbers\": \"[[EventFailFRUs]]\", \"severity\": \"[[EventSeverityNumber]]\", \"sourceID\": \"[[EventSourceUUID]]\", \"sourceLogSequence\": \"[[EventSourceLogSequenceNumber]]\", \"failFRUSNs\": \"[[EventFailSerialNumbers]]\", \"failFRUUUIDs\": \"[[EventFailFRUUUIDs]]\", \"eventClass\": \"[[EventClassNumber]]\", \"componentID\": \"[[EventComponentUUID]]\", \"mtm\": \"[[EventMachineTypeModel]]\", \"msgID\": \"[[EventMessageID]]\", \"sequenceNumber\": \"[[EventSequenceID]]\", \"timeStamp\": \"[[EventTimeStamp]]\", \"args\": \"[[EventMessageArguments]]\", \"service\": \"[[EventServiceNumber]]\", \"commonEventID\": \"[[CommonEventID]]\", \"eventDate\": \"[[EventDate]]\"}
```

You can click **Reset to defaults** to change the output format back to the default fields.

- Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.
- Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.
- Step 8. Click **Next** to display the **Devices** tab.
- Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox. If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you

select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category.**
 1. To forward all audit events regardless of the status level, select **Include All Audit events**.
 2. To forward all warranty events, select **Include Warranty events**.
 3. To forward all health-status-change events, select **Include Status Change events**.
 4. To forward all health-status-update events, select **Include Status Update events**.
 5. Select the event classes and serviceability level that you want to forward.
 6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, FQXHMEM0214I,FQXHMEM0214I).
- **Match by event code.** Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category.**
 1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
 2. To exclude all warranty events, select **Exclude Warranty events**.
 3. To exclude all health-status-change events, select **Exclude Status Change events**.
 4. To exclude all health-status-update events, select **Exclude Status Update events**.
 5. Select the event classes and serviceability level that you want to exclude.
 6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code.** Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Choose whether to include certain types of events.

- **Include All Audit events.** Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events.** Send notifications about warranties.
- **Include Status Change events.** Sends notifications about changes in status.
- **Include Status Update events.** Sent notifications about new alerts.
- **Include Bulletin events.** Sends notification about new bulletins.

Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.

- Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.

Event Forwarding

Event Monitors | Push Services | Push Filters

This page is a list of all remote event recipients. You can define up to 20 unique recipients.

| Generate Test Event | All Actions | Filter

<input type="checkbox"/>	Name	Notification Method	Description	Status
<input type="checkbox"/>	x880 Critical events	Syslog		Enabled
<input type="checkbox"/>	SAP ITOA	Syslog		Enabled
<input type="checkbox"/>	Log Insight	Syslog		Enabled

Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate REST Web Service.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ().
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ().
- Suspend event forwarding (see [Suspending event forwarding](#)).

Setting up event forwarding to a remote SNMPv1 or SNMPv3 manager

You can configure Lenovo XClarity Administrator to forward specific events to a remote SNMPv1 or SNMPv3 manager.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

For information about the XClarity Administrator MIB, see [lenovoMgrAlert.mib](#) file.

Procedure

Complete the following steps to create an event forwarder for a remote SNMPv1 or SNMPv3 manager.

Step 1. From the XClarity Administrator menu bar, click **Monitoring** → **Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forwarder** tab.

Step 3. Click the **Create** icon (). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **SNMPv1** or **SNMPv3** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name and destination host for the event forwarder.
- Enter the port to use for forwarding events. The default is 162.
- **Optional:** Enter additional information, including the description, contact name, and location.
- Select the SNMP version. This can be one of the following values.
 - **SNMPv1.** If this version is selected, specify the community password that is sent with every SNMP request to the device.
 - **SNMPv3.** This is the default version and is recommended for enhanced security. If SNMPv3 is selected, optionally specify the user ID, authentication type and password, and privacy type and password.

If the SNMPv3 trap receiver requires the engine ID for the XClarity Administrator instance, you can find the engine ID by performing the following steps:

1. Ensure that the connection parameters (username, authProtocol, authPassword, privProtocol, privPassword) match the ones set in XClarity Administrator.
2. Using your preferred software (such as snmpwalk), perform an SNMP GET request on the XClarity Administrator server using one of the following OIDs:
 - EngineID: 1.3.6.1.6.3.10.2.1.1.0
 - EngineBoots : 1.3.6.1.6.3.10.2.1.2.0

Use the following syntax for the `snmpget` command. Note that the `-a` forwarder authentication type can be SHA or blank (no authentication).

```
snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDER_A
```

For example, if the XClarity Administrator IP address is 192.0.1.0, the authentication type is SHA, and the privacy type is AES, the following command shows the engineID.

```
snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_1
```

The following example response is returned. In this example, the engineID is 0x80001370017F00000134C27E12.

iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12

- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- **Optional:** If trap authentication is needed, enter the user ID and authentication password. The same user ID and password must be entered in the remote SNMP manager to which the traps are forwarded.
- Select the authentication protocol that is used by the remote SNMP manager to verify the trap sender. This can be one of the following values
 - **SHA.** Uses the SHA protocol to authentication to the specified SNMP server using the specified user ID, password, and domain name.
 - **None.** No authentication is used
- If trap encryption is needed, enter the privacy type (encryption protocol) and password. This can be one of the following values. The same protocol and password must be entered in the remote SNMP manager to which the traps are forwarded.
 - **AES**
 - **DES**
 - **None**

Step 5. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 6. Select **Enable this forwarder** to activate event forwarding for this event forwarder.

Step 7. Click **Next** to display the **Devices** tab.

Step 8. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox. If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 9. Click **Next** to display the **Events** tab.

Step 10. Select the filters to use for this event forwarder.

- **Match by event category.**
 1. To forward all audit events regardless of the status level, select **Include All Audit events.**
 2. To forward all warranty events, select **Include Warranty events.**
 3. To forward all health-status-change events, select **Include Status Change events.**
 4. To forward all health-status-update events, select **Include Status Update events.**
 5. Select the event classes and serviceability level that you want to forward.
 6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, FQXHMEM0214I,FQXHMEM0214I).
- **Match by event code.** Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category.**
 1. To exclude all audit events regardless of the status level, select **Exclude All Audit events.**
 2. To exclude all warranty events, select **Exclude Warranty events.**
 3. To exclude all health-status-change events, select **Exclude Status Change events.**
 4. To exclude all health-status-update events, select **Exclude Status Update events.**
 5. Select the event classes and serviceability level that you want to exclude.

6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code.** Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 11. Choose whether to include certain types of events.

- **Include All Audit events.** Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events.** Send notifications about warranties.
- **Include Status Change events.** Sends notifications about changes in status.
- **Include Status Update events.** Sent notifications about new alerts.
- **Include Bulletin events.** Sends notification about new bulletins.

Step 12. Select the types of events and severities for which you want to be notified.

Step 13. Select whether to filter events by serviceability.

Step 14. Click **Next** to display the **Scheduler** tab.

Step 15. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 16. Click **Create**.

The event forwarder is listed in the Event Forwarding table.

Event Forwarding

Name	Notification Method	Description	Status
x880 Critical events	Syslog		Enabled
SAP ITOA	Syslog		Enabled
Log Insight	Syslog		Enabled

Step 17. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate remote SNMP manager.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ().
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ().
- Suspend event forwarding (see [Suspending event forwarding](#)).
- Download the MIB file that contains information about SNMP traps by clicking the **Create** icon (), and then clicking **Download MIB File** on the General tab of New Event Forwarding dialog

lenovoMgrAlert.mib file

This management information base (MIB) file describes the SNMP traps that Lenovo XClarity Administrator generates, including alerts that were raised by XClarity Administrator and managed devices. You can compile this MIB file in any SNMP trap manager so that the SNMP traps that are sent from XClarity Administrator can be rendered meaningfully.

You can download the MIB file from the web interface by clicking **Monitoring** → **Event Forwarding** from the menu bar, clicking the **Create** icon () , selecting **SNMP** for the event-forwarder type, and then clicking **Download MIB File** at the bottom of the dialog.

The following objects are included in all outgoing SNMP traps. Additional objects might be included in some SNMP traps. All objects are described in the MIB file. Note that recovery information is not included in the trap.

Note: This list might differ from one release of XClarity Administrator to another.

- **mgrTrapApplId.** This is “Lenovo Event Manager.”
- **mgrTrapCommonEvtID.** Common event ID
- **mgrTrapDateTime.** Local date and time when the event was raised
- **mgrTrapEventClass.** The source of the event. This can Audit, Cooling, Power, Disks, Memory, Processors, System, Test, Adaptor, Expansion, IOModule, or Blade.

- **mgrTrapEvtID.** The unique identifier for the event
- **mgrTrapFailFRUs.** A comma separated list of the failing FRU UUIDs, if applicable
- **mgrTrapFailSNs.** A comma separated list of the serial numbers for failing FRUs, if applicable.
- **mgrTrapFullyQualifiedDomainName.** The fully qualified domain name: the hostname and the domain name
- **mgrTrapID.** Trap ID
- **mgrTrapMsgText.** Message text (English only)
- **mgrTrapMsgID.** Message identifier
- **mgrTrapMtm.** Model type model of the device that raised the event
- **mgrTrapService.** Serviceability indicator. This can be 000 (Unknown), 100 (None), 200 (Service Center), or 300 (Customer)
- **mgrTrapSeverity.** Severity indicator. This can be Informational, Warning, Minor, Major, or Critical
- **mgrTrapSN.** Serial number of the device that raised the event
- **mgrTrapSrcIP.** IP address of the device from which the raised event was received
- **mgrTrapSrcLoc.** Location of the device that raised the event, in English only (for example, Slot#xx)
- **mgrTrapSrcName.** Hostname or display name of the device that raised the event
- **mgrTrapSysContact.** User-configured contact ID
- **mgrTrapSysLocation.** User-configured device-location information
- **mgrTrapSystemName.** Device name, component name, and slot location
- **mgrTrapTxtd.** Host name or IP address of Lenovo Event Manager server that raised the trap
- **mgrTrapUserid.** User ID that is associated with the event (if the event is internal and event class is Audit)
- **mgrTrapUuid.** UUID of the device that raised the event

Setting up event forwarding to a syslog

You can configure Lenovo XClarity Administrator to forward specific events to a syslog.

About this task


You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for a syslog.

- Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.
- Step 2. Click the **Event Forwarder** tab.
- Step 3. Click the **Create** icon (). The **General** tab of New Event Forwarder dialog is displayed.
- Step 4. Select **Syslog** as the event-forwarder type, and fill in the protocol-specific information:
 - Enter the name, destination host, and optional description for the event forwarder.
 - Enter the port to use for forwarding events. The default is 514.
 - Select the protocol to use for forwarding events. This can be one of the following values.
 - **UDP**
 - **TCP**
 - Enter the time-out period (in seconds) for the request. Default is 30 seconds.

- Optionally select the format for the timestamp in the syslog. This can be one of the following values.
 - **Local time.** The default format, for example Fri Mar 31 05:57:18 EDT 2017.
 - **GMT time.** International standard (ISO8601) for dates and times, for example 2017-03-31T05:58:20-04:00.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarder.

The following example output format is the default format for syslog recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for syslog recipients are listed in the Output Format dialog.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

You can click **Reset to defaults** to change the output format back to the default fields.

- Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.
- Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.
- Step 8. Click **Next** to display the **Devices** tab.
- Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox. If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

- Step 10. Click **Next** to display the **Events** tab.
- Step 11. Select the filters to use for this event forwarder.

- **Match by event category.**
 1. To forward all audit events regardless of the status level, select **Include All Audit events**.
 2. To forward all warranty events, select **Include Warranty events**.
 3. To forward all health-status-change events, select **Include Status Change events**.
 4. To forward all health-status-update events, select **Include Status Update events**.
 5. Select the event classes and serviceability level that you want to forward.
 6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, FQXHMEM0214I,FQXHMEM0214I).
- **Match by event code.** Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category.**
 1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
 2. To exclude all warranty events, select **Exclude Warranty events**.
 3. To exclude all health-status-change events, select **Exclude Status Change events**.
 4. To exclude all health-status-update events, select **Exclude Status Update events**.

5. Select the event classes and serviceability level that you want to exclude.
 6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code.** Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Choose whether to include certain types of events.

- **Include All Audit events.** Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events.** Send notifications about warranties.
- **Include Status Change events.** Sends notifications about changes in status.
- **Include Status Update events.** Sent notifications about new alerts.
- **Include Bulletin events.** Sends notification about new bulletins.

Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Event Forwarding

Name	Notification Method	Description	Status
x880 Critical events	Syslog		Enabled
SAP ITOA	Syslog		Enabled
Log Insight	Syslog		Enabled

Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate syslog.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon (.
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon (.
- Suspend event forwarding (see [Suspending event forwarding](#)).

Suspending event forwarding

You can suspend event forwarding by disabling the event forwarder. Suspending event forwarding stops the monitoring of incoming events. Events that are received while monitoring is suspended are not forwarded.

About this task

The disabled state is not persistent. If the management node is restarted, all event forwarders become enabled.

Procedure

Complete the following steps to disable the forwarding of events.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring** → **Forwarding Events**. The Event Forwarding page is displayed.

Step 2. Select **Disable** in the **Status** column for each event forwarder that you want to suspend.

Forwarding events to mobile devices

You can configure Lenovo XClarity Administrator to push event notifications to mobile devices

Before you begin

The following requirements must be met to forward events to mobile devices:

- Ensure that a valid DNS server is configured to allow Lenovo XClarity Administrator to connect to the Apple or Google push servers. This can be configured by clicking the **Administration → Network Access → Edit Network Access** and then clicking the **Internet Settings** tab (see [Configuring network access](#) in the Lenovo XClarity Administrator online documentation).
- Ensure that all required ports for event management are open on the network and firewalls. For information about port requirements, see [Port availability](#) in the Lenovo XClarity Administrator online documentation.

About this task

When the Lenovo XClarity Mobile app is installed on a mobile device, you can enable each connected Lenovo XClarity Administrator instance to push event notifications to that mobile device. When push notifications are enabled for a specific instance, a subscription is created in Lenovo XClarity Administrator for that mobile device.

You can define the events that are pushed to the mobile device by assigning predefined or customized global event filters for each Lenovo XClarity Administrator instance. The predefined global event filters are enabled by default. Lenovo XClarity Administrator starts monitoring for incoming events based on the filter criteria. When a match is found, the event is forwarded to the mobile device.

For more information about Lenovo XClarity Mobile and supported mobile devices, see [Using the Lenovo XClarity Mobile app](#) in the Lenovo XClarity Administrator online documentation.

Procedure

To set up push notifications to that mobile device, complete the following steps from the Lenovo XClarity Mobile app on your mobile device.

Step 1. Enable push notifications:

- You can enable push notifications when you create a connection to a Lenovo XClarity Administrator instance. Push notifications are enabled by default.
- You can enable push notifications on existing connections by enabling one or more event filters

Step 2. Assign global event filters to specify which events are to be forwarded to the mobile device:

Note: You can add or remove global filters from the subscription only from the Lenovo XClarity Mobile app. You can create global filters only from the Lenovo XClarity Administrator web interface. For information about creating customized global event filters, see [Creating event filters for mobile devices and WebSockets](#).

1. Tap **Settings → Push notifications**. A list of Lenovo XClarity Administrator connections is displayed.
2. Tap the Lenovo XClarity Administrator instance to display a list of push filters.
3. Enable the event filters for the events that you want pushed to the mobile device for the Lenovo XClarity Administrator instance.
4. Tap **Touch to generate test push notification** to verify that the event notifications are pushed correctly.

Results

You can manage subscriptions from the Event Forwarding page in the Lenovo XClarity Administrator web interface. Click **Monitoring → Event Forwarding** to display the Event Forwarding page.

Event Forwarding

Name	Description	State
<input type="radio"/> Android Service	The Google device push service	ON
<input type="radio"/> iOS Service	The Apple device push service	ON
<input type="radio"/> WebSocket Service	The XClarity WebSockets push service	ON

- You can change the device notification service properties from the **Push Service** tab on the Event Forwarding page by clicking the link for the push notification service (Google or Apple) in the **Name** column to display the Change Push Notification dialog, and then click the **Properties** tab.

Change Push Notification

Name
Android Service

Description
The Google device push service

State
ON

- You can enable and disable subscriptions:
 - Enable or disable all subscriptions for a specific device notification service from the **Push Service** tab on the Event Forwarding page by selecting the **ON** or **OFF** state in the table for the device notification service.
 - Enable or disable all subscriptions for a specific device from the Lenovo XClarity Mobile app by tapping **Settings** → **Push notification**, and then enabling or disabling Enabled push notification.
 - Enable or disable a specific subscription from the Lenovo XClarity Mobile app by tapping **Settings** → **Push notification**, tapping a Lenovo XClarity Administrator connection, and enabling at least one event filter or disabling all event filters.
- You can generate a test event for all subscriptions for a specific mobile service from the **Push Service** tab on the Event Forwarding page by selecting the mobile service and clicking **Generate Test Event**.
- You can view a list of current subscriptions. From the **Push Service** tab on the Event Forwarding page, click the link for the applicable device notification service (Android or iOS) in the **Name** column to display the Change Push Notification dialog, and then click the **Subscriptions** tab. The device ID identifies each subscription.

Tips:

- The device ID is the first and last 6 digits of the push registration ID. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**.
- If you are logged in as a user with one of the following roles, all subscriptions are displayed; otherwise, subscriptions for only the logged-in user are displayed.
 - **lxc-admin**
 - **lxc-supervisor**
 - **lxc-security-admin**
 - **lxc-sysmgr**
- You can view the list of event filters that are assigned to the subscription from the **Subscriptions** tab on the Change Push Notification dialog by expanding the **Filter list** in the **Event Filters** column for the subscription.

Change Push Notification

Device ID	Subscription Type	User Name	Event ID	Status	Time Stamp	Event Filters
cxA85W ... 3xKkT9	Android Subscriber	USERID	NA	NA		Filter list
						Match All Critical
cxA85W ... 3xKkT9	Android Subscriber	USERID	NA	NA		Filter list
						Match All Critical

- You can create event filters for a specific subscription from the **Subscriptions** tab on the Change Push Notification dialog by selecting the subscription, and click the **Create** icon (📄).

Note: These event filters apply to only a specific subscription and cannot be used by other subscriptions.

You can also edit or remove an event filter by selecting the event filter and clicking the **Edit** icon (✎) or **Remove** icon (✖), respectively.

- You can determine the status of the last attempted push for a specific subscription from the **Subscriptions** tab on the Change Push Notification dialog. The **Time Stamp** column indicates the date and time of the last push. The **Status** indicates whether the push notification was successfully delivered to the push service. No status is available regarding whether the push notification was successfully delivered to the device from the service. If the delivery to the push service failed, the Status column provides additional information about the failure.
- You can generate a test event for a specific subscription from the **Subscriptions** tab on the Change Push Notification dialog by selecting the subscription and clicking **Generate Test Event**.
- You can remove a subscription from the **Subscriptions** tab on the Change Push Notification dialog by selecting the subscription, and clicking the **Remove** icon (✖).

Forwarding events to WebSocket services


You can configure Lenovo XClarity Administrator to push event notifications to WebSocket services.

About this task

The WebSocket subscriptions are not stored persistently in Lenovo XClarity Administrator. When Lenovo XClarity Administrator is rebooted, the WebSocket subscribers must subscribe again.



Procedure

To push event notification to a WebSocket service, complete the following steps.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring** → **Event Forwarding**. The Event Forwarding page is displayed.
- Step 2. Click the **Push Services** tab.
- Step 3. Click the link for the **WebSocket Service** in the **Name** column. The Change Push Notification dialog is displayed.
- Step 4. Click the **Subscriptions** tab.
- Step 5. Click the **Create** icon ()
- Step 6. Enter the IP address of the destination host.
- Step 7. Click **Create**.
- Step 8. Select the new subscription, click **Generate Test Event**, and then verify that the events are forwarded correctly to the WebSocket service.

Results

From the **Subscriptions** tab on the Change Push Notification dialog, you can perform the following actions on a selected WebSocket subscription:

- Refresh the list of WebSocket services by clicking the **Refresh** icon ()
- Delete subscriptions by selecting the subscriptions and clicking the **Delete** icon ()
- Determine the status of the last attempted push for a specific subscription by viewing the content of the **Status** column. If the attempt failed, this column contains a message that describes the error.

From the **Properties** tab on the Change Push Notification dialog, you can perform the following actions:

- Change the WebSocket service properties, including the connection idle time, maximum buffer size, maximum number of subscribers, and the register time-out period.
- You can reset the WebSocket service to the default settings by clicking **Restore Defaults**.
- Suspend pushing event notifications to all subscriptions for the WebSocket service by setting the **State** to Off.

From the **Push Service** tab on the Event Forwarding page, you can generate a test event for all WebSocket subscriptions by selecting the WebSocket service and clicking **Generate Test Event**.

Creating event filters for mobile devices and WebSockets

You can create global events filters that can be used in one or more subscriptions for mobile devices and WebSockets. You can also create event filters that are unique to a subscription.

Before you begin

You must have supervisor authority to create event filters.

You can create up to 20 global event filters.


About this task

The following global event filters are predefined:

- **Match All Critical.** This filter matches all critical events that are generated by any managed device or by XClarity Administrator.
- **Match All Warning.** This filter matches all warning events that are generated by any managed device or by XClarity Administrator.

Procedure

To create a global event filter, complete the following steps.


- Create a global event filter that can be used by any subscription.
 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.
 2. Click the **Push Filters** tab.
 3. Click the **Create** icon (). The **General** tab of New Push Filter dialog is displayed.
 4. Specify the name and option description for this event filter.
 5. Click **Next** to display the **Systems** tab.
 6. Select the devices that you want monitor.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox. If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

7. Click **Next** to display the **Events** tab.
8. Select the components and severities for which you want events to be forward.

Tip:

- To forward all hardware events, select **Match all events**.
- To forward audit events, select **Include All Audit events**.
- To forward warranty events, select **Include Warranty events**.

9. Click **Create**.
- Create an event filter for a specific subscription:
 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The New Event Forwarding page is displayed.
 2. Click the **Push Filters** tab.
 3. Select the link for the type of mobile device (Android or iOS) in the Name column of the table. The Change Push Notification dialog is displayed.
 4. Click the **Subscriptions** tab to display a list of active subscriptions.
 5. Select the subscription, and click the **Create** icon (). The **General** tab of New Event Filter dialog is displayed.
 6. Specify the name and option description for this event filter.
 7. Click **Next** to display the **Systems** tab.
 8. Select the devices that you want monitor.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox. If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not

yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

9. Click **Next** to display the **Events** tab.
10. Select the components and severities for which you want events to be forward.



Tip:

- To forward all hardware events, select **Match all events**.
- To forward audit events, select **Include All Audit events**.
- To forward warranty events, select **Include Warranty events**.

11. Click **Create**.

After you finish

From the Push Filters tab on the Event Forwarding page, you can perform the following actions on a selected event filter:

- Refresh the list of event filters by clicking the **Refresh** icon ()
- View details about a specific event filter by clicking the link in the **Name** column.
- Change the event filter properties and filter criteria by clicking the **Edit** icon ()

Delete the event filter by clicking the **Delete** icon ()

Working with jobs

Jobs are longer running tasks that are performed against one or more devices. You can schedule certain jobs to run only one time (immediately or at later time), on a reoccurring basis, or when a specific event occurs.

Jobs run in the background. You can see the status of each job from the jobs log.

Monitoring jobs

You can view a log of all jobs that are started by Lenovo XClarity Administrator. The jobs log includes jobs that are running, completed, or have errors.

About this task

Jobs are longer running tasks that are performed against one or more devices. For example, if you deploy an operating system to multiple servers, each server deployment is listed as a separate job.

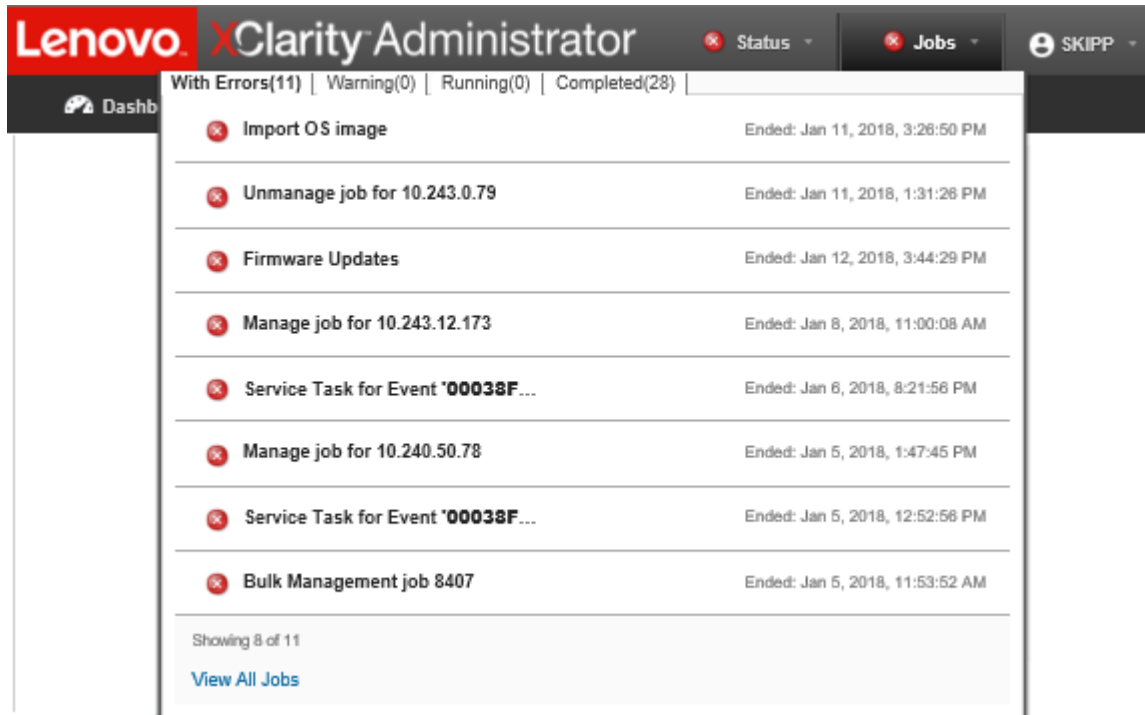
Jobs run in the background. You can see the status of each job from the jobs log.

The jobs log contains information about each job. The log can contain a maximum of 1000 jobs or 1 GB. When the maximum size is reached, the oldest jobs that completed successfully are deleted. If there are no jobs that completed successfully in the log, the oldest jobs that completed with warnings are deleted. If there are no jobs that completed successfully or with warnings in the log, the oldest jobs that completed with errors are deleted.

Procedure

Complete one of the following steps to display the jobs log.

- From the XClarity Administrator title bar, click **Jobs** to display a summary of jobs that are running, completed, and have errors.



From this pull down, you can click the following tabs:

- **Errors.** Displays a list of all jobs that have errors associated with them.
- **Warnings.** Displays a list of all jobs that have warnings associated with them.
- **Running.** Displays a list of all jobs that are currently in progress.
- **Completed.** Displays a list of all jobs that are completed.


Hover over a job entry in the pull down to get more information about the job, including the status, progress, and user that created the job.

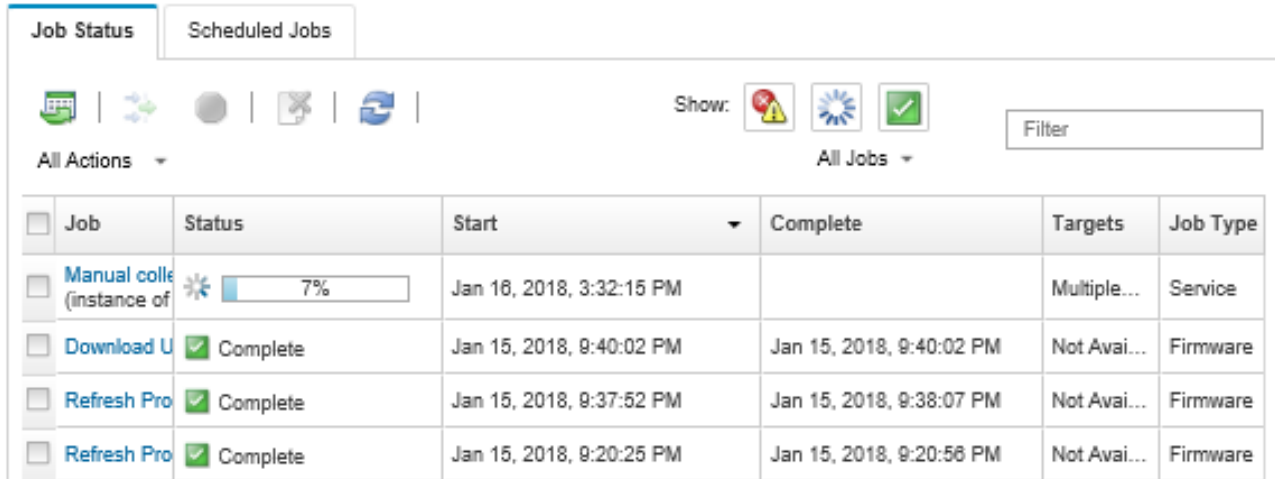
- From the XClarity Administrator title bar, click **Jobs**, and click the **View All Jobs** link to display the Jobs Status page.
- From the XClarity Administrator menu bar, click **Monitor** → **Jobs** and click the **Job Status** tab to display the Jobs Status page.

After you finish





The Jobs page is displayed with a list of all jobs for XClarity Administrator.

Jobs

 Jobs are longer running tasks performed against one or more target systems. After selecting a job, you can choose to cancel it, delete it, or obtain details about it.












The screenshot shows the 'Jobs' management interface. At the top, there are tabs for 'Job Status' and 'Scheduled Jobs'. Below the tabs is a toolbar with various icons for actions like refresh, delete, and search. A 'Show:' dropdown menu is set to 'All Jobs', and there is a 'Filter' input field. The main area contains a table with the following columns: Job, Status, Start, Complete, Targets, and Job Type. The table lists several jobs, including a 'Manual collection' job that is 7% complete and three 'Refresh Profile' jobs that are complete.

<input type="checkbox"/>	Job	Status	Start	Complete	Targets	Job Type
<input type="checkbox"/>	Manual collection (instance of)	 7%	Jan 16, 2018, 3:32:15 PM		Multiple...	Service
<input type="checkbox"/>	Download U...	 Complete	Jan 15, 2018, 9:40:02 PM	Jan 15, 2018, 9:40:02 PM	Not Avai...	Firmware
<input type="checkbox"/>	Refresh Pro...	 Complete	Jan 15, 2018, 9:37:52 PM	Jan 15, 2018, 9:38:07 PM	Not Avai...	Firmware
<input type="checkbox"/>	Refresh Pro...	 Complete	Jan 15, 2018, 9:20:25 PM	Jan 15, 2018, 9:20:56 PM	Not Avai...	Firmware

From this page, you can perform the following actions:

- Create job schedules by clicking the **Scheduled Jobs** tab (see [Scheduling jobs](#)).
- View more information about a specific job by clicking the job description in the **Jobs** column. A dialog is displayed with a list of subtasks (subjobs) and their targets, a summary of the subtasks including any necessary actions, and log details including the severity and timestamp for each message. You can choose to hide or show logs for child tasks.
- For scheduled jobs, view information about the job schedule by clicking the “this” link under the job description in the **Jobs** column.
- Change the number of jobs that are displayed per page. The default is 10 jobs. You can display 25, 50, or all jobs.
- Narrow the list of jobs that are displayed:
 - List only jobs from a specific source by clicking **Job Types** and choosing from the following options.
 - **All Job Types**
 - **Service**
 - **Management**
 - **Configuration**
 - **Firmware**
 - **Health**
 - **Power**
 - **Remote Access**
 - **System ID**
 - **OS Images**
 - **OS Deployment**
 - **OS Profile Export**
 - **Custom**
 - **Inventory**
 - **Unknown**
 - List only scheduled jobs that are associated with a specific schedule type by clicking **Schedule Types** and choosing from the following options.
 - **All Schedule Types**

- **One Time**
 - **Recurring**
 - **Triggered**
 - Hide or show jobs that have errors or warnings by clicking the **Hide error/warning jobs** icon (.
 - Hide or show jobs that are currently running by clicking the **Hide running jobs** icon (.
 - Hide or show jobs that are completed by clicking the **Hide completed jobs** icon (.
 - List only jobs that contain specific text by entering the text in the **Filter** field.
 - If filtering is applied to the page, remove the filter by clicking the **Show All Jobs** icon (.
 - Sort the jobs by column by clicking a column heading.
 - Export the jobs list as a CSV file by clicking the **Export as CSV** icon (.
- Note:** The timestamps in the exported log use the local time that is specified by the web browser.
- Cancel running jobs or subtasks by selecting one or more running jobs or subtasks and clicking the **Stop** icon (.
- Note:** It might take several minutes to cancel the job.
- Delete completed jobs or subtasks from the jobs log by selecting one or more completed jobs or subtasks and clicking the **Delete** icon (.
 - Export information about specific jobs by selecting the jobs and clicking the **Export as CSV** icon (.
 - Refresh the jobs log by clicking the **Refresh** icon (.

Scheduling jobs

You can create schedules in Lenovo XClarity Administrator to run certain tasks at specific times.

About this task

You can schedule the following types of jobs:

- Simple tasks, such as powering off and rebooting
- Collecting service data for specific devices
- Refreshing the firmware-update and OS device-driver catalogs from the Lenovo website
- Refreshing the XClarity Administrator updates catalog from the Lenovo website
- Downloading firmware from the Lenovo website
- Updating firmware and OS device drivers on managed devices
- Backing up XClarity Administrator data and settings
- Backing up and restoring switch configuration data


You can schedule jobs to run:

- Only one time (immediately or at a later time)
- On a recurring basis
- When a specific event occurs

Procedure

To create and schedule a job, complete the following steps.

- For complex tasks, such as updating firmware and collecting service data, create the job from the current the task page or dialog.

1. Click **Schedule** to create a schedule for running this task. The Schedule New Job dialog is displayed.
 2. Enter a name for the job.
 3. Specify when the job is to be run. The available options depend on the type of job. Some jobs cannot be recurring or triggered by an event
 - **One Time.** These jobs run only one time. Specify the date and time when you want this job to run.
 - **Recurring.** These jobs run more than one time. Specify the when and how often you want this job to run.
 - **Triggered by Event.** These jobs run when a specific event occurs.
 - a. Specify the date and time when you want this job to run, and click **Next**.
 - b. Select the event to trigger the job.
 4. Click **Create Job**.
- For simple tasks, such as powering on and rebooting, create the job schedule from the Jobs page.
 1. From the XClarity Administrator menu bar, click **Monitor → Jobs**, and click the **Scheduled Job** tab to display the Scheduled Jobs page.
 2. Click the **Create** icon () to display the Schedule New Jobs dialog.
 3. Enter a name for the job.
 4. Specify when the job is to be run.
 - **One Time.** These jobs run only one time.
 - a. Specify the date and time when you want this job to run, and click **Next**.
 - b. Select managed devices on which the job is to run.
 - **Recurring.** These jobs run more than one time.
 - a. Specify the when and how often you want this job to run.
 - b. Select managed devices on which the job is to run.
 - **Triggered by Event.** These jobs run when a specific event occurs.
 - a. Specify the date and time when you want this job to run, and click **Next**.
 - b. Select managed devices on which the job is to run, and click **Next**.
 - c. Select the event to trigger the job.
 5. Click **Create**.

After you finish

The Scheduled Jobs tab is displayed with a list of all job schedules in XClarity Administrator.





Jobs

? Jobs are longer running tasks performed against one or more target systems. After selecting a job, you can choose to cancel it, delete it, or obtain details about it.

<input type="checkbox"/>	Title	Schedule	State	Last Run	Last Result	Next Run	Targets	Created By	Action
<input type="checkbox"/>	My Delayed	One Time	Ended	Sep 22, 2022 Show Jobs..	Job started	Not Available	IMM2-40...	EERKO...	Custom

From this page, you can perform the following actions:

- View information about all active and completed jobs for a specific job schedule by clicking the link in the **Job** column.
 - Narrow the list of job schedules that are displayed by a specific schedule type by clicking **Schedule Types** and choosing from the following options:
 - **All Schedule Types**
 - **One Time**
 - **Recurring**
 - **Triggered**
 - Hide or show only job schedules that are in a specific state by clicking one of the following icons:
 - All scheduled jobs that are active by clicking the **Active** icon (✓).
 - All scheduled jobs that are not active by clicking the **Paused** icon (⏸).
 - All scheduled jobs that already ran and are not scheduled to run again by clicking the **Ended** icon (⊖).
 - List only scheduled jobs that contain specific text by entering the text in the **Filter** field.
 - Sort the scheduled jobs by column by clicking a column heading.
- View when the job ran last by looking at the **Last Run** column. View the status of the last run job by clicking the “Job Status” link in that column.
- View when the job is scheduled to run next by looking at the **Next Run** column. View a list of all future dates and times by clicking the “More” link in that column.
- Immediately run the job that is associated with the schedule by clicking the **Run** icon (▶▶).
- Disable or enable a job schedule by clicking the **Pause** icon (⏸) or **Activate** icon (▶) respectively.


- Copy and then modify a job schedule by clicking the **Copy** icon (.
- Edit a job schedule by clicking the **Edit** icon (.
- Delete one or more selected job schedules by clicking the **Delete** icon (.
- Export information about specific job schedules by selecting the schedules and clicking the **Export as CSV** icon (.
- Refresh the list of job schedule by clicking the **All Actions → Refresh**.

Adding a resolution and comments to a job

You can add a resolution and comments to a completed job, regardless of the success or error state. You can do this for a parent job and for subtasks in the job.

Procedure

Complete one of the following steps to add a resolution and comments to a job.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitor → Jobs**, and click the **Job Status** tab to display the Jobs Status page.
- Step 2. Click the link for the job in the **Job** column to display the job details.
- Step 3. Click the **Notes** icon () to display the Notes dialog.

From this dialog, you can see a history of all notes and resolutions that were added to the job. You can clear the history by clicking **Clear All Records**.

- Step 4. Choose one of the following resolutions.
 - **No Changes**
 - **Investigating**
 - **Resolved**
 - **Aborted**
- Step 5. Add a remark in the **Note** field.
- Step 6. Click **Apply**.

On the Job Status page, the resolution is displayed in the **Status** column for that job.

Chapter 3. Working with service and support

The Lenovo XClarity Administrator web interface provides a set of tools that you can use to define support contacts for each managed device, collect and send service files to Lenovo Support, set up automatic notification to service providers when certain serviceable events occur on specific devices, view service-ticket status, and warranty information. You can contact Lenovo Support to get help and technical assistance when you run into problems.

Learn more:  [XClarity Administrator: Service and support](#)

Getting bulletins from Lenovo

Lenovo continually updates the Support web site with announcements, including security alerts and impacts to online services. You can enable Lenovo to send these announcements to you as bulletins in the Lenovo XClarity Administrator web interface.

Before you begin

XClarity Administrator must have access to the Internet to receive announcements from Lenovo.

Ensure that a connection exists to the Internet addresses that are required by bulletins.


About this task

Getting bulletins is enabled by default.

When enabled, Lenovo sends the following types of bulletins.

- New releases of XClarity Administrator or firmware are available
- Security alerts, such as vulnerabilities were found that affect firmware or the management server
- Planned outages that impact Lenovo XClarity online services

You can view bulletins in several ways.

- New bulletins are shown in pop-up messages in the XClarity Administrator web interface.
- You can view a list of bulletins from the last 30 days from the Login page and by clicking the user-actions menu () and then clicking **Lenovo Bulletins Service**.
- You can set up an email forwarder that enables the **Include Bulletin events** option to send bulletins to you through email (see [Setting up event forwarding to an email service using SMTP](#) in the XClarity Administrator online documentation).

Procedure

Complete the following steps to enable receiving bulletins.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration** → **Service and Support**, and then click **Lenovo Bulletins Service** in the left navigation to display the Lenovo Bulletin Service page.
- Step 2. Select **I agree to receive bulletins from Lenovo**.
- Step 3. Click **Apply**.

Viewing warranty information

You can determine the warranty status (including extended warranties) of the managed devices.

Before you begin

Lenovo XClarity Administrator must have access to the following URLs to collect warranty information for the managed devices. Ensure that there are no firewalls blocking access to these URLs. For more information, see [Firewalls and proxy servers](#) in the XClarity Administrator online documentation.

- Lenovo Warranty Database (world-wide) – <https://ibase.lenovo.com/POIRequest.aspx>
- Lenovo Warranty Database (China only) – <http://service.lenovo.com.cn:83/webservice/NewProductQueryService.aspx>
- Lenovo Warranty Web Service – <http://supportapi.lenovo.com/warranty/> or <https://supportapi.lenovo.com/warranty/>

You can enable or disable these warranty URLs in XClarity Administrator by clicking **All Actions** → **Configure Warranty Links**.

Note: For RackSwitch device, the **Serial Number** column shows the entitled serial number.

Procedure

To view the warranty status of managed devices, complete the following steps.

- Step 1. From the XClarity Administrator menu bar, click **Administration** → **Service and Support**.
- Step 2. Click **Warranty** in the left navigation to display the Warranty page.

This page contains a table that lists warranty information (such as start date, stop date, and status) for each managed device.

Warranty

Expiration Warning (days):





All Actions

<input type="checkbox"/>	Endpoint	Product Name	Type-Model	Warranty Number	Serial Number	Start Date	Expiration Date
<input type="checkbox"/>	rpx-fc-xinyi2	Lenovo Con...	5462/AC1	3XL	06ERPEF	Apr 6, 2015, ...	Apr 15, 20...
<input type="checkbox"/>	IMM2-40f2e9a	Lenovo Syst...	5462/25Z	Not Available	1111111	Not Available	Not Availa
<input type="checkbox"/>	+ SN#Y011BG38	IBM Chassis...	7893/92X	Not Available	10007AA	Not Available	Not Availa
<input type="checkbox"/>	IMM2-40f2e9a	Lenovo Syst...	5464/AC1	3XL	06CHKBW	Sep 19, 201...	Sep 18, 20...
<input type="checkbox"/>	+ SN#Y030BG16	IBM Chassis...	7893/92X	Not Available	100086A	Not Available	Not Availa
<input type="checkbox"/>	+ SN#Y034BG16	IBM Chassis...	7893/92X	Not Available	100077A	Not Available	Not Availa
<input type="checkbox"/>	+ SN#Y034BG17	IBM Flex Sy...	8721/HC1	Not Available	KQ2Y83A	Not Available	Not Availa
<input type="checkbox"/>	YuanShan-GA	System x35...	5464/AC1	Not Available	J30A29W	Not Available	Not Availa
<input type="checkbox"/>	3850_20_Y		6241/AC1	Not Available	23Y6478	Not Available	Not Availa
<input type="checkbox"/>	+ SN#Y031BG23	IBM Chassis...	8721/HC1	IBM	23EHP64	Jul 24, 2011,...	Jul 24, 20...

[Lenovo Privacy Statement](#)

After you finish

From the Warranty page, you can perform the following actions:

- Set the when you want to be warned about the warranty expiration for a managed device using the **Expiration Warning** field. The default is 30 days before the warrant expires.
- Look up warranty information (if available) for a specific device on the Lenovo Support website by clicking the link in the **Status** column.
- Export warranty status for all managed devices to a CSV file by clicking the **Download CSV** icon (.
- Refresh warranty information for all managed devices by clicking the **Refresh Server List** icon (.

Setting up automatic problem notification

You can create a service forwarder that automatically send service data to your preferred service provider when a serviceable event occurs on specific managed devices. You can send service data for the device to Lenovo Support (Call Home), to your Lenovo service technician using the Lenovo Upload Facility, or to another service provider using SFTP.

You can create and enable up to 50 total service forwarders for Call Home, Lenovo Upload Facility, or SFTP.

Setting up automatic problem notification to Lenovo Support (Call Home)

You can create a service forwarder that automatically sends service data for any managed device to Lenovo Support using Call Home when certain serviceable events, such as an unrecoverable memory, are received

from specific managed devices so that the issue can be addressed. This service forwarder is named “Default Call Home.”

Lenovo is committed to security. When enabled, Call Home Lenovo Support Center when a device reports a hardware failure or when you choose to initiate a manual Call Home. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later; your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel.

Before you begin

Attention: You must accept the [Lenovo Privacy Statement](#) before you can transfer data to Lenovo Support.

Ensure that all ports that are required by Lenovo XClarity Administrator (including ports that are required for Call Home) are available before you enable Call Home. For more information about ports, see [Port availability](#) in the XClarity Administrator online documentation.

Ensure that a connection exists to the Internet addresses that are required by Call Home. For information about firewalls, see [Firewalls and proxy servers](#) in the XClarity Administrator online documentation.

If XClarity Administrator accesses the Internet through an HTTP proxy, ensure that the proxy server is configured to use basic authentication and is set up as a non-terminating proxy. For more information about setting up the proxy, see [Configuring network access](#) in the XClarity Administrator online documentation.

After you configure Call Home, the **Default Lenovo Call Home** service forwarder is added to the Service Forwarders page. You can edit this forwarder to configure additional settings, including which devices to associate with this forwarder. All devices are matched by default.

Attention: If **Match All Devices** is disabled, devices that are not explicitly selected, either individually or through resource groups, in any enabled Call Home forwarder *will not* initiate a Call Home to Lenovo Support for serviceable events.

Currently, there is no exclude Call Home option for specific devices. In the unlikely situation that you want to have a subset of devices not Call Home for serviceable events, you can create a mixture of static and dynamic resource groups that avoid the intended devices, and then add those resource groups to the Call Home forwarder.

Attention: If **Match All Devices** is not enabled for any Call Home forwarders, Call Home is not initiated for any devices. For this reason, it is recommended that you have at least one default Call Home forwarder with **Match All Devices** enabled as a last resort forwarder.

About this task

A *service forwarder* defines information about where to send the service data files when a serviceable event occurs. You can define up to 50 service forwarders.

- **If a Call Home service forwarder is not configured**, you can manually open a service ticket and send service files to the Lenovo Support Center by following the instructions on the [New Service Request webpage](#). For information about collecting and downloading service files, see [Collecting and downloading Lenovo XClarity Administrator service files](#) and [Collecting and downloading service data for a device](#).
- **If a Call Home service forwarder is configured but not enabled**, you can *manually* open a service ticket using the Call Home function to collect and transfer service files to the Lenovo Support Center at any time. For more information, see [Submitting a service request for hardware issues to the Lenovo Support Center](#).

- **If a Call Home service forwarder is configured and enabled**, XClarity Administrator *automatically* collects service data, opens a service ticket, and transfers service files to the Lenovo Support Center when a serviceable event occurs so that the issue can be addressed.

Important: When you enable a Call Home service forwarder in Lenovo XClarity Administrator, Call Home is disabled on each managed device to avoid duplicate problem records from being created. If you intend to discontinue using XClarity Administrator to manage your devices or if you intend to disable Call Home in XClarity Administrator, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time. For information about re-enabling Call Home on all managed devices when the service forwarder for Call Home is disabled, see [Re-enabling Call Home on all managed devices](#). For servers with XCC2, XClarity Administrator saves service data in two files in the repository.

- **Service file.** (.zip) This file contains service information and inventory in an easily readable format. This file is automatically sent to the Lenovo Support Center when a serviceable event occurs.
- **Debug file.** (.tzz) The file contains all service information, inventory, and the debug logs for use by Lenovo Support. You can manually send this file to Lenovo Support if additional information is needed to resolve an issue.

For other devices, XClarity Administrator saves service data (including service information, inventory, and debug logs) in a single service file in the repository. This file is sent to the Lenovo Support Center when a serviceable event occurs.

Although XClarity Administrator supports Call Home for ThinkAgile and ThinkSystem devices, the baseboard management controller for some ThinkAgile and ThinkSystem devices does not include Call Home support. Therefore, you cannot enable or disable Call Home on those devices themselves. Call Home can be enabled only for those devices at the XClarity Administrator level.

Call home is suppressed for repeated events for any device if a service ticket is open for that event on that device. Call Home is also suppressed for similar events for any ThinkAgile and ThinkSystem device if a service ticket is open for an event on that device. ThinkAgile and ThinkSystem events are 16-character strings in the following format `xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx` (for example, `806F010D0401FFFF`). Events are similar if they have the same reading type, sensor type, and entity ID. For example, if a service ticket is open for event `806F010D0401FFFF` on a specific ThinkAgile or ThinkSystem device, any events that occur on that device with event IDs like `xx6F01xx04xxxxxx`, where `x` is any alphanumeric character, are suppressed.

For information about viewing service tickets that were opened automatically by a Call Home service forwarder, see [Viewing service tickets and status](#).

Procedure

Complete the following steps to setup a service forwarded for Call Home.


- Setup Call Home for all managed devices (current and future):
 1. From the XClarity Administrator menu bar, click **Administration** → **Service and Support**.
 2. Click **Call Home Configuration** in the left navigation to display the Call Home Configuration page.

Call Home Configuration

Customer Number


Customer Number

Default Call Home Forwarder

 Lenovo Forwarder State: **Enabled**

Configure Call Home

* Contact Name	<input type="text" value="JohnDoe"/>
* Email	<input type="text" value="j_doe@lenovo.com"/>
* Phone Number	<input type="text" value="5551212"/>
* Company Name	<input type="text" value="SomeCompany"/>
* Street Address	<input type="text" value="100 Main St"/>
* City	<input type="text" value="SomeTown"/>
* State or Province	<input type="text" value="NY"/>
* Country or Region	<input type="text" value="UNITED STATES"/>
* Zip Code	<input type="text" value="10000"/>
Method for contact	<input type="text" value="Any"/>

 System Information

[Lenovo Privacy Statement](#)

Apply

Reset Configuration

Call Home Connection Test

- (Optional) Specify the default Lenovo customer number to use when reporting problems with XClarity Administrator.

Tip: You can find your customer number in the proof-of-entitlement email that you received when you purchased Lenovo XClarity Pro.


- Fill in the contact and location information.
- Select the preferred method of contact by Lenovo Support.
- (Optional) Fill in the system information.
- Click **Apply**.

A Call Home service forwarder named “Default Call Home” is created for all managed devices using the specified contact information.

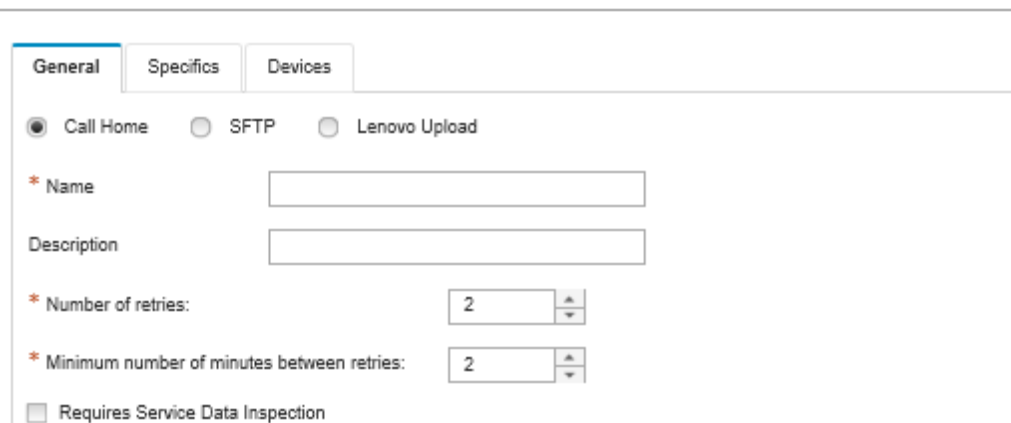
- Enable and test the “Default Call Home” service forwarder.
 - Click **Service Forwarder** in the left navigation to display the Service Forwarders page.
 - Select **Enable** in the **Status** column for the “Default Call Home” service forwarder.
 - Select the “Default Call Home” service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with the Lenovo Support Center.

You can monitor the test progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

Note: The service forwarder must be enabled before it can be tested

- Setup Call Home for specific managed devices:
 1. From the XClarity Administrator menu bar, click **Administration → Service and Support**.
 2. Click **Service Forwarders** in the left navigation to display the Service Forwarders page.
 3. Click the **Create Service Forwarder** icon () to display the New Service Forwarder dialog.
 4. Click the **General** tab.

New Service Forwarder



The screenshot shows the 'New Service Forwarder' dialog box with the 'General' tab active. It contains three radio buttons: 'Call Home' (selected), 'SFTP', and 'Lenovo Upload'. Below these are four input fields: 'Name', 'Description', 'Number of retries' (set to 2), and 'Minimum number of minutes between retries' (set to 2). At the bottom, there is a checkbox labeled 'Requires Service Data Inspection'.

- a. Select **Call Home** as the service forwarder:
 - b. Enter the name of the service forwarder and a description.
 - c. Specify the number of automatic-notification retries. The default is 2.
 - d. Specify the minimum number of minutes between retries. The default is 2.
 - e. (Optional) Click **Requires Service Data Inspection** if you want to inspect the service-data files before they are transferred, and optionally specify the e-mail address of the contact to be notified when service files must be inspected.
5. Click the **Specific** tab, and fill in the contact and system information.

Tip: To use the same contact and location information that is configured on the Call Home Configuration page, select **General Configuration** in the **Configuration** drop-down menu.

6. Click the **Devices** tab, and select the managed devices and resource groups for which you want this service forwarder to forward service files.

Tip: To forward service files for all managed devices (current and future), select the **Match all devices** checkbox.

7. Click **Create**. The service forwarder is added to the Service and Support page.
8. On the Service Forwarders page, select **Enable** in the **Status** column to enable the service forwarder.
9. Select the service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with the Lenovo Support Center.

You can monitor the test progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.




Note: The service forwarder must be enabled before it can be tested.

After you finish

From the Service and Support page, you can also perform the following actions:

- If **Requires Service Data Inspection** is selected and a serviceable event was received from one of the managed devices that is associated with the service forwarder, you must inspect service files before the files are forwarded to the service provider. For more information, see .
- Determine whether Call Home is enabled or disabled on a managed device by clicking **Endpoint Actions** in the left navigation and verifying the state in the **Call Home Status** column.

Tip: If “Unknown State” is displayed in the **Call Home Status** column, refresh the web browser to display the correct status.

- Define the support contact and location information for a specific managed device by clicking **Endpoint Actions** in the left navigation, selecting the device, and then clicking the **Create Contact Profile** icon () or **Edit Contact Profile** icon (). The contact and location information for the managed device is included in the service ticket that Call Home sends to the Lenovo Support Center. If unique contact and location information is specified for a managed device, that information is included in the service ticket. Otherwise, general information that is specified for the XClarity Administrator Call Home configuration (on the **Call Home Configuration** page or **Service Forwarders** page) is used. For more information, see Lenovo Support Center. For more information, see [Defining the support contacts for specific devices](#).
- View service tickets that have been submitted to the Lenovo Support Center by clicking **Service Ticket Status** in the left navigation. This page lists service tickets that have been opened automatically or manually by a Call Home service forwarder, the status, and service files that were transmitted to the Lenovo Support Center. For more information, see [Viewing service tickets and status](#).
- Collect service data for a specific device by clicking **Endpoint Actions** in the left navigation, selecting the device, and then clicking the **Collect Service Data** icon (). For more information, see [Collecting and downloading service data for a device](#).
- Manually open a service ticket in the Lenovo Support Center, collect service data for a specific device, and send those files to the Lenovo Support Center by clicking **Endpoint Actions** in the left navigation, selecting the device, and then clicking **All Actions → Perform Manual Call Home**. If the Lenovo Support Center requires additional data, the Lenovo Support might instruct you to recollect service data for that device or for another device.

For more information, see [Submitting a service request for hardware issues to the Lenovo Support Center](#).

- Re-enable Call Home on all managed devices by clicking **Endpoint Actions** in the left navigation, and then clicking **All Actions → Enable Call Home on all devices**.

When you enable a Call Home service forwarder in Lenovo XClarity Administrator, Call Home is disabled on each managed device to avoid duplicate problem records from being created. If you intend to discontinue using XClarity Administrator to manage your devices or if you intend to disable Call Home in XClarity Administrator, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time.

Setting up automatic problem notification to the Lenovo Upload Facility

You can create a service forwarder that automatically sends service data for any managed device to your Lenovo service technician using the Lenovo Upload Facility when certain serviceable events, such as an unrecoverable memory, are received from specific managed devices so that the issue can be addressed. This service forwarded is named “Default Lenovo Upload Facility.”

Lenovo is committed to security. Your business data is never transmitted. Access to service data in the Lenovo Upload Facility is restricted to authorized service personnel.

Before you begin

Attention: You must accept the [Lenovo Privacy Statement](#) before you can transfer data to Lenovo Support.

Ensure that all ports that are required by Lenovo XClarity Administrator are available before you set up a service forwarder. For more information about ports, see [Port availability](#) in the XClarity Administrator online documentation.

Ensure that a connection exists to the required Internet addresses are required by the Lenovo Upload Facility. For information about firewalls, see [Firewalls and proxy servers](#) in the XClarity Administrator online documentation.

If XClarity Administrator accesses the Internet through an HTTP proxy, ensure that the proxy server is configured to use basic authentication and is set up as a non-terminating proxy. For more information about setting up the proxy, see [Configuring network access](#) in the XClarity Administrator online documentation.

Note: If multiple service forwarders are set up for the same device, only one of the service forwarders transfers service data. The email and upload URL that is used depends on which service forwarder is triggered first.

About this task

A *service forwarder* defines information about where to send the service data files when a serviceable event occurs. You can define up to 50 service forwarders.

- **If a Lenovo Upload Facility service forwarder is configured but not enabled**, you can *manually* transfer collected service files to the Lenovo Upload Facility at any time. For more information, see [Submitting a service request for hardware issues to the Lenovo Support Center](#).
- **If a Lenovo Upload Facility service forwarder is configured and enabled**, XClarity Administrator *automatically* collects service data and transfers the service file to the Lenovo Upload Facility when a serviceable event occurs so that the issue can be addressed.

For servers with XCC2, XClarity Administrator saves service data in two files in the repository.

- **Service file.** (.zip) This file contains service information and inventory in an easily readable format. This file is automatically sent to the Lenovo Upload Facility when a serviceable event occurs.
- **Debug file.** (.tzz) The file contains all service information, inventory, and the debug logs for use by Lenovo Support. You can manually send this file to Lenovo Support if additional information is needed to resolve an issue.

For other devices, XClarity Administrator saves service data (including service information, inventory, and debug logs) in a single service file in the repository. This file is sent to the Lenovo Upload Facility when a serviceable event occurs.

Procedure

Complete the following steps to setup a service forwarder for the Lenovo Upload Facility.


- Setup a service forwarder to Lenovo Upload Facility for all managed devices:
 1. From the XClarity Administrator menu bar, click **Administration** → **Service and Support**.
 2. Click **Lenovo Upload Facility** in the left navigation to display the Lenovo Upload Facility page.

Lenovo Upload Facility

From this page, you can configure the Lenovo Upload Facility. When this is configured, you can choose to collect service data from the management server or managed endpoints, and the data will be transferred directly to the Lenovo, for use in resolving issues with those managed endpoints, or the management server. It enables this additional capability on those service collection pages.

In addition, when this is configured, you can choose to create a new service forwarder that automatically sends service data for any managed endpoint to Lenovo when certain serviceable events occur on that managed endpoint. This service forwarder is named "Default Lenovo Upload Facility." [Learn more.](#)

Default Lenovo Upload Facility Forwarder

 Forwarder state: **Enabled**

Configure Lenovo Upload Facility

Provide the email address that you typically use to communicate with Lenovo Support. This email address is used to correlate the reporter with the issue. Lenovo does not directly communicate with or sell this email address. Please enter a prefix to be prepended to file names. This will be used by the support team to correlate uploaded files with the reporter of an issue. Its suggested that it be your company name or something else that will uniquely identify this instance of XClarity Administrator.

* Prefix

JVanh

* Email

jvanh@lenovo.com

[Lenovo Privacy Statement](#)

Apply

Reset Configuration

Lenovo Upload Connection Test


3. Enter the email address and URL that was provided to you by Lenovo Support.
4. Click **Apply**.

A service forwarder named "Default Lenovo Upload Facility" is created for all managed devices using the specified contact information.

5. Enable and test the "Default Lenovo Upload Facility" service forwarder.
 - a. Click **Service Forwarders** in the left navigation to display the Service Forwarders page.
 - b. Select **Enable** in the **Status** column for the "Default Lenovo Upload Facility" service forwarder.
 - c. Select the "Default Lenovo Upload Facility" service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with the Lenovo Upload Facility.

You can monitor the test progress by clicking **Monitoring** → **Jobs** from the XClarity Administrator menu bar.

Note: The service forwarder must be enabled before it can be tested.

- Setup a service forwarder to Lenovo Upload Facility for specific managed devices:
 1. From the XClarity Administrator menu bar, click **Administration** → **Service and Support**. The Service and Support page is displayed.
 2. Click **Service Forwarders** in the left navigation to display the Service Forwarders page.
 3. Click the **Create Service Forwarder** icon () to display the New Service Forwarder dialog.
 4. Click the **General** tab.

New Service Forwarder

The screenshot shows a configuration form for a new service forwarder. It has three tabs: 'General', 'Specifics', and 'Devices'. The 'General' tab is selected. At the top, there are three radio buttons: 'Call Home' (selected), 'SFTP', and 'Lenovo Upload'. Below these are two text input fields: '* Name' and 'Description'. There are two spinner controls: '* Number of retries' (set to 2) and '* Minimum number of minutes between retries' (set to 2). At the bottom, there is a checkbox labeled 'Requires Service Data Inspection'.

- a. Select **Lenovo Upload** for the service forwarder.
 - b. Enter the name of the service forwarder and a description.
 - c. Specify the number of automatic-notification retries. The default is 2.
 - d. Specify the minimum number of minutes between retries. The default is 2.
 - e. (Optional) Click **Requires Service Data Inspection** if you want to inspect the service files before they are transferred, and optionally specify the e-mail address of the contact to be notified when service files must be inspected.
5. Click the **Specific** tab, and fill in the email address and upload URL that was provided to you by Lenovo Support.
 6. Click the **Devices** tab, and select the managed devices and resource groups for which you want this service forwarder to forward service data.


Tip: To forward service data for all managed devices (current and future), select the **Match all devices** checkbox.



7. Click **Create**. The service forwarder is added to the Service and Support page.
8. On the Service and Support page, select **Enable** in the **Status** column to enable the service forwarder.
9. Select the service forwarder, and click **Test Service Forwarders** to generate a test event for each service forwarder and verify that XClarity Administrator is able to transfer to the Lenovo Upload Facility.

Note: The service forwarder must be enabled before it can be tested.

After you finish

From the Service and Support page, you can also perform the following actions:

- If **Requires Service Data Inspection** is selected and a serviceable event was received from one of the managed devices that is associated with the service forwarder, you must inspect and service files before the files are forwarded to the service provider. For more information, see [Inspecting service files](#).
- Modify the service-forwarder information by clicking **Service Forwarders** in the left navigation and clicking the **Edit Service Forwarder** icon (.
- Enable or disable a service provider by clicking **Service Forwarders** and selecting **Enable** or **Disable** in the **Status** column.

- Delete the service provider by clicking **Service Forwarders** and clicking the **Delete Service Forwarders** icon ()
- Collect service data for a specific device by clicking **Endpoint Actions** in the left navigation, selecting the device, and then clicking the **Collect Service Data** icon () . For more information, see [Collecting and downloading service data for a device](#).

Setting up automatic problem notification to a preferred service provider

You can create a service forwarder that automatically sends service data to your preferred service provider using SFTP when certain serviceable events, such as an unrecoverable memory error, are received from specific managed devices so that the issue can be addressed.

Before you begin

Attention: You must accept the [Lenovo Privacy Statement](#) before you can transfer data to Lenovo Support.

Ensure that all ports that are required by XClarity Administrator (including ports that are required for call home) are available before you setup a service forwarder. For more information about ports, see [Port availability](#) in the XClarity Administrator online documentation.

Ensure that a connection exists to the Internet addresses that are required by the service provider.

If you choose to use Lenovo Support, ensure that a connection exists to the Internet addresses that are required by Call Home. For information about firewalls, see [Firewalls and proxy servers](#) in the XClarity Administrator online documentation.

If XClarity Administrator accesses the Internet through an HTTP proxy, ensure that the proxy server is set up as a non-terminating proxy. For more information about setting up the proxy, see [Configuring network access](#) in the XClarity Administrator online documentation.

About this task

A *service forwarder* defines information about where to send the service data files when a serviceable event occurs. You can define up to 50 service forwarders

For each service forwarder, you can choose to automatically transfer service data to Lenovo Support (called *Call Home*), to the Lenovo Upload Facility, or to another service provider using SFTP. For information about setting up a service forwarder for Call Home, see [Setting up automatic problem notification](#). For information about setting up a service forwarder for the Lenovo Upload Facility, see [Setting up automatic problem notification to the Lenovo Upload Facility](#).

If a service forwarder is configured and enabled for SFTP, XClarity Administrator *automatically* transfers collects service data and transfers service files to the specified SFTP site for your preferred service provider.

For servers with XCC2, XClarity Administrator saves service data in two files in the repository.


- **Service file.** (.zip) This file contains service information and inventory in an easily readable format. This file is automatically sent to your preferred service provider when a serviceable event occurs.
- **Debug file.** (.tzz) The file contains all service information, inventory, and the debug logs for use by Lenovo Support. You can manually send this file to Lenovo Support if additional information is needed to resolve an issue.

For other devices, XClarity Administrator saves service data (including service information, inventory, and debug logs) in a single service file in the repository. This file is sent to your preferred service provider when a serviceable event occurs.

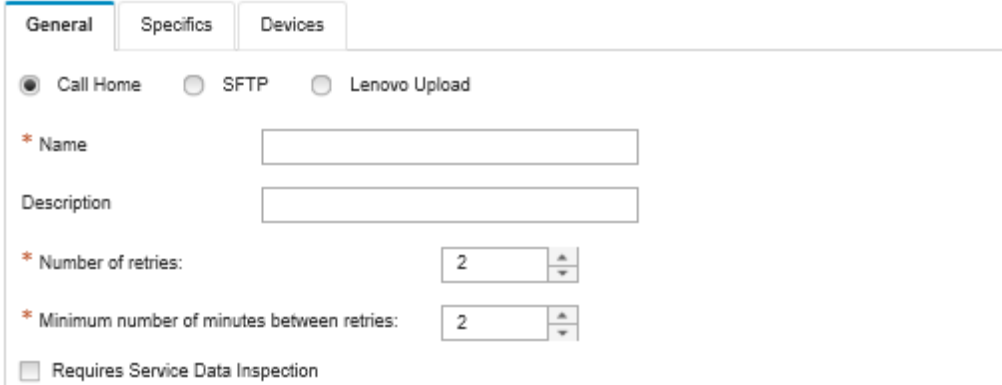
Note: If multiple SFTP service forwarders are set up for the same device, only one of the service forwarders transfers service data. The address and port that is used depends on which service forwarder is triggered first.

Procedure

Complete the following steps to define and enable a service forwarder.

- Step 1. From the XClarity Administrator menu bar, click **Administration** → **Service and Support**. The Service and Support page is displayed.
- Step 2. Click **Service Forwarders** in the left navigation to display the Service Forwarders page.
- Step 3. Click the **Create Service Forwarder** icon () to display the New Service Forwarder dialog.
- Step 4. Click the **General** tab.

New Service Forwarder



1. Select **SFTP** for the service forwarder:
 2. Enter the name of the service forwarder and a description.
 3. Specify the number of automatic-notification retries. The default is 2.
 4. Specify the minimum number of minutes between retries. The default is 2.
 5. (Optional) Click **Requires Service Data Inspection** if you want to inspect the service files before they are transferred, and optionally specify the e-mail address of the contact to be notified when service files must be inspected.
- Step 5. Click the **Specific** tab, and fill in the following information:
- IP address and port number of the SFTP server
 - User ID and password for authentication to the SFTP server
- Step 6. Click the **Device** tab, and select the managed devices and resource groups for which you want this service forwarder to forward service data.
- Tip:** To forward service data for all managed devices (current and future), select the **Match all devices** checkbox.
- Step 7. Click **Create**. The service forwarder is added to the Service and Support page
- Step 8. On the Service and Support page, select **Enable** in the **Status** column to enable the service forwarder.






Step 9. Optional: To prevent serviceable events that are in the list of excluded events from automatically opening problem reports, select **No** next to the question **Do you want excluded events to open problem reports?**

Step 10. Select the service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with each service provider.

Note: The service forwarder must be enabled before it can be tested.

After you finish

From the Service and Support page, you can also perform the following actions:

- If **Requires Service Data Inspection** is selected and a serviceable event was received from one of the managed devices that is associated with the service forwarder, you must inspect and service files before the files are forwarded to the service provider. For more information, see [Inspecting service files](#).
- Modify the service-forwarder information by clicking **Service Forwarders** in the left navigation and clicking the **Edit Service Forwarder** icon (.
- Enable or disable a service provider by clicking **Service Forwarders** and selecting **Enable** or **Disable** in the **Status** column.
- Delete the service provider by clicking **Service Forwarders** and clicking the **Delete Service Forwarder** icon (.
- Define the support contact and location information for a specific managed device by clicking **Endpoint Actions** in the left navigation, selecting the device, and then clicking the **Create Contact Profile** icon () or **Edit Contact Profile** icon (). The contact and location information for the managed device is included in the problem record that call home creates in the Lenovo Support Center. If unique contact and location information is specified for a managed device, that information is included in the problem record. Otherwise, general information that is specified for the XClarity Administrator call-home configuration (on the **Call Home Configuration** page or **Service Forwarders** page) is used. For more information, see [Defining the support contacts for specific devices](#).
- Collect service data for a specific device by clicking **Endpoint Actions**, selecting the device, and then clicking the **Collect Service Data** icon (). For more information, see [Collecting and downloading service data for a device](#).

For more information about these service and support tasks, see [Working with service and support](#).

Changing the service-recovery password

If Lenovo XClarity Administrator becomes unresponsive and cannot be recovered, you can use the service-recovery password to collect and download service data and logs for that XClarity Administrator instance.

Before you begin

You must have **lxc-service-admin** or **lxc-supervisor** authority to change the password.

Procedure

To change the service-recovery password, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration** → **Service and Support**. The Service and Support page is displayed.

- Step 2. Click **Service Recovery Password** in the left navigation to display the Service Recovery Password page.
- Step 3. Enter the new password
- Step 4. Click **Apply**.

Inspecting service files

You can set up a service forwarder so that the service files must be inspected and accepted before the files are sent.

About this task

The **Requires Attention** column in the service-forwarder table identifies whether service files require inspection before they are forwarded to the service provider. If one or more service files are available for inspection, **Yes** is displayed in the column; otherwise, **No** is displayed.

Procedure

Complete the following steps to forward specific service files to the service provider.

- Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.
- Step 2. Click **Service Forwarders** in the left navigation to display a table of service forwarders.
- Step 3. Click the **Yes** link in the **Requires Attention** column to display the Required Attention dialog with a list of service files that require inspection.
- Step 4. Select one or more the service files, and click **Download** to download and inspect the file.
- Step 5. Select one or more the service files again, and click **Accept** to start the transfer of the file to the configured service provider.

Note: If you choose **Decline** instead, the service files are removed from the Requires Attention dialog but remain in the repository until you delete them.

Defining the support contacts for specific devices


Specifying support-contact information that is unique for one or more specific devices is valuable in cases where devices are administered by multiple users.

About this task

If support-contact information is defined for a device, the device-specific information is included in the problem records that are opened automatically by Call Home for that device. If device-specific information is not defined, then the general contact information for Lenovo XClarity Administrator that is defined on the **Service Forwarders** page or **Call Home Configuration** page is included instead.



Procedure

Complete the following steps to define the support-contact and location information for a specific device.

- Step 1. From the XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.
- Step 2. Click **Endpoint Actions** in the left navigation to display the Endpoint Actions page
- Step 3. Select one or more devices, and click the **Create Contact Profile** icon () to display the Create Contact Profile dialog.

Step 4. Fill in the required fields, and then click **Save**.

After you finish

After you define contact information for a device, you can modify or delete the contact information by selecting the device and clicking the **Edit Contact Profile** icon () or the **Delete Contact Profile** icon ()

Note: If a contact profile does not exist for the selected device, the Create Contact Profile dialog is displayed when you attempt to edit the profile.

Collecting and downloading service data for a device

When there is an issue on a managed device that requires the assistance of a service provider to resolve, you can use the Lenovo XClarity Administrator web interface to manually collect service data (including service information, inventory, and debug logs) for that device to help identify the cause of the issue. The service data is saved as a service file in tar.gz format. You can download or send the service files to your preferred service provider.

About this task

You can run up to 20 service-data collection processes at a time.

For servers with XCC2, XClarity Administrator saves service data in two files in the repository.

- **Service file.** (.zip) This file contains service information and inventory in an easily readable format.
- **Debug file.** (.tzz) The file contains all service information, inventory, and the debug logs for use by Lenovo Support.

For other devices, XClarity Administrator saves service data (including service information, inventory, and debug logs) in a single service file in the repository.

When a managed device generates a serviceable event that triggers Call Home, XClarity Administrator automatically collects service data for that device. If a service forwarder is configured and enabled, XClarity Administrator also sends the service file to the specified service provider (for example, the Lenovo Support Center using Call Home or an SFTP site). If the service provider requires additional data, you might be instructed to re-collect service data for that device or for another device using the procedure described below.

When the service-data repository reaches its maximum capacity, the oldest set of files is deleted to make room for the new file.

Notes:

- For stacked switches, you can collect service data for the *master switch* and *standby switches* that have IP addresses that are accessible by XClarity Administrator. You cannot collect service data for *member switches* or switches that are in protected mode.
- You cannot collection service data for switches that support stack mode but are in standalone mode.


For information about downloading service data for XClarity Administrator, see [Collecting and downloading Lenovo XClarity Administrator service files](#).

For information about manually sending service data to the Lenovo Support Center, see [Submitting a service request for hardware issues to the Lenovo Support Center](#).

For information about setting up an automated service forwarder, see [Setting up automatic problem notification](#).

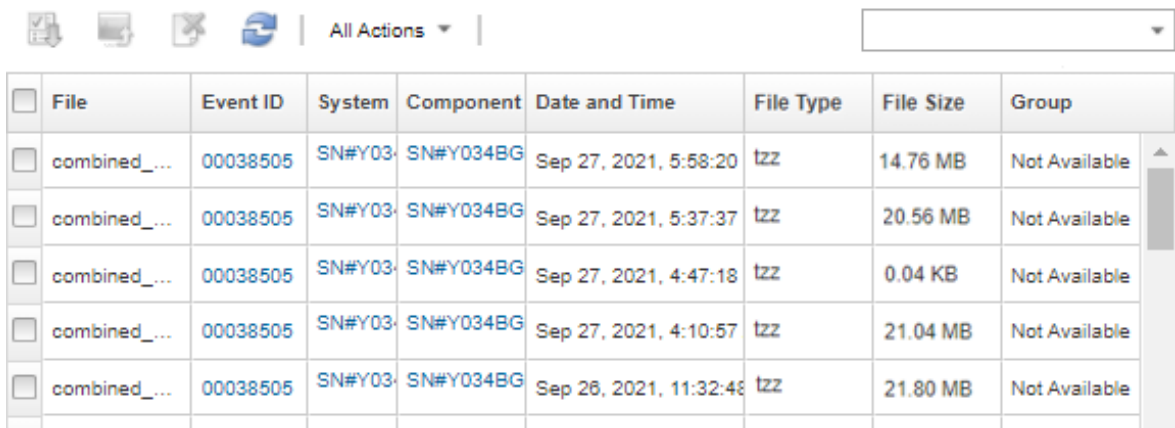
Procedure

Complete the following steps to collect and download service data for a specific managed device.

- Step 1. From the XClarity Administrator menu bar, click **Administration** → **Service and Support**.
- Step 2. Click **Endpoint Actions** in the left navigation to display the Endpoint Actions page.
- Step 3. Select the device for which you want to collect service data, and click the **Collect Service Data** icon (.
- Step 4. Optionally save the service file to your local system.
- Step 5. Click **Device Service Data** in the left navigation to display the Device Service Data page. The service-data archive is listed in the table.

Endpoint Service Data

Use this tab to download diagnostic files collected from the endpoints.





The screenshot shows the 'Endpoint Service Data' interface. At the top, there is a toolbar with icons for file operations and a dropdown menu labeled 'All Actions'. Below the toolbar is a table with the following columns: File, Event ID, System, Component, Date and Time, File Type, File Size, and Group. The table contains five rows of data, each representing a service data archive.

<input type="checkbox"/>	File	Event ID	System	Component	Date and Time	File Type	File Size	Group
<input type="checkbox"/>	combined_...	00038505	SN#Y03	SN#Y034BG	Sep 27, 2021, 5:58:20	tzz	14.76 MB	Not Available
<input type="checkbox"/>	combined_...	00038505	SN#Y03	SN#Y034BG	Sep 27, 2021, 5:37:37	tzz	20.56 MB	Not Available
<input type="checkbox"/>	combined_...	00038505	SN#Y03	SN#Y034BG	Sep 27, 2021, 4:47:18	tzz	0.04 KB	Not Available
<input type="checkbox"/>	combined_...	00038505	SN#Y03	SN#Y034BG	Sep 27, 2021, 4:10:57	tzz	21.04 MB	Not Available
<input type="checkbox"/>	combined_...	00038505	SN#Y03	SN#Y034BG	Sep 26, 2021, 11:32:48	tzz	21.80 MB	Not Available

After you finish

From the Device Service Data page, you can also perform these tasks.

- Manually send service files directly to a Lenovo service technician (see [Transferring service files to Lenovo Support](#)).
- Manually send service files to the Lenovo Support Center and open a service ticket, see [Submitting a service request for hardware issues to the Lenovo Support Center](#).
- Attach service files to an existing service ticket and send to Lenovo Support Center by selecting the files and clicking **Attach to Service Ticket**. Then, select the service ticket, and click **Associate**.
- Download service files by selecting one or more files and clicking the **Download Selected Service Files** icon (). If multiple files are selected, the files are compressed into a single .tar.gz file before downloading.
- Remove service files that are no longer needed by selecting one or more files and clicking the **Delete Selected Service Files** icon (.

Collecting and downloading Lenovo XClarity Administrator service files

You can manually collect service data for Lenovo XClarity Administrator and specific managed devices, and then save the information as a service file in tar.gz format and the download or send the service files to your preferred service provider to get assist in resolving issues as they arise.

About this task

Note: Ensure that you *do not* already have a job in progress for downloading all service files (see [Monitoring jobs](#)). If a user started a job that is still in progress, that same user must wait until the job completes before attempting to download all service files again; otherwise, the second attempt will fail.

Work with Lenovo Support to determine if you should download all or specific service files or logs.

Up to 100 service files for XClarity Administrator can be stored in the repository.

When you download XClarity Administrator service data and logs, you can choose to include service data for specific devices in the downloaded file. You can choose to use service files that already exist or to collect current service data as part of the download process.

Attention: Do not change the number of service files to keep unless directed to do so by your service provider.

Procedure

To collect and download the XClarity Administrator service data or logs, complete the following steps.

- Step 1. From the XClarity Administrator menu bar, click **Administration → Service and Support**.
- Step 2. Click **Management Server Files** in the left navigation to display the Management Server Files page.

Management Server Files

Use this tab to download diagnostic files from the Lenovo® XClarity Administrator.

Number of diagnostic file instances to keep :

Apply


 **Download All Service Data**



All Actions ▾

<input type="checkbox"/>	Date and Time ▾	File	Type	Description
<input type="checkbox"/>	Sep 27, 2021, 5:53:30 PM	ssCapture[id-4003]_20.tar.gz	Exception	Big gap of missing events detected b
<input type="checkbox"/>	Sep 27, 2021, 9:15:11 AM	ssCapture[id-4002]_19.tar.gz	Exception	FFDC EP Collect - Name: IO Module
<input type="checkbox"/>	Sep 27, 2021, 9:15:05 AM	ssCapture[id-4002]_18.tar.gz	Exception	FFDC EP Collect - Name: IO Module
<input type="checkbox"/>	Sep 27, 2021, 7:07:44 AM	ssCapture[id-4003]_17.tar.gz	Exception	Missing events detected between ma
<input type="checkbox"/>	Sep 27, 2021, 5:25:35 AM	ssCapture[id-4003]_16.tar.gz	Exception	Missing events detected between ma
<input type="checkbox"/>	Sep 26, 2021, 4:40:41 PM	ssCapture[id-4003]_15.tar.gz	Exception	Missing events detected between ma
<input type="checkbox"/>	Sep 26, 2021, 3:59:33 PM	ssCapture[id-4002]_14.tar.gz	Exception	FFDC EP Collect - Name: IO Module
<input type="checkbox"/>	Sep 26, 2021, 3:59:30 PM	ssCapture[id-4002]_13.tar.gz	Exception	FFDC EP Collect - Name: IO Module
<input type="checkbox"/>	Sep 23, 2021, 8:07:41 PM	ssCapture[id-4003]_12.tar.gz	Exception	Missing events detected between ma
<input type="checkbox"/>	Sep 23, 2021, 5:43:53 PM	ssCapture[id-4002]_11.tar.gz	Exception	FFDC EP Collect - Name: ite-bv-1524
<input type="checkbox"/>	Sep 22, 2021, 8:12:58 PM	ssCapture[id-2001]_10.tar.gz	Exception	Failed to load Data Management plug
<input type="checkbox"/>	Sep 22, 2021, 6:58:59 PM	ssCapture[id-2001]_9.tar.gz	Exception	Failed to load Data Management plug

Step 3. Choose to download all service data or all service logs.

- Click  **Download All Service Data** to download all service files, management server logs, and specific device service files.
- Click **All Actions** → **Download All Service Logs** to download all management server logs and specific device service files.

A message is displayed that shows the estimated amount of data to be downloaded. Downloading service files might take a significant amount of time, depending on the number and size of the files

Step 4. Optional: Choose to **Include service data that was already collected for managed devices**, select the service-data files to include, and click **Apply**.

Step 5. Optional: Choose **Select the managed devices for which you want to collect new service data**, select the target devices, and then click **Apply**.

Step 6. Choose to send the service files to Lenovo Support or save the files to your local system or to network storage. The service data or log files are compressed into a single .tar.gz file before sending.

- If you click **Lenovo Upload**, optionally enter a case number and then click **OK** to collect and transfer the service files to the Lenovo Upload Facility.

Note: It is recommended that you provide the case number to make it easier for Lenovo Support to locate the file.



- If you click **Save locally**, use your web browser functions to save the file to the local system.
- If you click **Save to network storage**, specify the IP address, credentials, directory and port, and click Save to transfer the service files to the remote server.

After you finish

From the Management Server Files page, you can also perform these tasks:

- Download existing service files by selecting one or more the files and clicking **All Actions → Download Selected Service Files**.

You can choose to send the service files to Lenovo Support or save the files to your local system or to network storage. If multiple files are selected, the files are compressed into a single .tar.gz file before sending.

- Delete one or more selected service files by clicking the **Delete Selected Service Files** icon (.
- Delete all service files by clicking the **Clear All Service Files** icon (.
- Delete all management server logs by clicking the **All Actions → Clear All Service Logs**.

Collecting and downloading service files for an unresponsive Lenovo XClarity Administrator

If Lenovo XClarity Administrator becomes unresponsive and cannot be recovered, you can collect and download service data and logs for that XClarity Administrator instance. Service data and logs are downloaded as a service file in tar.gz format to your local system

Before you begin

The XClarity Administrator web interface works with the following web browsers.

- Chrome™ 48.0 or later (55.0 or above for Remote Console)
- Firefox® ESR 38.6.0 or later
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 or later (IOS7 or later and OS X)

Ensure that you log in to the web interface from a system that has network connectivity to system on which XClarity Administrator is installed.

Procedure

To collect and download service data or logs for an unresponsive XClarity Administrator instance, complete the following steps.

- Step 1. Point your browser to the IP address of the XClarity Administrator virtual machine using the following URL.

`https://<IP_address>/backupffd`

For example:

`https://192.0.2.0/backupffd`

Step 2. Specify the service-recovery password in the **passKey** field.

This is the password that you specified when you initially setup XClarity Administrator or changed the password on the **Service Recovery Password** tab on the Service and Support page (see [Changing the service-recovery password](#)).

Step 3. Select the types of files that you want to collect.

- **All Service Data.** Collect all service files and management-server logs.
- **All Service Logs.** Collect all management-server logs.

Step 4. Click **Collect**, and then use your web browser functions to save the file to your local system. The service data or log files are compressed into a single .tar.gz file before sending.

Submitting a service request for hardware issues to the Lenovo Support Center

If Call Home is enabled using a service forwarder and a serviceable event occurs on a managed device, Lenovo XClarity Administrator automatically opens a service ticket, collects service files for the managed device, and sends the files to the Lenovo Support Center. You can also manually collect and download service files for a managed device and send the files to the Lenovo Support Center at any time using XClarity Administrator. Opening a service ticket starts the process of determining a resolution to your hardware issues by making the pertinent information available to Lenovo Support quickly and efficiently. Lenovo service technicians can start working on your resolution as soon as you have completed and opened a service ticket.

Lenovo is committed to security. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later; your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel

Before you begin

Attention: You must accept the [Lenovo Privacy Statement](#) before you can transfer data to Lenovo Support.

- Ensure that the Call Home contact information is configured.
 1. From the XClarity Administrator menu bar, click **Administration** → **Service and Support**. The Service and Support page is displayed.
 2. Click **Call Home Configuration** in the left navigation to display the Call Home Configuration page.
 3. Fill in the contact and location information.
 4. Optional: Fill in the system information.
 5. Click **Apply**.
- Ensure that all ports that XClarity Administrator requires (including ports that are required for Call Home) are available before you enable Call Home. For more information about ports, see [Port availability](#) in the XClarity Administrator online documentation.
- Ensure that a connection exists to the Internet addresses that are required by Call Home. For information about firewalls, see [Firewalls and proxy servers](#) in the XClarity Administrator online documentation
- If XClarity Administrator accesses the Internet through an HTTP proxy, ensure that the proxy server is configured to use basic authentication and is set up as a non-terminating proxy. For more information about setting up the proxy, see [Configuring network access](#) in the XClarity Administrator online documentation.

About this task

On the Endpoints Actions page, the **Call Home Status** column indicates whether Call Home is enabled on the baseboard management controller. A value of "Not Applicable" indicates that Call Home is not supported by the management controller. XClarity Administrator can perform a Call Home for a device regardless of whether the management controller supports Call Home. To determine whether Call Home is supported for a specific device,

For more information about configuring and enabling Call Home to automatically send service data to Lenovo Support Center, see [Setting up automatic problem notification to Lenovo Support \(Call Home\)](#).

For information about manually collecting and downloading service data, see [Collecting and downloading service data for a device](#) and [Collecting and downloading Lenovo XClarity Administrator service files](#).

Procedure

Complete the following steps to manually open a service ticket.

- If Call Home is configured but not enabled, perform the following steps to open a service ticket, collect and download service data, and send the files to the Lenovo Support Center:
 1. From the XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.
 2. Click **Endpoint Actions** in the left navigation to display the Endpoint Actions page.
 3. Select the device, and click the **All Action → Perform Manual Call Home**.
Tip: You can test communication with the Lenovo Support Center to ensure that Call Home is set up correctly without actually sending data to Lenovo Support by clicking **All Action → Perform Call Home Test**.
 4. Provide a description of the problem that is being reported, including relevant event IDs.
 5. Click **OK**.
- If Call Home is not configured or enabled, you can submit a service request by calling the Lenovo Support Line. For more information, see [Getting help and technical assistance](#).

After you finish

You can monitor open service tickets from the **Service Ticket Status** page (see [Viewing service tickets and status](#)).

Reporting XClarity Administrator problems


When you submit a service request to report software (management server) problems, Lenovo XClarity Administrator opens a service ticket, collects service data from the management server, and sends the files to the Lenovo Support Center using Call Home. Opening a service ticket starts the process of determining a resolution to your software problems by making the pertinent information available to Lenovo Support quickly and efficiently. Lenovo service technicians can start working on your resolution as soon as you have completed and opened a service ticket.

Lenovo is committed to security. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later; your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel


Before you begin

Attention: You must accept the [Lenovo Privacy Statement](#) before you can transfer data to Lenovo Support.

- Before submitting a problem request for XClarity Administrator, consider finding help using the following resources:

- Submit ideas or provide feedback about XClarity Administrator by clicking the user-actions menu () on the XClarity Administrator title bar, and then clicking **Submit ideas** or **Submit feedback**.

You can also submit ideas and feedback from the Internet using the following links:

- [Lenovo XClarity Ideation website](#)
- Ask questions and find answers on the [Lenovo XClarity Community forum website](#) by clicking the user-actions menu () on the XClarity Administrator title bar, and then clicking **Visit forum**.
- Check the [Lenovo Data Center Support website](#) for the latest tips and techniques that you can use to solve issues that you might have with XClarity Administrator. These *tech tips* provide procedures to work around issues that are related to the operation of XClarity Administrator.

To find tech tips that are available for your server:

1. Go to the [Lenovo Data Center Support website](#).
2. Enter “XClarity Administrator” in the **Search** field.
3. Either click **View All** in the **Top Articles** section to view all tips, or enter keywords in the **Search** field to find a specific tip.

Tip: You can sort the list by **Relevance**, **Popularity**, or **Newest** tips.

- Submitting a service request with Lenovo Support for XClarity Administrator issues requires Lenovo XClarity Pro. Lenovo XClarity Pro provides entitlement to service and support and the full-function-enablement license. For more information about purchasing Lenovo XClarity Pro, contact your Lenovo representative or authorized business partner.
- Ensure that the **Default Lenovo Call Home** forwarder is configured and enabled (see [Setting up automatic problem notification to Lenovo Support \(Call Home\)](#)).
- Ensure that all ports that XClarity Administrator requires (including ports that are required for Call Home) are available before you enable Call Home. For more information about ports, see [Port availability](#) in the XClarity Administrator online documentation.
- Ensure that a connection exists to the Internet addresses that are required by Call Home. For information about firewalls, see [Firewalls and proxy servers](#) in the XClarity Administrator online documentation.
- If XClarity Administrator accesses the Internet through an HTTP proxy, ensure that the proxy server is configured to use basic authentication and is set up as a non-terminating proxy. For more information about setting up the proxy, see [Configuring network access](#) in the XClarity Administrator online documentation.

About this task

If a Call Home is already in progress when another Call Home is initiated, data is collected and sent to Lenovo Support for the first Call Home before data is collected and sent for the second Call Home. Therefore, there might be a delay in sending data for the second Call Home.

Procedure

Complete the following steps to report a problem with XClarity Administrator.

- If Call Home is configured, perform the following steps to open a service ticket, collect and download the service data for the management server, and send the files to the Lenovo Support Center:
 1. From the XClarity Administrator title bar, click **Report Problem**. The management server tests the connection to Lenovo Support.

2. Click **Continue** to display the Software Problem Information dialog.
3. Provide your Lenovo customer number that you received when you purchased Lenovo XClarity Pro.
4. Provide information about the problem, including relevant event IDs and devices that are associated with the problem.

Notes:

- Service logs and data for the management server is collected and sent automatically.
 - If you selected devices that are associated with the problem, service data for the devices is also collected and sent automatically.
 - You can attach additional files to aid the Lenovo Support in troubleshooting the problem (including screen captures and video clips) by clicking **Upload File**.
5. Provide steps to reproduce the problem.
 6. Select the functional area where the problem occurred.
 7. Click **Next**.
 8. Specify information about the primary person to contact about the problem. To specify additional contacts, click **Add Another Contact**.
 9. Click **Submit to Lenovo** to create a service ticket with Lenovo Support.
- If Call Home is not configured or is configured but not enabled, you can submit a service request by calling the Lenovo Support Line. For more information, see [Getting help and technical assistance](#) .

After you finish

You can monitor open service tickets from the **Service Ticket Status** page (see [Viewing service tickets and status](#)).

You can attach additional files to the open service ticket after the problem is submitted.

1. From the XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.
2. Click **Service Ticket Status** in the left navigation to display the Service Ticket Status page.
3. Select the service ticket.
4. Click the **Attach Service File**, and then select the service-data archive or another file that you want to attach to the service ticket and send to Lenovo Support.

Attaching a service file to an open service ticket

You can attach service-data files for a specific device to an open service ticket in the Lenovo Support Center.

Before you begin

Attention: You must accept the [Lenovo Privacy Statement](#) before you can transfer data to Lenovo Support.

About this task

You can attach additional files to an open service ticket, such as current service-data archives, screen captures, and video clips.

Procedure

Complete the following steps to add a service file to an open service ticket.

- From the **Device Service Data** page:
 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.
 2. Click **Endpoint Service Data** in the left navigation to display the Endpoint Service Data page.
 3. Select a service file that you want to attach to a service ticket.
 4. Click the **Actions → Attach to Service Ticket**, and then select the service ticket to which you want to attach the service file.
 5. Click **Associate** to attach the file to the service ticket and send to Lenovo Support.
- From the **Service Ticket Status** tab:
 1. From the XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.
 2. Click **Service Ticket Status** in the left navigation to display the Service Ticket Status page.
 3. Select the service ticket.
 4. Click the **Attach Service File**, and then select the service file that you want to attach to the service ticket and send to Lenovo Support.

Viewing service tickets and status

You can view information about service tickets that were manually and automatically submitted to the Lenovo Support Center using Call Home, including the current status and associated service files that were transferred to the Lenovo Support Center, and service tickets that were generated by support services other than Call Home.

Procedure

To view service tickets in XClarity Administrator, click the **Administration → Service and Support**, and then click **Service Ticket Status** in the left navigation to display the Service Ticket Status page.

The **Service Ticket Number** column shows the ID of the service ticket that was opened for an event. If multiple service tickets were opened for the same event (for example, one in the Lenovo Support Center and another in a ServiceNow integrator), there are separate rows in the table for each service ticket. You can find the corresponding service ticket in the **Cross Reference ID** column. For example, if the **Service Ticket Number** shows the Lenovo Support service ticket ID, then the **Cross Reference ID** shows the ServiceNow service ticket ID, and vice versa.

The **Type** column identifies the type of service ticket that is listed in **Service Ticket Number** column. The service-ticket type can be one of the following values.

- **IBM Call Home**
- **IBM Call Home Test**
- **Lenovo Call Home**
- **Lenovo Call Home Test**
- **Lenovo Software Call Home**
- **Lenovo Software Call Home Test**
- **Cherwill**
- **ServiceNow**




A service ticket can be in one of the following states:

- **Active**
- **Canceled**
- **Resolved**

- **Unknown**

The **Cross Reference ID** column contains the ID of service tickets from external support services (such as ServiceNow) that are related to the Lenovo service ticket.




Service Ticket Status

Attach Service File Attach Note  |  |  | All Actions ▾ |

<input type="checkbox"/>	Service ticket number	State	Type	Event ID	Source	Component	Last Update	Creation Date
<input type="checkbox"/>	USE...	U...	IB...	00038	SN#Y03	DUMMY-C3A	Sep 27, 2021, 5:55:28 PM	Sep 27, 2021, 5:55:28 PM
<input type="checkbox"/>	USE...	CI...	IB...	00038	SN#Y03	DUMMY-C3A	Sep 27, 2021, 5:35:50 PM	Sep 27, 2021, 5:35:50 PM
<input type="checkbox"/>	USE...	CI...	IB...	00038	SN#Y03	DUMMY-C3A	Sep 27, 2021, 4:45:40 PM	Sep 27, 2021, 4:45:40 PM
<input type="checkbox"/>	USE...	U...	IB...	0EA1A	SN#Y03	IO Module 0	Sep 27, 2021, 9:15:46 AM	Sep 27, 2021, 9:15:46 AM
<input type="checkbox"/>	USE...	U...	IB...	00038	SN#Y03	DUMMY-C3A	Sep 27, 2021, 4:08:14 AM	Sep 27, 2021, 4:08:14 AM
<input type="checkbox"/>	USE...	U...	IB...	00038	SN#Y03	DUMMY-C3A	Sep 26, 2021, 11:30:09 PM	Sep 26, 2021, 11:30:09 PM
<input type="checkbox"/>	USE...	CI...	IB...	0EA1A	SN#Y03	IO Module 0	Sep 26, 2021, 3:59:09 PM	Sep 26, 2021, 3:59:09 PM
<input type="checkbox"/>	USE...	U...	IB...	00038	SN#Y03	DUMMY-C3A	Sep 26, 2021, 2:27:11 PM	Sep 26, 2021, 2:27:11 PM
<input type="checkbox"/>	USE...	U...	IB...	00038	SN#Y03	DUMMY-C3A	Sep 25, 2021, 7:20:02 PM	Sep 25, 2021, 7:20:02 PM
<input type="checkbox"/>	USE...	CI...	IB...	00038	SN#Y03	DUMMY-C3A	Sep 25, 2021, 6:59:05 AM	Sep 25, 2021, 6:59:05 AM

After you finish

From the Service Ticket Status page, you can perform the following steps on a selected service ticket.

- Attach a service file for a specific device to an open service ticket in the Lenovo Support Center by clicking **Attach Service File** (see [Attaching a service file to an open service ticket](#))
- Attach a note to an open service ticket in the Lenovo Support Center by clicking **Attach Note**.
- Delete a service ticket by clicking the **Delete Service Tickets** icon (). You can delete only service tickets that *are not* in the Active state.
- Retrieve the latest information about all open service tickets from the Lenovo Support Center by clicking the **Refresh Service Ticket Status State** icon ().
- Export the status of all service ticket to a CSV file by clicking the **Export all as CSV** icon ().

Transferring service files to Lenovo Support

If you are working with Lenovo Support to resolve an issue, you can manually transfer service files directly to your Lenovo Support representative using the Lenovo Upload Facility.

Before you begin

Attention: You must accept the [Lenovo Privacy Statement](#) before you can transfer data to Lenovo Support.


Procedure

Complete the following steps to transfer service files directly to Lenovo Support.

Step 1. Configure the Lenovo Upload Facility.

- a. From the Lenovo XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.
- b. Click **Lenovo Upload Facility** in the left navigation.
- c. Enter an email address.
- d. Click **Apply**.

Step 2. Click **Management Server Files** or **Endpoint Service Data** in the left navigation, depending on the logs that you need to send.

Step 3. Select one or more service files that you want to send to Lenovo Support, and click the **Lenovo Upload Selected** icon (). The Lenovo Upload Information dialog is displayed.

Step 4. Optionally enter a case number.

Step 5. Click **OK** to transfer the service files.

Configuring management-server log settings

The log settings are used by Lenovo Support to adjust logging granularity only when needed.

About this task

Attention: Do not modify the settings on this page unless directed to do so by Lenovo Support.

Procedure

Complete the following steps to configure log settings.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.

Step 2. Click **Server Logging Settings** in the left navigation to display the Server Logging Settings page.

Step 3. Adjust each setting as directed by Lenovo Support, and click **Apply**.

After you finish

From the Server Logging Settings page, you can also perform the following steps.

- Download management-server log-configuration settings to the local system by clicking **Download LogBack**. The settings are downloaded to the default download directory as a file named logback.xml.
- Restore the default settings by clicking **Restore Defaults**.
- Import a configuration file by clicking **Upload Configuration File** and selecting the file that you want to import in XClarity Administrator. The file must be named logback.xml.

Important: Only configuration files that were given to you by your Lenovo service technician should be imported and only by direction of the service technician.

Re-enabling Call Home on all managed devices

When you enable a Call Home service forwarder in Lenovo XClarity Administrator, Call Home is disabled on each managed device to avoid duplicate problem records from being created. If you intend to discontinue using XClarity Administrator to manage your devices or if you intend to disable Call Home in XClarity Administrator, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time.

About this task

Attention: Re-enabling Call Home on all devices might not cause Call Home to become operational for those devices. Configuration might be required on each individual device if it had not been configured on those devices previously.

Although XClarity Administrator supports Call Home for ThinkAgile and ThinkSystem devices, the baseboard management controller for some ThinkAgile and ThinkSystem devices does not include Call Home support. Therefore, you cannot enable or disable Call Home on those devices themselves. Call Home can be enabled only for those devices at the XClarity Administrator level.

Procedure

Complete the following steps to re-enable Call Home on all managed devices.

- Step 1. From the XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.
- Step 2. Click **Service Forwarders** in the left navigation to display the Service Forwarders page.
- Step 3. Change the status for all Call Home service forwarders, including “Default Call Home,” to **Disabled**.
- Step 4. Click **Endpoint Actions** in the left navigation to display the Endpoint Actions page.
- Step 5. Click **All Actions → Enable Call Home on all devices** to enable Call Home on each managed device.

Sending periodic data to Lenovo

You can optionally allow XClarity Administrator to collect information about how you use the product and changes in your environment and to send that data to Lenovo on periodic basis. Lenovo uses this data to improve your experience with the Lenovo products and with Lenovo support.

Before you begin

Attention: You must accept the [Lenovo Privacy Statement](#) before you can transfer data to Lenovo Support.

About this task

You can collect and send the following types of data to Lenovo.

- **Usage data**

By analyzing usage data from multiple users, Lenovo can learn more about how XClarity Administrator is being used. This allows Lenovo to know the functions that are used the most and to identify problems that are occurring on the XClarity Administrator instances. This data can be then used to make future investment decisions on product enhancements that better meet your needs, to fix problems in future releases, and to improve product quality.

When you agree to send usage data to Lenovo, the following data is collected and sent on a weekly basis. This data *is anonymous*. No private data (including serial numbers, UUIDs, host names, IP addresses, and user names) is collected or sent to Lenovo.

- Log of actions that were performed
- List of events that were raised, and the timestamp when they were raised
- List of audit events that raised, and the timestamp when they were raised
- List of jobs that were run, and success or failure information for each job
- XClarity Administrator metrics, including memory usage, processor usage, and disk space
- Limited inventory data about all managed devices

- **Hardware data**

By analyzing hardware data from multiple users, Lenovo can learn about hardware changes that regularly occur. This data can then be used to improve predictive analytics and to enhance your service and support experience by stocking parts in the right geographies.

When you agree to send hardware data to Lenovo, the following data is collected and sent on a periodic basis. This data *is not anonymous*. Hardware data includes attributes, such as UUIDs and serial numbers. It does not include IP addresses or hostnames.

- **Daily hardware data.** The following data is included for each inventory change.
 - Inventory-change event (FQXHMDM0001)
 - Changes to inventory data for the device that is associated with that event
- **Weekly hardware data.** Inventory data is included for all managed devices.

When data is sent to Lenovo, it is transmitted from the XClarity Administrator instance to the Lenovo Upload Facility using HTTPS. REST APIs are called over this HTTPS connection to send the data. A certificate that is pre-loaded on XClarity Administrator is used for authentication. If an XClarity Administrator instance does not have direct access to the Internet, and there is a proxy configured in XClarity Administrator, the data is transmitted through that proxy.

The data is then moved to the Lenovo Customer Care repository, where it is stored for up to 5 years. This repository is a secure location that is also used when debug data is sent to Lenovo to troubleshoot problems. It is used by most Lenovo server, storage, and switch products.

From the Lenovo Customer Care repository, queries are run on all hardware and usage data, and graphs are made available to the Lenovo product team for analysis.

Procedure

Complete the following steps to allow XClarity Administrator to collect and send customer data to Lenovo.

Step 1. From the XClarity Administrator menu bar, click **Administration** → **Service and Support**. The Service and Support page is displayed.

Periodic Data Upload

We'd like to ask a favor. In order to improve the product, and make your experience better, would you allow us to collect information on how you use this product?

[Lenovo Privacy Statement](#)

No Thanks

Hardware [?](#)

I agree to send hardware inventory and system event data to Lenovo on a periodic basis. Lenovo can use the data to enhance future support experience (for example, to stock and move the right parts closer to you).

To download an example of data, click [here](#).

Usage [?](#)

I agree to send usage data to Lenovo on a periodic basis to help Lenovo understand how the product is being used. All data is anonymous.

To download an example of data, click [here](#).

The data was last changed at Oct 9, 2020, 4:28:57 PM

Apply

Step 2. Click **Periodic Data Upload** in the left navigation to display the Periodic Data Upload page

Step 3. Optionally agree to send hardware and usage data to Lenovo

Step 4. Click **Apply**.

After you finish

You can perform the following actions from this page if you agreed to send data.

- Determine the last time data was sent by looking at the date under the appropriate check box.
- Download the data archive that was last sent by clicking the link under the appropriate check box.

Sample usage data

The following examples are collected and sent to Lenovo on a periodic basis when you agree to send usage data to Lenovo.

XClarity Administrator metrics data

Timestamp	cpuLoad	usedSpace	usedRam	usedJavaCpu	usedJavaRam
1497861662	0.99	12.6225	13.3644	71.9	9.4
1497861668	1.23	12.6343	18.5676	0	14.4
1497861674	1.89	12.6371	19.6182	77.9	15.3
1497861679	1.98	12.6442	23.0782	37.9	18.6
1497861685	2.06	12.647	23.2412	77.9	18.6
1497861690	2.14	12.6654	25.3697	10	19
1497861696	2.37	7.75276	25.8952	2	19.4
1497861701	2.34	7.76077	26.0184	24	19.5
1497861056	2.55	7.77003	26.4222	85.9	19.7
1497861061	2.82	7.77877	26.5485	159.9	19.7
1497861067	3	7.7954	27.0066	131.9	20

Actions data

```
/updates/images/userdefined.png={"GET"\:1}
/config/profile={"GET"\:865}
/node/AD9547AB3C8011E79DCC000E1E7D4EE0={"GET"\:1}
/usage/data={"GET"\:12}
/compliancePolicies/persistedResult={"GET"\:3}
/jobs/88={"PUT"\:31}
/osdeployment/rest/internal/event/aicc={"POST"\:186}
/aicc={"GET"\:56}
/updates/images/powerStates.png={"GET"\:2}
/jobs/84={"PUT"\:3}
/updates/images/ActionSprite.png={"GET"\:1}
/nodes/AD9547AB3C8011E79DCC000E1E7D4EE0/lock={"GET"\:1,"PUT"\:2}
/updates/customUI/gridxExtensions/Mark.js={"GET"\:2}
/updates/images/ac22_deleteall_inactive_24.png={"GET"\:1}
/service/forwarders={"GET"\:12}
/nodes/7C64A0A8413811E7A6C6000E1EB35A90/lock={"GET"\:1,"PUT"\:2}
/config/deploy/status={"GET"\:865}
/node/235435543C7D11E7AA13000E1E7D54A0={"GET"\:1}
/updates/ApplyActivateUpdates.js={"GET"\:2}
/discovery={"GET"\:3}
/userAccountSettings={"GET"\:1}
/discoverRequest/jobs/610={"GET"\:9}
/compliancePolicies/events={"POST"\:25}
/events/audit={"GET"\:5}
/updates/images/st22_filterRunning_24.png={"GET"\:2}
/updates/images/st16_running_24.gif={"GET"\:1}
/updates/images/complianceStatus.png={"GET"\:2}
/usage={"GET"\:4}
/updates/json/firmwareRepository/exportPayloads.json={"GET"\:1}
/updates/images/ac22_collapseall_OneUI_24.png={"GET"\:3}
/chassis/0AC502DEFCD6419FB20FB5A9A49D0293={"GET"\:17}
/updates/images/ac22_copy_inactive_24.png={"GET"\:1}
/service/endpoint/collectedArchives={"GET"\:4}
/jobs/lock/88={"DELETE"\:1}
/updates/customUI/gridxModules/IndirectSelect.js={"GET"\:2}
/stgupdates/inventory/events={"POST"\:70}
/electronicDownload={"GET"\:1}
/updates/images/st16_firm_normal_24.png={"GET"\:3}
/updates/images/st16_Empty_24.png={"GET"\:1}
/updates/json/compliancePolicy/getCompByUxsp.json={"GET"\:1}
```

Event data

```
{
  "action":100,
  "commonEventID":"FQXHMSE0203I",
  "cn":"1",
  "eventClass":200,
  "eventID":"FQXHMSE0203I",
  "flags":"","
  "mtm":"","
  "msgID":"","
  "service":100,
  "severity":200},
  "timeStamp":"2017-06-16T15:56:06Z"
}
```

Audit data

```
{
```

```

"action":100,
"commonEventID":"FXMHMSE0200I",
"cn":"1",
"eventClass":200,
"eventID":"FXMHMSE0200I",
"flags":"","
"msgID":"","
"mtm":"","
"service":100,
"severity":200,
"timeStamp":"2017-06-16T15:56:06Z"
}

```

Inventory data

```

-377665639={
  "firmwareList"\: [{
    "build"\:"2PET41C",
    "date"\:"2017-12-19T05\:00\:00Z",
    "name"\:"CMM firmware",
    "type"\:"CMM firmware",
    "version"\:""
  }],
  "mtm"\:"/",
  "productName"\:" ",
  "stillManaged"\:"true",
  "uuid"\:"-377665639"
}
-177044123={
  "firmwareList"\: [{
    "build"\:"A3E117D",
    "date"\:"2018-01-26T00\:00\:00Z",
    "name"\:"UEFI Firmware/BIOS",
    "type"\:"UEFI",
    "version"\:"A3E117D-1.80"
  }], {
    "build"\:"A3E113C",
    "date"\:"2016-12-16T00\:00\:00Z",
    "name"\:"UEFI Backup Firmware/BIOS",
    "type"\:"UEFI-Backup",
    "version"\:"A3E113C-1.60"
  }, {
    "build"\:"DSALB1Q",
    "date"\:"2018-05-15T00\:00\:00Z",
    "name"\:"DSA Diagnostic Software",
    "type"\:"DSA",
    "version"\:"DSALB1Q-10.3"
  }, {
    "build"\:"TC0039A",
    "date"\:"2018-01-19T00\:00\:00Z",
    "name"\:"IMM2 Firmware",
    "type"\:"IMM2",
    "version"\:"TC0039A-4.70"
  }, {
    "build"\:"TC0039A",
    "date"\:"2018-01-19T00\:00\:00Z",
    "name"\:"IMM2 Backup Firmware",
    "type"\:"IMM2-Backup",
    "version"\:"TC0039A-4.70"
  }],
  "mtm"\:"7162/CC1",

```

```

    "productName":"Lenovo Flex System x240 Compute Node",
    "stillManaged":"true",
    "uuid":"-177044123"
  }
-734000615={
  "firmwareList":[],
  "mtm":"8721/HC1",
  "productName":"IBM Flex System Enterprise Chassis Midplane Card",
  "stillManaged":"true",
  "uuid":"-734000615"
1150304995={
  "firmwareList":[{
    "date":"06/12/2014",
    "build":"",
    "name":"Boot ROM",
    "type":"Boot ROM",
    "version":"7.8.5.0"
  }],{
    "date":"06/12/2014",
    "build":"",
    "name":"Main Application 1",
    "type":"Main Application 1",
    "version":"7.8.5.0"
  },{
    "date":"03/29/2013",
    "build":"",
    "name":"Main Application 2",
    "type":"Main Application 2",
    "version":"7.5.3.0"
  }],
  "mtm":"/",
  "productName":"IBM Flex System Fabric EN4093 10Gb Scalable Switch",
  "stillManaged":"true",
  "uuid":"1150304995"
}
-1050714125={
  "firmwareList":[{
    "date":"04/19/2016",
    "build":"",
    "name":"Main Application",
    "type":"Main Application",
    "version":"7.4.1c"
  }],
  "mtm":"/",
  "productName":"IBM Flex System FC5022 12-port 16Gb ESB SAN Scalable Switch",
  "stillManaged":"true",
  "uuid":"-1050714125"
}
}

```

Sample hardware data

The following example is collected and sent to Lenovo on a periodic basis when you agree to send hardware data to Lenovo.

Data is collected daily and weekly.

- [“Daily hardware data” on page 88](#). Includes inventory-change event (FQXHMDM00011) and changes to hardware inventory for each inventory change.
- [“Weekly hardware data” on page 92](#). Includes inventory for all devices.

Daily hardware data

```
[{
  "2020-03-23T12:32:24.765": {
    "event": {
      "severity": 200,
      "timeStamp": "2020-03-23T16:32:21Z",
      "eventID": "FQXHMDM0001I",
      "eventClass": 800,
      "service": 100,
      "mtm": "",
      "flags": ["Hidden"],
      "action": 100,
      "msgID": "",
      "commonEventID": "FQXHMDM0001I",
      "cn": ""
    },
    "deviceInventoryChanges": [{
      "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36": [{
        "MODIFIED": [
          { "nodes": [] },
          { "accessState": "Pending" },
          { "powerSupplies": [{
            "cmmDisplayName": "Power Supply 06",
            "cmmHealthState": "Non-Critical",
            "dataHandle": 0,
            "description": "Power Supply",
            "excludedHealthState": "Normal",
            "firmware": [{
              "build": "",
              "classifications": [],
              "date": "",
              "name": "Power Supply Firmware",
              "revision": "0",
              "role": "",
              "softwareID": "",
              "status": "",
              "type": "Power Supply Firmware",
              "version": ""
            }
          ]},
          { "FRU": "69Y5817",
            "fruSerialNumber": "ZK125115V0VS",
            "hardwareRevision": "5.0",
            "healthState": "NA",
            "inputVoltageMax": -1,
            "inputVoltageIsAC": true,
            "inputVoltageMin": -1,
            "leds": [{
              "color": "Green",
              "location": "Planar",
              "name": "OUT",
              "state": "Off"
            }
          ],
          {
            "color": "Amber",
            "location": "Planar",
            "name": "FAULT",
            "state": "Off"
          },
          {
            "color": "Green",
```



```

        "location": "Planar",
        "name": "IN",
        "state": "Off"
    }],
    "machineType": "",
    "manufactureDate": "2211",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Power Supply 06",
    "overallHealthState": "Normal",
    "parent": {
        "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
        "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
    },
    "partNumber": "69Y5801",
    "productName": "IBM 2500 W Power Supply",
    "posID": "60",
    "powerAllocation": {
        "totalInputPower": 0,
        "totalOutputPower": 343
    },
    "powerState": "Unknown",
    "productId": "303",
    "serialNumber": "",
    "slots": [6],
    "type": "PowerSupply",
    "userDescription": "",
    "uri": "powerSupply/04382F96885411E00095009500950095",
    "uuid": "04382F96885411E00095009500950095",
    "vpdID": "128"
},
{
    "cmmDisplayName": "Power Supply 04",
    "cmmHealthState": "Normal",
    "dataHandle": 0,
    "description": "Power Supply",
    "excludedHealthState": "Normal",
    "firmware": [{
        "build": "",
        "classifications": [],
        "date": "",
        "name": "Power Supply Firmware",
        "revision": "5",
        "role": "",
        "softwareID": "",
        "status": "",
        "type": "Power Supply Firmware",
        "version": ""
    }],
    "FRU": "69Y5806",
    "fruSerialNumber": "ZK128116T03B",
    "hardwareRevision": "75.54",
    "healthState": "NA",
    "inputVoltageIsAC": true,
    "inputVoltageMax": 240,
    "inputVoltageMin": 220,
    "leds": [{
        "color": "Green",
        "location": "Planar",
        "name": "OUT",

```

```

    "state": "On"
  },
  {
    "color": "Amber",
    "location": "Planar",
    "name": "FAULT",
    "state": "Off"
  },
  {
    "color": "Green",
    "location": "Planar",
    "name": "IN",
    "state": "On"
  }
}],
"machineType": "",
"manufactureDate": "2511",
"manufacturer": "IBM",
"manufacturerId": "20301",
"model": "",
"name": "Power Supply 04",
"overallHealthState": "Normal",
"parent": {
  "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
  "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partNumber": "69Y5802",
"productId": "304",
"productName": "IBM 2500 W Power Supply",
"powerAllocation": {
  "totalInputPower": 2505,
  "totalOutputPower": 343
},
"powerState": "Unknown",
"posID": "61",
"serialNumber": "",
"slots": [4],
"type": "PowerSupply",
"userDescription": "",
"uri": "powerSupply/FF2D840D7A644BCE91ADC16C78978A03",
"uuid": "FF2D840D7A644BCE91ADC16C78978A03",
"vpdID": "128"
}]],
{ "fanMuxes": [{
  "cmmDisplayName": "Fan Logic 01",
  "cmmHealthState": "Non-Critical",
  "dataHandle": 0,
  "description": "Fan Logic Module",
  "excludedHealthState": "Normal",
  "FRU": "81Y2912",
  "fruSerialNumber": "Y031BG16D00S",
  "hardwareRevision": "4.0",
  "leds": [{
    "color": "Amber",
    "location": "FrontPanel",
    "name": "FAULT",
    "state": "On"
  }
}],
"machineType": "",
"manufacturer": "IBM",
"manufactureDate": "2511",
"manufacturerId": "20301",

```



```
}}
```

Weekly hardware data

```
{
  "2020-03-23T12:41:28.045": {
    "cabinetList": [{
      "cabinetName": "STANDALONE_OBJECT_NAME",
      "chassisList": [{
        "itemName": "SN#Y010BG57Y01G",
        "itemUUID": "671D5D9EBB4440A49D9DAF08A9EDFB36",
        "itemParentUUID": "",
        "itemLocationRoom": "",
        "itemLocationRack": "",
        "itemLocation": "No Location ConfiguredL",
        "itemLowerUnit": 0,
        "itemType": "CHASSIS",
        "itemHeight": 10,
        "itemSubType": "unknown_type",
        "itemInventory": {
          "accessState": "Online",
          "activationKeys": [],
          "backedBy": "real",
          "bladeSlots": 14,
          "cmmDisplayName": "SN#Y010BG57Y01G",
          "cmmHealthState": "Non-Critical",
          "cmms": [{
            "accessState": "Online",
            "backedBy": "real",
            "cmmDisplayName": "Standby CMM",
            "dataHandle": 1584981183026,
            "cmmHealthState": "Normal",
            "description": "CMM",
            "firmware": [{
              "build": "1A0N580",
              "classifications": [],
              "date": "2020-03-20T04:00:00Z",
              "name": "CMM firmware",
              "revision": "58",
              "role": "",
              "status": "",
              "type": "CMM firmware",
              "version": "2.5.0"
            }],
          },
          "FRU": "68Y7032",
          "fruSerialNumber": "Y030BG168020",
          "hostConfig": [],
          "ipInterfaces": [{
            "IPv4DHCPmode": "UNKNOWN",
            "IPv4enabled": false,
            "IPv6DHCPenabled": false,
            "IPv6enabled": false,
            "IPv6statelessEnabled": false,
            "IPv6staticEnabled": false,
            "label": "External",
            "name": "eth0"
          }],
          "errorFields": [],
          "excludedHealthState": "Normal",
          "leds": [{
            "color": "Amber",
```

```

        "location": "FrontPanel",
        "name": "FAULT",
        "state": "Off"
    }],
    "machineType": "",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Standby CMM",
    "overallHealthState": "Normal",
    "partNumber": "68Y7054",
    "parent": {
        "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
        "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
    },
    "powerAllocation": {
        "maximumAllocatedPower": 20,
        "minimumAllocatedPower": 20
    },
    "productId": "65",
    "role": "backup",
    "serialNumber": "",
    "slots": [2],
    "type": "CMM",
    "uri": "cmm/F1F06BE6946511E089AEB9871E6892B2",
    "userDefinedName": "",
    "userDescription": "",
    "uuid": "F1F06BE6946511E089AEB9871E6892B2"
}],
"complex": [],
"contact": "No Contact Configured",
"dataHandle": 1584981227532,
"description": "Lenovo Flex System Chassis",
"displayName": "SN#Y010BG57Y01G",
"encapsulation": {
    "encapsulationMode": "normal"
},
"energyPolicies": {
    "acousticAttenuationMode": "Off",
    "hotAirRecirculation": {
        "chassisBay": [],
        "isEnabled": false,
        "maxVariation": 9.0
    },
    "powerCappingPolicy": {
        "cappingPolicy": "OFF",
        "currentPowerCap": 0,
        "maxPowerCap": 5010,
        "minPowerCap": 1504,
        "powerCappingAllocUnit": "watts"
    },
    "powerRedundancyMode": 4
},
"errorFields": [],
"excludedHealthState": "Warning",
"fanSlots": 10,
"fanMuxes": [{
    "cmmDisplayName": "Fan Logic 02",
    "cmmHealthState": "Non-Critical",
    "dataHandle": 0,
    "description": "Fan Logic Module",

```

```

"excludedHealthState": "Warning",
"FRU": "81Y2912",
"fruSerialNumber": "Y031BG16DOCE",
"hardwareRevision": "4.0",
"leds": [{
  "color": "Amber",
  "location": "FrontPanel",
  "name": "FAULT",
  "state": "On"
}],
"machineType": "",
"manufactureDate": "2511",
"manufacturer": "IBM",
"manufacturerId": "20301",
"model": "",
"name": "Fan Logic 02",
"overallHealthState": "Warning",
"parent": {
  "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
  "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partNumber": "81Y2990",
"productId": "338",
"productName": "IBM Fan Pack Multiplexor Card",
"serialNumber": "",
"slots": [2],
"status": "Non-Critical",
"type": "FanMux",
"uri": "fanMux/71F72BE3985011E0B5A8E216694D6175",
"uuid": "71F72BE3985011E0B5A8E216694D6175"
}],
"fanMuxSlots": 2,
"fans": [{
  "cmmDisplayName": "Fan 06",
  "cmmHealthState": "Normal",
  "dataHandle": 0,
  "description": "IBM Fan Pack",
  "errorFields": [],
  "excludedHealthState": "Normal",
  "firmware": [{
    "build": "",
    "classifications": [],
    "date": "",
    "name": "Fan Controller",
    "revision": "226",
    "role": "",
    "status": "",
    "type": "Fan Controller",
    "version": "226"
  ]
},
"FRU": "88Y6685",
"fruSerialNumber": "YK10JPB69582",
"hardwareRevision": "4.0",
"leds": [{
  "color": "Amber",
  "location": "FrontPanel",
  "name": "FAULT",
  "state": "Off"
}],
"machineType": "",
"manufactureDate": "2411",

```

```

"manufacturer": "IBM",
"manufacturerId": "20301",
"model": "",
"name": "Fan 06",
"overallHealthState": "Normal",
"parent": {
  "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
  "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partNumber": "88Y6691",
"posID": "11",
"powerAllocation": {
  "maximumAllocatedPower": 75,
  "minimumAllocatedPower": 75
},
"powerState": "Unknown",
"productId": "342",
"productName": "80mm Fan Pack for ITE Cooling",
"serialNumber": "",
"slots": [6],
"type": "Fan",
"userDescription": "",
"uri": "fan/7293CA21938011E0BC13CB5D330B7C19",
"uuid": "7293CA21938011E0BC13CB5D330B7C19",
"vpdID": "373"
}],
"height": 10,
"isConnectionTrusted": "true",
"lastOfflineTimestamp": -1,
"ledCardSlots": 1,
"leds": [{
  "color": "Blue",
  "location": "FrontPanel",
  "name": "Location",
"state": "Off"
}],
"location": {
  "location": "No Location ConfiguredL",
  "lowestRackUnit": 0,
  "rack": "",
  "room": ""
},
"machineType": "8721",
"managerName": "UNKNOWN",
"managerUuid": "UNKNOWN",
"manufacturer": "IBM",
"manufacturerId": "20301",
"mmSlots": 2,
"model": "HC1",
"name": "SN#Y010BG57Y01G",
"nist": {
  "currentValue": "Compatibility",
  "possibleValues": ["Nist_800_131A_Strict","unsupported","Nist_800_131A_Custom","Compatibility"]
},
"nodes": [{
  "accessState": "Online",
  "activationKeys": [],
  "addinCards": [],
  "addinCardSlots": 0,
  "arch": "Unknown",
  "backedBy": "real",

```

```

"bladeState": 0,
"bladeState_health": "CRITICAL",
"bladeState_string": "Init failed",
"bootMode": {
  "currentValue": "",
  "possibleValues": []
},
"bootOrder": {
  "bootOrderList": [],
  "uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)/bootOrder"
},
"cmmDisplayName": "Node 07",
"cmmHealthState": "Critical",
"complexID": -1,
"contact": "",
"dataHandle": 1584981175839,
"description": "",
"driveBays": 0,
"drives": [],
"embeddedHypervisorPresence": false,
"encapsulation": {
  "encapsulationMode": "notSupported"
},
"errorFields": [
  { "HostAndDomain": "NO_CONNECTOR" },
  { "PhysicalAndLocation": "NO_CONNECTOR" },
  { "Encapsulation": "NO_CONNECTOR" },
  { "Memory": "NO_CONNECTOR" },
  { "ServerFirmwareData": "NO_CONNECTOR" },
  { "RackCPU": "NO_CONNECTOR" },
  { "ServerOnboardPciDevices": "NO_CONNECTOR" },
  { "BootMode": "NO_CONNECTOR" },
  { "SecureBootMode": "NO_CONNECTOR" },
  { "BootOrder": "NO_CONNECTOR" },
  { "FlashDimm": "NO_CONNECTOR" },
  { "HostMacAddress": "NO_CONNECTOR" },
  { "VnicMode": "NO_CONNECTOR" },
  { "RemotePresenceEnabled": "NO_CONNECTOR" },
  { "ActivationKey": "NO_CONNECTOR" },
  { "LanOverUsbMode": "NO_CONNECTOR" },
  { "ServerStaticMetrics": "NO_CONNECTOR" },
  { "ScalableComplexPartitionUUIDData": "NO_CONNECTOR" },
  { "ActiveAlerts": "NO_CONNECTOR" },
  { "PFAConfiguration": "NO_CONNECTOR" },
  { "ServerIPAddresses": "NO_CONNECTOR" },
  { "FaceplateInfo": "NO_CONNECTOR" },
  { "IOCompatibilityData": "NO_CONNECTOR" },
  { "LanOverUsbPortForwardingModes": "NO_CONNECTOR" },
  { "ServerConfigFiles": "NO_CONNECTOR" }
],
"excludedHealthState": "Normal",
"expansionCards": [],
"expansionCardSlots": 0,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [],
"firmware": [],
"flashStorage": [],
"FRU": "",
"fruSerialNumber": "",
"hasOS": false,

```



```

"hostMacAddresses": "",
"ipInterfaces": [],
"isConnectionTrusted": "true",
"isITME": false
"isRemotePresenceEnabled": false,
"isScalable": false,
"lanOverUsb": "disabled",
"lanOverUsbPortForwardingModes": [],
"leds": [],
"location": {
  "location": "",
  "lowestRackUnit": 0,
  "rack": "",
  "room": ""
},
"logicalID": -1,
"m2Presence": false,
"machineType": "",
"manufacturer": "",
"manufacturerId": "",
"memoryModules": [],
"memorySlots": 0,
"mgmtProcType": "UNKNOWN",
"model": "",
"name": "Node 07",
"nist": {
  "currentValue": "Unknown",
  "possibleValues": ["Nist_800_131A_Strict","unsupported","Compatibility"]
},
"onboardPciDevices": [],
"osInfo": {
  "description": "",
  "storedCredential": ""
},
"overallHealthState": "Normal",
"parent": {
  "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
  "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partitionID": -1,
"partNumber": "",
"pciCapabilities": [],
"pciDevices": [],
"ports": [],
"posID": "",
"powerAllocation": {
  "maximumAllocatedPower": 0,
  "minimumAllocatedPower": 0
},
"powerStatus": 0,
"powerSupplies": [],
"primary": false,
"processors": [],
"processorSlots": 0,
"productId": "",
"productName": "",
"raidSettings": [],
"secureBootMode": {
  "currentValue": "",
  "possibleValues": []
},

```

```

"securityDescriptor": {
  "managedAuthEnabled": false,
  "managedAuthSupported": true,
  "publicAccess": false,
  "roleGroups": ["lxc-supervisor"],
  "storedCredentials": {
    "description": "Credentials for null",
    "id": "1703",
    "userName": "USERID"
  },
  "uri": "nodes/dummy-671d5d9ebb4440a4-chassis(1)-blade(7)"
},
"serialNumber": "",
"slots": [7],
"status": {
  "message": "managed",
  "name": "MANAGED"
},
"subSlots": [],
"subType": "",
"tlsVersion": {
  "currentValue": "Unknown",
  "possibleValues": ["unsupported","TLS_12","TLS_11","TLS_10"]
},
"type": "ITE",
"uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
"userDefinedName": "",
"userDescription": "",
"uuid": "DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
"vnicMode": "disabled",
"vpdID": ""
}],
"overallHealthState": "Warning",
"parent": {
  "uri": "cabinet/",
  "uuid": ""
},
"partNumber": "88Y6660",
"passThroughModules": [],
"posID": "14",
"powerAllocation": {
  "allocatedOutputPower": 1504,
  "midPlaneCardMaximumAllocatedPower": 38,
  "midPlaneCardMinimumAllocatedPower": 38,
  "remainingOutputPower": 3506,
  "totalInputPower": 5445,
  "totalOutputPower": 5010
},
"powerSupplies": [{
  "dataHandle": 0,
  "cmmDisplayName": "Power Supply 06",
  "cmmHealthState": "Non-Critical",
  "description": "Power Supply",
  "excludedHealthState": "Warning",
  "firmware": [{
    "build": "",
    "classifications": [],
    "date": "",
    "name": "Power Supply Firmware",
    "revision": "0",
    "role": ""
  }
}

```

```

        "softwareID": "",
        "status": "",
        "type": "Power Supply Firmware",
        "version": ""
    }
},
"FRU": "69Y5817",
"fruSerialNumber": "ZK125115V0VS",
"hardwareRevision": "5.0",
"healthState": "NA",
"inputVoltageIsAC": true,
"inputVoltageMax": -1,
"inputVoltageMin": -1,
"leds": [{
    "color": "Green",
    "location": "Planar",
    "name": "OUT",
    "state": "Off"
}],
"machineType": "",
"manufactureDate": "2211",
"manufacturer": "IBM",
"manufacturerId": "20301",
"model": "",
"name": "Power Supply 06",
"overallHealthState": "Warning",
"parent": {
    "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
    "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partNumber": "69Y5801",
"posID": "60",
"powerAllocation": {
    "totalInputPower": 0,
    "totalOutputPower": 343
},
"powerState": "Unknown",
"productId": "303",
"productName": "IBM 2500 W Power Supply",
"serialNumber": "",
"slots": [6],
"type": "PowerSupply",
"uri": "powerSupply/04382F96885411E00095009500950095",
"userDescription": "",
"uuid": "04382F96885411E00095009500950095",
"vpdID": "128"
}],
"powerSupplySlots": 6,
"productId": "336",
"productName": "IBM Chassis Midplane",
"securityDescriptor": {
    "managedAuthEnabled": false,
    "managedAuthSupported": true,
    "publicAccess": false,
    "roleGroups": ["lxc-supervisor"],
    "storedCredentials": {
        "description": "Credentials for null",
        "id": "1703",
        "userName": "USERID"
    },
},
"uri": "chassis/671d5d9ebb4440a49d9daf08a9edfb36"
},

```

```

"SecurityPolicy": {
  "cmmPolicyState": "ACTIVE",
  "cmmPolicyLevel": "SECURE"
},
"serialNumber": "23DVG73",
"status": {
  "message": "MANAGED",
  "name": "MANAGED"
},
"switches": [{
  "accessState": "Online",
  "accessStateRecords": [{
    "health": "OFFLINE",
    "ipAddress": "10.241.53.20",
    "messageBundle": "com.lenovo.lxca.inventory.base.bundle.connections.messages",
    "messageDisplay": "Authentication failed occurred due to HTTP 401 - Unauthorized (OpenPegasus Error: \"User Unauthorized\")",
    "messageID": "0510",
    "messageParameter": "HTTP 401 - Unauthorized (OpenPegasus Error: \"User Unauthorized\")",
    "protocol": "CIM",
    "username": "USERID",
    "timestamp": 1584709239559,
    "trusted": true
  }],
  "attachedNodes": [],
  "backedBy": "real",
  "cmmDisplayName": "IO Module 04",
  "cmmHealthState": "Normal",
  "dataHandle": 1584981209777,
  "description": "FC5022 16Gb SAN Scalable Switch",
  "deviceName": "FC5022",
  "errorFields": [{
    "IOCompatibilityData": "FETCH_FAILED"
  }],
  "excludedHealthState": "Normal",
  "firmware": [{
    "classifications": [],
    "build": "",
    "date": "2016-04-19T04:00:00Z",
    "name": "Main Application",
    "status": "Active",
    "type": "Main Application",
    "version": "7.4.1c"
  }],
  "FRU": "00Y3329",
  "fruSerialNumber": "Y050UZ67D009",
  "ipInterfaces": [{
    "IPv4DHCPmode": "DHCP_THEN_STATIC",
    "IPv4enabled": true,
    "IPv6enabled": true,
    "IPv6DHCPenabled": true,
    "IPv6statelessEnabled": true,
    "IPv6staticEnabled": false,
    "label": "",
    "name": "ioe0"
  }],
  "leds": [{
    "color": "Amber",
    "location": "FrontPanel",
    "name": "FRU Fault",
    "state": "Off"
  }],
}],

```

```

"machineType": "",
"manufacturer": "LNV",
"manufacturerId": "20301",
"model": "",
"name": "IO Module 04",
"ntpPushEnabled": false,
"ntpPushFrequency": 17,
"overallHealthState": "Normal",
"parent": {
  "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
  "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partNumber": "00MM452",
"ports": [],
"posID": "17",
"powerAllocation": {
  "maximumAllocatedPower": -1,
  "minimumAllocatedPower": -1
},
"powerState": "On",
"productId": "329",
"productName": "Flex System FC5022 24-port 16Gb SAN Scalable Switch",
"protectedMode": "Not supported",
"securityDescriptor": {
  "managedAuthEnabled": false,
  "managedAuthSupported": true,
  "publicAccess": false,
  "roleGroups": [],
  "storedCredentials": {
    "description": "Credentials for null",
    "id": "1702",
    "userName": "USERID"
  },
  "uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6"
},
"serialNumber": "",
"slots": [4],
"stackMode": "N/A",
"type": "Switch",
"uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6",
"userDefinedName": "",
"userDescription": "",
"uuid": "AE986BEC1DD1B201684FC4F57C3B16B6",
"vpdID": "309"
}],
"switchSlots": 4,
"tlsVersion": {
  "currentValue": "TLS_12_Server",
  "possibleValues": ["TLS_12_Server", "unsupported", "TLS_12_Server_Client", "SSL_30"]
},
"type": "Chassis",
"uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
"userDefinedName": "SN#Y010BG57Y01G",
"userDescription": "",
"uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
"vpdID": "336"
}
}],
"complexList": [],
"height": 52,
"nodeList": [],

```

```
    "location": "",
    "placeholderList": [],
    "room": "",
    "storageList": [],
    "switchList": [],
    "UUID": "STANDALONE_OBJECT_UUID"
  }
}
```

Chapter 4. Managing disk space

You can manage the amount of disk space that is used by Lenovo XClarity Administrator by moving large data files that are not immediately needed to a remote share or by deleting resources that are no longer needed.

About this task

To determine how much disk space is currently being used, click **Dashboard** from the XClarity Administrator menu bar. The disk space usage on the repository and remote shares is listed in the XClarity Administrator Activity section.

Procedure

Complete one or more of the following steps to free up disk space by moving files to a remote share and deleting unneeded resources.

- **Delete unneeded resources**

You can quickly delete files from the local repository that are no longer needed by completing the following steps.

1. From the XClarity Administrator menu bar, click **Administration → Disk Cleanup** to display the Disk Cleanup page.
2. Select the files that you want to delete. The section header identifies the amount of space that will be freed when the files are deleted.

- **Operating system related files**

You can delete OS Images, boot-option files, and software files.

- **Firmware updates**

You can delete payload files for all OS device drivers that are associated with UpdateXpress System Packs (UXSPs) and individual device drivers that are in the Downloaded state.

You can delete payload files for individual firmware updates that are in the Downloaded state and are not used in a firmware-compliance policy.

You can delete payload files for management-server updates that are in the Downloaded state.

Note: When the firmware-updates repository is located on a remote share, you cannot use the disk-cleanup function to delete individual firmware updates and UXSPs.

- **Service data files**

When service event occurs on a device, service data is collected automatically for that device. Service data is automatically captured for the management server every time an exception occurs in the XClarity Administrator. It is recommended that you periodically delete these archives if XClarity Administrator and the managed devices are running without issues.

When management-server updates are successfully applied, the update files are automatically removed from the repository.

3. Click **Delete Selected**.
4. Review the list of files that you selected, and click **Delete**.

- **Move firmware update packages to a remote repository**

By default, Lenovo XClarity Administrator uses a local (internal) repository for storing firmware updates. You can free up disk space that is available to the XClarity Administrator local repository by using a mounted remote share over SSH File System (SSHFS) as a remote repository. You can then use firmware update files directly from the remote repository to maintain firmware compliance on your devices. For more information, see [Using a remote repository for firmware updates](#) in the XClarity Administrator online documentation.

When you change the location of the firmware updates repository, you can choose to copy all firmware update from the original repository to the new repository.



Firmware update files in the original repository *are not* automatically cleaned up after switching locations.

Tip: The remote updates repository can be shared by multiple XClarity Administrator management servers.

To move firmware updates to a remote firmware-updates repository, complete the following steps.

1. Add a remote share to XClarity Administrator (see [Managing remote shares](#) in the XClarity Administrator online documentation).
2. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository**. The Firmware Updates Repository page is displayed.
3. Click **All Actions → Switch Repository Location** to display the Switch Repository Location dialog.
4. Select the remote share that you just created from the **Repository Location** drop down list.
5. Select **Copy update packages from current repository the new repository** to copy firmware update files to the new repository location before switching the repository location.
6. Click **OK**.

A job is created to copy firmware update packages to the new repository. You can monitor the job progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

7. Clean up firmware update files in the local repository.
 - a. Switch the location to the local repository by clicking **All Actions → Switch Repository Location**, select the **Local Repository** for the repository location, and then click **OK**.
 - b. Click the **Individual Updates** tab, click the select-all checkbox in the table to select all firmware updates, and then click the **Delete full update packages** icon ()
 - c. Click the **UpdateXpress System Pack (UXSP)** tab, click the select-all checkbox in the table to select all UXSPs, and then click the **Delete UXSP and associated policy** icon ()
 - d. Switch the location back to the remote repository by clicking **All Actions → Switch Repository Location**, selecting the new remote repository for the repository location, and then clicking **OK**.

- **Move XClarity Administrator backups to a remote share**

You can free up disk space that is available to the XClarity Administrator local repository by moving XClarity Administrator backups to a remote share. However, you cannot use the files directly on the remote share. To use the files, you must move them back to the XClarity Administrator local repository. For more information about remote shares, see [Managing remote shares](#) in the XClarity Administrator online documentation.

Important: It is recommended that you download backups to your local system or copy backups to a remote share before deleting the backups in XClarity Administrator.

1. From the XClarity Administrator menu bar, click **Administration** → **Back Up and Restore Data** to display the Back Up and Restore Data page.
Back Up and Restore Data



Back up and Restore this management server. [Learn more](#)

Repository usage: 0 KB of 50 GB



Label	Contains	Package location	Size	Date	Version	Requester
No items to display						

The **Package location** column identifies whether the backup is stored, either locally in the XClarity Administrator local repository or on a remote share.

2. Select the backup, and click the **Copy Backup** icon () to displays the Copy Backup dialog.
3. Choose the remote share to store the backup.
4. Click **Copy**.
5. Monitor the copy progress on the Jobs page. When the copy is complete, select the backup again, and click the **Delete Backup** icon () to display the Delete Backup dialog.
6. Select “Local” for the location.
7. Click **Delete**.

Chapter 5. Discovery and management issues

Use this information to troubleshoot device discovery and management issues.

Cannot discover a device

Use this information to troubleshoot issues when finding manageable devices.

1. Ensure that Lenovo XClarity Administrator supports the device. For a list of supported devices, see [XClarity Administrator Support – Compatibility webpage](#), click the **Compatibility** tab, and then click the link for the appropriate device types.
2. Ensure that the device is reachable on the network from XClarity Administrator and that XClarity Administrator is reachable on the network from the device.
3. Ensure that the correct ports are open in the firewall. For information about port requirements, see [Port availability](#) in the XClarity Administrator online documentation.
4. Ensure that unicast and multicast SLP is enabled on the network.
5. For ThinkServer servers,
 - a. Using the management web interface for the server, ensure that the hostname of the server is configured using a valid hostname or IP address.
 - b. Ensure that SLP is enabled and the hostname is enabled on ThinkServer System Manager (TSM).
 - To determine which ThinkServer servers have SLP enabled, send an SLP request querying for the WBEM service using your preferred SLP tool.

```
$ slptool findsrvs service:wbem
service:wbem:http://<TSM_IP>:5988,65535
service:wbem:https://<TSM_IP>:5989,65535
```
 - To determine whether SLP is enabled on a specific ThinkServer, send an SLP request querying for the WBEM service using your preferred SLP tool.

```
$ slptool unicastfindattrs <TSM_IP> service:wbem
(template-type=wbem),(template-version=2.0),(template-url-syntax=service:URL),
(service-hi-name=qom),(service-hi-description=Quasi Object Manager 1.0.0),
(CommunicationMechanism=cim-xml),(CommunicationMechanismsVersion=1.0),
(MultipleOperationsSupported=false),(AuthenticationMechanismsSupported=Basic),
(InteropSchemaNamespace=root/interop),(service-id=Lenovo G5 WBEM Service)
```
 - If a device is not responding to the SLP request, restart the TSM firmware by sending an IPMI command to the TSM using the following parameters. It might take several minutes for the TSM to restart.

```
NetFn = 0x06
Command = 0x03
Data = ()
```

The following example enables SLP using the `ipmitool` open-source tool.

```
$ ipmitool -H <TSM_IP> -U <ipmi_user> -P <ipmipassword> raw 0x06 0x03
```
6. For RackSwitch switches, ensure that SLP is enabled and the hostname is set in the switch configuration.
 - ThinkSystem DB series switches cannot be discovered. To manage these switches, manually input the IP address of the switch by clicking **Manual Input** on the Discover and Manage New Devices page.
 - NVIDIA Mellanox switches cannot be discovered. To manage these switches, manually input the IP address of the switch by clicking **Manual Input** on the Discover and Manage New Devices page.

- For other switches, ensure that SLP is enabled and the hostname is set in the switch configuration.
 - To determine which switches have SLP enabled, send the following SLP multicast request using your preferred SLP tool.

Note: This request finds only switches that are in the same subnet in which the SLP tool is running.

```
$ slptool findsrvs service:io-device.Lenovo:management-module
service:io-device.Lenovo:management-module://<RackSwitch IP>,64225
```

- To determine whether SLP is enabled on a specific switch, send the following unicast SLP request using your preferred SLP tool.

```
$ slptool findattrs service:io-device.Lenovo:management-module://<RackSwitch IP>
(level=1.0),(Type=switch),(data-protocols=ethernet),(serial-number=US71160000),
(sysoid=1.3.6.1.4.1.26543.1.7.6),(ipv4-enabled=TRUE),(ipv4-address=<RackSwitch IP>),
(ipv6-enabled=FALSE),ipv6-addresses,(ipv4-mgmt-protocols=http:80:true,https:443:true,
telnet:23:true,ssh:22:true,snmpv1v2v3:161:true,snmpv3only:161:false),
(snmp-engineid=80:00:67:af:03:08:17:f4:33:d3),
(ssh-fingerprint=8a:43:cb:be:47:d9:31:37:7a:3b:80:f6:dd:00:61:a6),
(deviceName=<RackSwitch hostname>)
```

7. For Lenovo Storage devices (other than ThinkSystem DE series), ensure that SLP is enabled and your network is not blocking SLP communication between XClarity Administrator and the storage device.

- To determine which storage devices have SLP enabled, send an SLP request querying for the API service using your preferred SLP tool.

```
$ slptool findsrvs service:api
service:api:https://<CONTROLLER_IP>:443/api,65535
service:api:https://<CONTROLLER_IP>:443/api,65535
```

- To determine whether SLP is enabled on a specific storage device, send an SLP request querying for the API service using your preferred SLP tool.

```
$ slptool unicastfindattrs <CONTROLLER_IP> service:api
(x-system-name=S3200_5.65),(x-system-location=rack\2Crack\2Crack),(x-system-contact=Support contact),
(x-system-information=S3200_65),(x-vendor-name=Lenovo),(x-product-id=S3200),(x-product-brand=Storage),
(x-midplane-serial-number=00C0FF2682A8),(x-platform-type=Gallium),(x-bundle-version=""),
(x-build-date=""),(x-health=OK),(x-wwnn=208000c0ff2682a8),(x-mac-address=00:00:00:00:00:EB)
```

If a storage device is not responding to the SLP request:

- Ensure that your network allows SLP communication between your devices.
- Ensure that your storage devices have **Storage Management Initiative Specification (SMI-S)** enabled, and restart the storage device using the management web interface or CLI.

Cannot manage a device

Use this information to troubleshoot issues when managing devices.

1. Ensure that the device is supported by Lenovo XClarity Administrator. For information about device support, see [XClarity Administrator Support – Compatibility webpage](#), click the **Compatibility** tab, and then click the link for the appropriate device types.
2. Ensure that the device is reachable on the network from XClarity Administrator and that XClarity Administrator is reachable on the network from the device.
3. Ensure that all ports that are appropriate for management are open on the network and firewalls. For information about port requirements, see [Port availability](#) in the XClarity Administrator online documentation.
4. Ensure that the minimum required firmware is installed on each server that you want to manage using XClarity Administrator. You can find minimum required firmware levels from the [XClarity Administrator](#)

[Support – Compatibility webpage](#) by clicking the **Compatibility** tab and then clicking the link for the appropriate device types.

5. Ensure that CIM over HTTPS is enabled on the device.
 - a. Log in to the management web interface for the server using the RECOVERY_ID user account,
 - b. Click **IMM Management → Security**.
 - c. Click the **CIM Over HTTPS** tab, and ensure that **Enable CIM Over HTTPS** is selected.
6. For ThinkSystem SR635 and SR655 servers:
 - Ensure that an operating system is installed, and that the server was booted to the OS, mounted bootable media, or efshell at least once so that XClarity Administrator can collect inventory for those servers.
 - Ensure that IPMI over LAN is enabled. IPMI over LAN is disabled by default on these servers and must be manually enabled before the servers can be managed. To enable IPMI over LAN using TSM, click **Settings → IPMI Configuration**. You might need to restart the server to activate the change.
7. If the device's server certificate is signed by an external certificate authority, ensure that the certificate authority certificate and any intermediate certificates are imported into the XClarity Administrator trust store (see [Deploying customized server certificates to managed devices](#) in the XClarity Administrator online documentation).
8. Ensure that the credentials are correct for the device.

Note: Ensure that the password follows the security and password policies for the device. Security and password policies might vary.

When the device is managed by XClarity Administrator, the management controller is put into centralized user management. This means that the user accounts that are defined in the XClarity Administrator internal or external authentication server are also used to log in to the management controller. A new local user account named RECOVERY_ID is created while all other local accounts are disabled on the management controller.

If the management process failed while configuring centralized user management, the local user accounts on the management controller might be disabled. Perform the following steps to recover the local user accounts:

- Converged, NeXtScale, and System x servers
 - a. Log in to the management web interface for the server using the RECOVERY_ID user account.
 - b. Click **IMM Management → User**.
 - c. Configure the user-authentication method on the management controller to **Local first, then LDAP**.
 - 1) Click **Global Login Settings**. The Global Login Settings dialog is displayed.
 - 2) Click the **General** tab.
 - 3) Select **Local first, then LDAP** for the user-authentication method, and click **OK**.
 - d. Delete and re-create any local user accounts (other than the RECOVERY_ID user account).
 - e. Attempt to manage the chassis again using the **Force management** option to clean up any remaining CIM subscriptions from the previous management attempt.
- Chassis
 - a. Log in to the management CLI for the chassis from an SSH session using the RECOVERY_ID user account.
 - b. Run the following command to disable centralized user management and allow you to authenticate to the management controller and other chassis components using local user accounts.

Note: After you run this command, the RECOVERY_ID user account is removed from the user registry, and the CLI session terminates. You can now authenticate to the management controller and other chassis components by using local user accounts.

```
fsmcm -off -T mm[p]
```

- c. Attempt to manage the chassis again using the **Force management** option to clean up any remaining CIM subscriptions from the previous management attempt.
9. For RackSwitch switches
 - Ensure that SSH is enabled on the switch.
 - If set, ensure that the “enable” password that is used to enter Privileged Exec Mode on the switch is correct.
 10. For a System x3950 X6 server, the servers must be managed as two 4U enclosures, each with its own baseboard management controller.
 11. If the system board was replaced in the device, the device was given a new serial number and UUID. If you want XClarity Administrator to recognize the device as the same device as before the replacement, you must update the serial number and UUID to match what it was previously. See the documentation for the device for instructions.
 12. If the device was managed by XClarity Administrator but was not unmanaged correctly, see the following information for recovery steps:
 - [Recovering chassis management with a CMM after a management server failure](#) in the XClarity Administrator online documentation
 - [Recovering server management after a management server failure](#) in the XClarity Administrator online documentation
 - [Recovering a RackSwitch switch that was not unmanaged correctly](#) in the XClarity Administrator online documentation
 - [Recovering management with a Lenovo storage device after a management server failure](#) in the XClarity Administrator online documentation

Cannot manage a storage device due to an invalid SSL/TSL certificate

Use this information to troubleshoot issues when managing storage arrays.

Each device has a self-signed SSL certificate that Lenovo XClarity Administrator uses to communicate with the device through HTTPS. This certificate has a common name (CN) that identifies the host name (or IP address) that is associated with the certificate. The common name represents the name that is protected by the SSL certificate, and the certificate is valid only if the request hostname matches the certificate common name. Therefore, if the IP address of the storage array is changed, the existing certificate becomes invalid, and XClarity Administrator cannot manage it due to an invalid SSL/TSL certificate.

To resolve this issue:

- Ensure that the IP address in the CN value of the certificate that sent from the DE storage device is in IPv4 format.
- Ensure that the existing SSL/TSL certificate is valid
 - For Lenovo ThinkSystem DE storage arrays, reset the management certificate on the storage array to the factory self-signed certificate. For more information, see [Reset management certificates](#) in the ThinkSystem Storage DE Series online documentation
 - For Lenovo ThinkSystem DS storage arrays, restart the management controllers in the storage device using the management web interface or CLI to regenerate the certificate with the correct CN using the new IP address or hostname.

Cannot manage a switch due to an invalid SSL/TSL certificate

Use this information to troubleshoot certificate issues when managing switches that are running CNOS.

Each device has a self-signed SSL certificate that Lenovo XClarity Administrator uses to communicate with the device through HTTPS. If you delete or regenerate the certificate on the switch, communication between the switch and XClarity Administrator fails and the switch appears offline.

To fix this problem, from the All switches page, select the switch and click **All Actions → Security → Resolve Untrusted Certificates**.

Cannot recover connectivity of a managed Flex System chassis after replacing the rear LED card or midplane assembly

Lenovo XClarity Administrator manages devices using its universally unique identifier (UUID) and UUID-based trusted certificate. For Flex System chassis, the UUID is stored as part of the vital product data (VPD) on the rear LED card that is on the midplane assembly. When you replace the rear LED card or midplane assembly, you must transfer the UUID of the replaced rear LED cards to the new rear LED card.

1. Obtain the UUID for the chassis. If the chassis is not operating, you can obtain the UUID by contacting Support and providing the machine type and serial number, which you can find on one of the chassis labels.
2. Change the UUID for a chassis. See the [Lenovo Flex System online documentation](#) for your device for midplane/rear LED card replacement and UUID change instructions.
3. Resolve untrusted certificates for the chassis.
 - a. From the XClarity Administrator menu bar, click **Hardware → Chassis**. The All Chassis page is displayed.
 - b. Select the chassis with the replaced part.
 - c. Click **All Actions → Security → Resolve Untrusted Certificates**.
 - d. Click **Install Certificate**.

XClarity Administrator retrieves the current certificate from the target chassis and places it in the XClarity Administrator trust store, overriding the previous certificate for that chassis.

4. Refresh inventory for the chassis by clicking **All Actions → Inventory → Refresh Inventory**.

Cannot recover connectivity of a managed server after replacing the system board

Lenovo XClarity Administrator manages devices using its universally unique identifier (UUID) and UUID-based trusted certificate. For servers, the UUID is stored as part of the vital product data (VPD) on the system board. When you replace the system board, you must transfer the UUID of the replaced system board to the new system board.

Important: It is a best practice to unmanage the server before replacing the system board. You can then remanage the server after the system board is replaced.

To transfer the UUID of the replaced system board to the new system board, complete the following steps.

1. Obtain the UUID for the server. If the server is not operating, you can obtain the UUID by contacting Support and providing the machine type and serial number, which you can find on one of the server labels.

2. Change the UUID for a server. See the hardware manual for your device for component replacement and UUID change instructions.
3. Resolve untrusted certificates for the server.
 - a. From the XClarity Administrator menu bar, click **Hardware** → **Server**. The All Chassis page is displayed.
 - b. Select the server with the replaced part.
 - c. Click **All Actions** → **Security** → **Resolve Untrusted Certificates**.
 - d. Click **Install Certificate**.

XClarity Administrator retrieves the current certificate from the target server and places it in the XClarity Administrator trust store, overriding the previous certificate for that server.

4. Refresh inventory for the server by clicking **All Actions** → **Inventory** → **Refresh Inventory**.

Encapsulation is not disabled after a server is unmanaged

If global encapsulation is enabled, the encapsulation mode changes to “encapsulation lite” when you manage a server. Typically, when you unmanage the server, the encapsulation mode is set back to “normal” (disabled).

If the encapsulation mode does not change to “normal,” complete the following step to disable encapsulation:

1. Reboot the baseboard management controller.
2. Connect to the target server from a system that is configured to use the IP address of the failed Lenovo XClarity Administrator virtual appliance. Then, disable encapsulation by opening an SSH session to the device and running the following command:
`encaps lite off`

Compute node does not display in the user interface after management

If you swap a ThinkSystem SD530 in a chassis without first unmanaging the existing server, the new server might not display in the user interface.

To resolve this issue, unmanage the chassis using the Force option, and then manage all ThinkSystem SD530 in a chassis again.

Server power state is not correct

If a server without an operating system is powered on, Lenovo XClarity Administrator might show an incorrect power state for that server.

Perform one of the following procedures to resolve this issue:

- Ensure that bare-metal servers are powered off.
- For XClarity Administrator v1.2.2 or later, boot the server to BIOS/UEFI (F1) Setup (see [Powering on and off a server](#) in the XClarity Administrator online documentation).

Chapter 6. Installation, removal, update, and data migration issues

Use this information to troubleshoot installation, removal, update, and data migration issues.

Video output does not display when installing XClarity Administrator in Red Hat KVM

When installing Lenovo XClarity Administrator virtual appliance using the Red Hat KVM user interface, the video output might not display through the console, resulting in a black console screen when you powered the XClarity Administrator virtual machine instead of the virtual-machine banner with XClarity Administrator IP info.

To see video output through the console, ensure that the video device is set to **Cirrus** by opening the XClarity Administrator virtual hardware details screen and clicking **Video** in the left navigation. By default, the RedHat KVM user interface sets the video device to QXL.

Adapter changes are not recognized

After removing, replacing, or configuring adapters, Lenovo XClarity Administrator does not recognize the changes.

Restart the device to allow the baseboard management-controller (BMC) to recognize the changes. See [System x online documentation](#) for more information.

During initial setup, unable to open the initial setup wizard in a web browser

Use this information to troubleshoot issues when initially setting up Lenovo XClarity Administrator.

1. Ensure that your physical host system meets the minimum system requirements (see [Supported host systems](#) in the XClarity Administrator online documentation).
2. Ensure you are using a supported virtual system that meets the minimum system requirements (see [Supported host systems](#) in the XClarity Administrator online documentation).
3. Ensure that the version of your web browser is compatible with XClarity Administrator. For a list of supported web browsers, see [Accessing the XClarity Administrator web interface](#) in the XClarity Administrator online documentation.
4. By default, DHCP is enabled for network configurations. Verify a valid IP address was assigned by logging in to the virtual machine locally and running the `ifconfig` command. If you are using a static configuration, ensure that you follow the following steps to correctly configure your installation For more information, see [Installing XClarity Administrator in VMware ESXi-based environments](#) in the XClarity Administrator online documentation.

Lenovo XClarity Administrator deployment unexpectedly fails

Use this information to troubleshoot issues when initially setting up Lenovo XClarity Administrator.

1. Check the event log for any events that are related to deployment, and resolve those first. For more information about the event log, see [Working with events](#) in the XClarity Administrator online documentation.

2. Ensure that your physical host system meets the minimum system requirements.
3. Ensure your system or virtual system meets the minimum system requirements.
4. Ensure you are using a supported virtual machine manager.

For more information about requirements, see [Supported host systems](#) in the XClarity Administrator online documentation.

Lenovo XClarity Administrator update has failed

Use this information to troubleshoot issues with updating Lenovo XClarity Administrator.

1. Ensure that you have installed any prerequisite updates.
2. Ensure that you have the user permissions to install updates.

For more information about updating XClarity Administrator, see [Updating the XClarity Administrator management server](#) in the XClarity Administrator online documentation.

Chapter 7. Connectivity issues

Use this information to troubleshoot connectivity issues.

Cannot access Lenovo XClarity Administrator

Use this information to troubleshoot issues when connecting to Lenovo XClarity Administrator.

If the host operating-system was shut down unexpectedly, restore XClarity Administrator from the last backup. For information about backing up and restoring XClarity Administrator, see [Backing up and restoring XClarity Administrator](#) in the XClarity Administrator online documentation.

Cannot connect to Lenovo XClarity Administrator using Safari Browser

Use this information to troubleshoot issues when connecting to XClarity Administrator using the Safari web browser.

When attempting to connect to the XClarity Administrator web interface using a Safari web browser, you are presented with a list of client certificates that are associated with your user account. Choosing any of those certificates might result in an “unable to connect” error. This issue might occur because the Safari web browser is attempting to send a client certificate to XClarity Administrator, but the client certificate is not valid for the XClarity Administrator server. To resolve the issue, delete the client certificate, and attempt to connect to the XClarity Administrator web interface again. For more information about this issue when using a Safari browser, see the [Safari client certificate problem webpage](#).

Cannot log in

Use this information to troubleshoot issues when logging in to Lenovo XClarity Administrator, CMM, and baseboard management controller.

Cannot log in to Lenovo XClarity Administrator

Use this information to troubleshoot issues when logging in to Lenovo XClarity Administrator.

1. Ensure that the password is correct and that the Caps Lock and Number Lock keys are not on.
2. Ensure that the user account is not locked. If it is locked, have a supervisor unlock the user account (see [Unlocking a user](#) in the XClarity Administrator online documentation).
3. Ensure that the user account is not disabled. If it is disabled, have a supervisor enable the user account (see [Enabling or disabling a user](#) in the XClarity Administrator online documentation).
4. If you are using an external authentication server:
 - a. Ensure that correct role groups are configured in XClarity Administrator. For information about role groups, see [Creating a role group](#) in the Lenovo XClarity Administrator online documentation.
 - b. Ensure that the user accounts are defined as members of one of those role groups on the external authentication server.
 - c. If you changed the password for the client account that is used to bind XClarity Administrator to the external authentication server, ensure that you also updated the new password in the XClarity Administrator web interface:
 - 1) Log in to XClarity Administrator using the client name and password that is currently defined in XClarity Administrator (see [Setting up an external authentication server](#) in the XClarity Administrator online documentation).

- 2) From the XClarity Administrator menu bar, click **Administration → Security**.
- 3) Click **LDAP Client** under the Users and Groups section to display the LDAP Client Settings dialog.
- 4) Update the password in the **Client password** field, and click **Apply**.

If the client account is locked out due to too many failed login attempts after the password was changed in external authentication server, either unlock the account directly in the external authentication server or wait for the lockout period to expire before trying to change the password in XClarity Administrator.

- d. If password for the client account that is used to bind XClarity Administrator to the external authentication server has expired, perform the following steps to unlock the account and change the password in XClarity Administrator.
 - 1) Unlock the client account and then change the client password in the external authentication server.
 - 2) Log in to XClarity Administrator using the client name and password that is currently defined in XClarity Administrator (see [Setting up an external authentication server](#) in the XClarity Administrator online documentation).
 - 3) From the XClarity Administrator menu bar, click **Administration → Security**.
 - 4) Click **LDAP Client** under the Users and Groups section to display the LDAP Client Settings dialog.
 - 5) Update the password in the **Client password** field, and click **Apply**.
5. If the host operating system was shut down unexpectedly, and you are now getting an authentication error, restore XClarity Administrator from the last backup. For information about backing up and restoring XClarity Administrator, see [Backing up and restoring XClarity Administrator](#) in the XClarity Administrator online documentation.

Password for a local recovery or supervisor user is forgotten

If supervisor account or if another supervisor account does not exist, you can reset the password for a local user with **lxc-recovery** or **lxc-supervisor** authority by mounting an ISO image that contains a configuration file with the new password.

Before you begin

Attention: This procedure does not work for XClarity Administrator v3.3.x and v3.4.x. If you using one of these versions, contact Lenovo Support for assistance to recover access to XClarity Administrator.

To reset the password using this method, you must have access on the XClarity Administrator host system.

The user name that is being reset must have **lxc-recovery** or **lxc-supervisor** authority.

The password must adhere to the same validation rules that XClarity Administrator enforces

After the password is reset, the user is not required to change the password on the first access

Procedure

To create and mount the ISO image, complete the following steps.

1. Power off the virtual machine.
2. Create a file named `passwordreset.properties` that contains the following parameters.


```
user=
password=
```

You can use the echo command to create the file, for example:

```
ECHO user=admin > ./ passwordreset.properties  
ECHO password=New_PasswOrd >> ./ passwordreset.properties
```

3. Create an ISO image that contains the passwordreset.properties file.

To create an ISO image on Windows, use your favorite ISO software. On Linux, use the `mkisofs` command, for example

```
mkisofs -V passreset -J -o ./passreset.iso ./passwordreset.properties
```

where **-V** is the volume label, **-J** is for Joliet format, **-o** is the output file name, and **/ passwordreset.properties** is the file to be included in the ISO image

4. Upload the ISO image to a suitable location using the Datastore Browser.
5. Mount the ISO image to the virtual machine.

- **For Citrix:**

- a. Mount the configuration .ISO image as a physical CD drive to the virtual machine.
- b. From Citrix , select the XClarity Administrator virtual machine.
- c. Click the **Console** tab.
- d. Select the physical CD from the drive list.

- **For Nutanix AHV hosts:**

- a. Click the **Settings** menu (⚙️), and then click **Image configuration** to display the Image Configuration dialog.
- b. Upload the `eth0_config.iso` image.
 - 1) From the Image Configuration dialog, click **Upload Image** to display the Create Image dialog again.
 - 2) Specify a name for the ISO image.
 - 3) Select ISO for the image type.
 - 4) Select **Upload a file**, click **Choose File**, and select the `eth0_config.iso` image.
 - 5) Click **Save** to upload the file.
 - 6) Click **Close** to close the Image Configuration dialog.
- c. Wait until the upload processes are completed before continuing with the setup steps. The status circle in the menu indicates when the processes are complete.
- d. Add a disk for the `eth0_config.iso` image.
 - 1) From the VM, click **Update** from the bottom menu bar.
 - 2) Click the **Edit** icon for the CDROM disk to display the Edit Disk dialog.
 - 3) Select **Clone** from Image Service for the operations.
 - 4) Select the ISO image that you created earlier from the image list.
 - 5) Click **Update**.
 - 6) Click **Save**.

- **For RedHat KVM hosts:**

- a. From Virtual Machine Manager, select the virtual machine, and then click **Add Hardware** to display the Add new Virtual Hardware dialog.
- b. Click the **Storage** tab.
- c. Select **Select managed or other existing storage**, click **Browse**, and select the `eth0_config.iso` image.
- d. Select **VirtIO** for the device type.

Note: For XClarity Administrator 1.4.0 and earlier, select **IDE** for the disk bus.

- e. Select **None** for the cache mode.
- f. Click **Finish**.

- **For VMware ESXi hosts:**

The ISO file must reside in the datastore of the ESXi host so that it can be mounted as a CD/DVD drive on the XClarity Administrator virtual machine.

- a. Right click the virtual machine, and click **Edit Settings**.
- b. Click **Add** to display the Add Hardware wizard.
- c. Click **CD/DVD Drive**, and click **Next**.
- d. Select **Use ISO image**, and click **Next**.
- e. Select the ISO image, and click **Next**.
- f. Select the virtual device node, and click **Next**.
- g. Click **Finish**.

- **For Windows Hyper-V hosts:**

Important: The virtual machine must be powered off before mounting the ISO image.

- a. In the Hyper-V Manager window, right-click the virtual appliance, and click **Connect** to display the Virtual Machine Connection window.
- b. Click **Media → DVD Drive → Insert Disk**.
- c. Select the ISO image, and click **Open**.

6. Power on the virtual machine, and then log in to the XClarity Administrator web interface using the user name and password that is specified in the passwordreset.properties file (see [Accessing the XClarity Administrator web interface](#) in the XClarity Administrator online documentation).

7. Unmount the drive, and delete the ISO image.

- For Citrix

- a. From the Citrix hypervisor, select the XClarity Administrator virtual machine.
- b. Click the **Console** tab.
- c. Clear the physical CD associated with the configuration ISO from the driver list.

- **For Nutanix AHV hosts:**

- a. From the VM, click **Update** from the bottom menu bar.
- b. Click the **Edit** icon for the CDRom disk to display the Edit Disk dialog.
- c. Click the **Eject** icon.
- d. Click **Save**.

- **For VMware ESXi hosts:**

- a. Right click the virtual machine, and click **Edit Settings**.
- b. Select the mounted drive from the list of hardware, and click **Remove**.
- c. Click **OK**. The drive is now disconnected.
- d. Right click the virtual machine, and click **Edit Settings** again.
- e. Select the drive from the list of hardware, and clear the **Connect at power on** checkbox.
- f. Click **OK**.
- g. Delete the ISO image from the datastore.

- **For Windows Hyper-V hosts:**

- a. In the Hyper-V Manager window, right-click the virtual appliance, and click **Connect** to display the Virtual Machine Connection window.

- b. Click **Media → DVD Drive → Eject** *iso_image_name.iso*.
- c. Delete the ISO image from the datastore.

Cannot log in to the managed CMM directly

Use this information to troubleshoot issues when logging in to a managed CMM directly.

1. Ensure that the password is correct and that the Caps Lock and Number Lock keys are not on.
2. Ensure that the credentials match those stored on Lenovo XClarity Administrator. If the CMM is managed by XClarity Administrator, you cannot log in using local CMM accounts. For information about centralized and decentralized user management in XClarity Administrator, see [Managing the authentication server](#) in the XClarity Administrator online documentation.

Cannot log in directly to the management controller

Use this information to troubleshoot issues when logging in directly to a management controller .

1. Ensure that the password is correct and that the Caps Lock and Number Lock keys are not on.
2. Ensure that the credentials match those stored on Lenovo XClarity Administrator.
3. Ensure that the management-controller version is compatible with XClarity Administrator.
4. Ensure that only one XClarity Administrator server is managing the management controller.

Cannot log in to managed Flex Power System servers

Use this information to troubleshoot issues when logging in to a managed Flex Power System servers directly - Lenovo XClarity Administrator

If you have a chassis that contains both Flex System and Flex Power System servers, you might not be able to log directly in to the Flex Power System servers due to authentication issues.

When the chassis is managed by XClarity Administrator, the CMM is put into central user management. This means that the user accounts that are defined in the internal or external authentication server are also used to log in to the Chassis Management Module (CMM), and local CMM user accounts are disabled.

To login to the management controller web interface of a managed Flex Power System server, use the RECOVERY_ID account that was created when the chassis was managed by XClarity Administrator. Log in to the CMM using this account, and change the password. (The password must be changed on first access.) After the password is changed, you can log in to the management controller web interface of the Power System node using the RECOVERY_ID account.

If you want to manage a Flex Power System node from an HMC (Hardware Management Console), complete the following steps:

1. Log in to the management CLI interface using SSH.
2. Run the following commands to configure the user-authentication method on the CMM to **Local then external authentication** and to delete and re-create the USERID account.

```
env -T mm[p]
accsecfg -am localldap
users -n USERID -clear
users -add -n USERID -p <password> -g Supervisor -ms 0
```

Sudden connectivity loss to a device

Use this information to troubleshoot issues when connecting to a single device

1. If the device that uses a stored credential is offline, verify that the stored credential has not become expired or invalid. If it has become expired or invalid, complete the following steps:
 - a. From the all devices page, select the device to be resolved.
 - b. Click **All Actions** → **Security** → **Resolve Stored Credentials**.
 - c. Change the password for the stored credential or select another stored credential to use for the managed device.
2. Check the event log for any network events for the device, and resolve those first. For more information about the event log, see [Working with events](#) in the Lenovo XClarity Administrator online documentation.
3. Ensure that the network hardware is functioning correctly for the connection path to the device.
4. Ensure that the correct switch and firewall ports are enabled for the device. For information about required ports, see [Port availability](#) in the XClarity Administrator online documentation.
5. Ensure that the device has a valid network configuration by logging in to the device and verifying that the IP address is valid for the network. You can also ping the device to test if it is visible on the network.
6. Attempt to log in directly to the device.

Chapter 8. Lenovo XClarity Administrator configuration issues

Use this information to troubleshoot issues with Lenovo XClarity Administrator configuration.

External LDAP setup issues

Use this information to troubleshoot issues when setting up an external authentication server.

1. Ensure that the root distinguished name is correct.
2. Ensure that the Lenovo XClarity Administrator user account is the member of at least one role group. For information about role groups, see [Creating a role group](#) in the XClarity Administrator online documentation.
3. Ensure that the XClarity Administrator role group matches at least one role group on the LDAP server.
4. If you are using preconfigured server addresses, ensure that the IP address and port number of the server are correct.
5. Ensure that the DNS configuration settings are correct.
6. If you are using DNS to discover servers, ensure that the domain name and forest name are correct.
7. Ensure that the client distinguished name and password are correct

For information about setting up the external authentication server, see [Setting up an external authentication server](#) in the XClarity Administrator online documentation.

User does not have sufficient authorization to configure servers

Use this information to troubleshoot issues when configuring managed servers.

1. Ensure that you are logged in to a user account that belongs to a supervisor or administrative role group. For information about user roles, see [Creating a role group](#) in the Lenovo XClarity Administrator online documentation.
2. Contact your system administrator to have your authority updated.

Features on Demand activation issues

Use this information to troubleshoot issues when activating features.

Ensure that you are following the directions for the tool that you are using to apply the Features on Demand (FoD) key. For more information about FoD keys, see [Viewing Feature on Demand keys](#) in the Lenovo XClarity Administrator online documentation.

VMware warning that VMXNET 3 driver is not supported

You might see a warning that the VMXNET 3 driver is not supported when installing Lenovo XClarity Administrator, editing the XClarity Administrator appliance virtual machine settings, performing vmotion of XClarity Administrator, or within VMware associated management and monitoring infrastructure.

The XClarity Administrator appliance includes the VMXNET 3 driver. You can safely ignore any VMware errors that state that the driver is not supported.

Chapter 9. Performance issues

Use this information to troubleshoot performance issues.

Lenovo XClarity Administrator performance issues

Use this information to troubleshoot performance issues with Lenovo XClarity Administrator.

If you have an environment with a large number of devices and a large number of concurrent user sessions, and you experience reduced system performance, reduce the number of concurrent user sessions to the XClarity Administrator web interface or increase the virtual CPU resources that are allocated to the virtual appliance.

Ensure that resources that are available to the virtual machine (memory, disk size, processor) are suitable for the number of devices that are being managed. For more information about the virtual machine requirements, see [Supported host systems](#) in the XClarity Administrator online documentation.

For additional performance considerations and tips, see the [XClarity Administrator: Performance Guide \(White paper\)](#).

Poor or slow network performance

Use this information to troubleshoot issues with poor or slow network performance.

1. Ensure that no major network operations are being performed, such as system discoveries, operating system deployments, or rolling firmware updates.
2. Ensure that the rest of the network is operating at a nominal usage.
3. If you have implemented quality of service, ensure that it is configured to allow optimal connectivity to Lenovo XClarity Administrator.
4. Ensure that your network topology is optimized for XClarity Administrator connectivity and performance.

Chapter 10. Security issues

Use this information to troubleshoot security issues, including user management and authentication.

SSL Certificate Cannot Be Trusted

The certificate chain might contain a signature that is self-signed or does not originate from a known Certificate Authority.

Ports 443, 3888, 9090, 50636, 50637

Each Lenovo XClarity Administrator instance has a unique, internally generated Certificate Authority (CA). By default these ports (used for communication between the user and virtual appliance or between the managed devices and virtual appliance) use a certificate that is signed by that CA. If the SSL certificate cannot be trusted, generate and deploy a customized externally-signed server certificate to XClarity Administrator. For more information, see [Deploying customized server certificates to XClarity Administrator](#) in the XClarity Administrator online documentation.

Port 8443

Each XClarity Administrator instance has a unique Certificate Authority (CA) that is used for only OS deployment. That CA signs a certificate that is used for the target server on port 8443. When OS deployment is initiated, the CA certificate is included in the OS image that is pushed to the target server. As part of the deployment process, that server connects back to port 8443, and verifies the certificate that port 8443 provide during the handshake because they have the CA certificate.

Server certification validation fails

Use this information when you attempt to install a server certificate in Lenovo XClarity Administrator and the validation of the certificate fails.

About this task

Server certification validation might fail when XClarity Administrator attempts to:

- Connect to managed devices using CIM-XML over HTTPS.
- Reach an external authentication server using secure LDAP (if you have configured a secure LDAP connection).
- Reach an external SAML identity provider using a secure connection (if you have configured SAML).
- Connect to the remote file servers for importing OS images (if you have configured an HTTPS image server).
- Connect to Lenovo to obtain warranty status information.
- Connect to the Apple and Google push-notification server (if Lenovo XClarity Mobile push notifications are enabled for an iOS or Android device).

Procedure

To resolve this issue, complete the following steps.

- Ensure that the certificate or its signing certificate exists in the Trusted Certificates trust store or the External Services Certificates trust store in XClarity Administrator. For more information about trusted certificates and external services certificates, see [Working with security certificates](#) in the XClarity Administrator online documentation.

- Ensure that the certificate has not been revoked (see [Adding and replacing a certificate revocation list](#) in the XClarity Administrator online documentation).
- Ensure that the server's IP address or hostname matches one of the subject alternative names or the common name (if SAN is not present) in the certificate.
- Ensure that today's date is between the "Not valid before" and "Not valid after" dates in the certificate.
- Ensure that the certificate is signed using a supported algorithm, either SHA1 or stronger if in legacy mode, or SHA256 or stronger if in NIST strict mode (see [Setting the cryptography mode and communication protocols](#) in the XClarity Administrator online documentation).

Samba and Apache vulnerabilities

Lenovo XClarity Administrator uses Samba and Apache servers as a read-only remote share when deploying operating system and updating OS device drivers. If you do not intend to use XClarity Administrator to manage operating systems, you can disable the Samba and Apache servers by setting the XClarity Administrator network role to discover and manage hardware only.

Procedure

To disable Samba and Apache servers, complete the following steps.

1. From the XClarity Administrator menu bar, click **Administration** → **Network Access**. The currently defined network settings are displayed.
2. Click Edit **Network Access** to display the Edit Network Access page.

Edit Network Access

IP Settings
Advanced Routing
DNS & Proxy

IP Settings

If you use DHCP and an external security certificate, make sure that the address leases for the management server on the DHCP server are permanent to avoid communication issues with managed resources when the management server IP address changes.

One network interface detected:

Eth0: Enabled - used to ?

	IPv4	IPv6
Eth0:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Use statically assigned IP address</div> <p>* IP address: <input type="text" value="10.243.2.107"/></p> <p>Network Mask: <input type="text" value="255.255.224.0"/></p>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Use stateless address auto configuration</div> <p>IP address: <input type="text" value="fd55:faaf:e1ab:2021:5054:ff:fec4:df97"/></p> <p>Prefix Length: <input type="text" value="64"/></p>
Default gateway:	<p>Gateway: <input type="text" value="10.243.0.1"/></p>	<p>Gateway: <input type="text" value="AUTO"/></p>

Save IP Settings
Restart
Back

3. Select the **discover and manage hardware only** option for the network interface.
4. Click **Save IP Settings**.
5. Click **Restart** to restart the management server.

Chapter 11. Troubleshooting backup and restore issues

Use this information to troubleshoot backup and restore issues.

Backup process seems to hang during management server restart

Generating a Lenovo XClarity Administrator backup might take a while. A progress bar shows the status of the job.

Procedure

If the backup process seems to hang, complete the following steps.

- If the **Cancel** button is visible, you can cancel the backup process.
- If the **Cancel** button is not visible, open a new tab to see if the **Cancel** button appears.
- If not this does not resolve the issue, reboot the virtual machine.

Note: If you cancel the backup process or reboot the virtual machine, a backup might not be created.

XClarity Administrator window is blank after refreshing during backup

Lenovo XClarity Administrator is quiesced during the procedure to prevent data from being modified. If you refresh or close the XClarity Administrator window before the backup process completed and the management server is restarted, the XClarity Administrator window might appear blank if the management server is still in quiesced mode.

Procedure

Complete the following steps to resolve this issue.

1. Refresh the page periodically to check if it loads.
2. If the window remains blank after a considerable amount of time, restart the virtual machine.
3. If it still does not load, manually delete `/opt/lenovo/lxca/bin/QUIESCE_MODE_FLAG` file.

Note: This step requires root access. Contact Support before performing this step.

4. Restart the XClarity Administrator virtual machine.

Chapter 12. Event monitoring and forwarding issues

Use this information to troubleshoot event monitoring and forwarding issues.

Events are not forwarded

Use this information to troubleshoot issues when forwarding events.

- If a schedule is created for the event forwarder, only events that occur during the scheduled time slot are forwarded. Ensure that the scheduled time has not elapsed.
- For email-based web services:

- If a secure connection type is selected for the event forwarder, Lenovo XClarity Administrator attempts to download and import the SMTP server certificate to its truststore. You are asked to accept adding this certificate to the truststore. If this fails, the connection to the SMTP server is not possible.

To resolve this issue, manually import the certificate into the XClarity Administrator truststore by clicking **Administration** → **Security** → **Trusted Certificates**, and the **Create** icon ().

- Verify whether your SMTP server accept only emails that have been sent by a registered user. If this is the case, the default sender address (LXCA.<source_identifier>@<smtp_host>) will be rejected. To resolve his issue, specify at least a domain name in the **From address** field in the event forwarder.
- If you are using OAUTH2 authentication, ensure that the security token has not expired. If it has expired, use the [oauth2.py](#) Python script and the refresh token to generate a new security token. Then, update the event forwarder in XClarity Administrator with the new security token. For more information, see [Setting up event forwarding to a Gmail SMTP service](#).

Chapter 13. Device management issues

Use this information to troubleshoot issues with device management-operation issue..

Cannot securely erase drive data on frozen drives

Use this information to troubleshoot issues when secure erase fails on SATA hard drives with the error Disks are frozen and cannot be erased.

Onboard SATA hard drives are in the frozen state by default. If the server has a frozen drive, Lenovo XClarity Administrator temporarily unfreezes the frozen drive and then boots to Bare Metal Update (BMU) to erase the drive. When the XClarity Administrator BMU quits and the server boots to the operating system, the drive becomes frozen again automatically.

When a server is managed in XClarity Administrator using *managed authentication* mode, the XClarity Administrator creates the SYSMGR_xxx LDAP account to manage and monitor the server instead of local credentials (see [Managing the authentication server](#) in the XClarity Administrator online documentation). The SYSMGR_xxx LDAP account does not have an IPMI privilege, so XClarity Administrator cannot unfreeze the disk, causing the secure-erase operation to fail on that server.

To resolve this issue, manage the server using *local authentication* mode, and then attempt to securely erase the drives.

Cannot securely erase SATA SDD volumes when connected to Marvel RAID

Use this information to troubleshoot issues when secure erase fails on SATA SDDs with volumes when connected to Marvell RAID controllers.

You cannot securely erase SATA SDD volumes that are connected to Marvell RAID controllers. Instead, consider the following recommendations.

- For 7mm SATA SSDs, connect to Broadcom RAID controllers to perform secure erase.
- For M.2 SATA SSDs, connect to Marvell non-RAID controllers (such as ThinkSystem M.2 SATA/NVMe 2-Bay Enablement Kit) to perform secure erase.

There is an internal timeout (9 seconds) in the Marvell RAID firmware. If the SSD does not respond to the command in time (does not finish the erase), the Marvell RAID firmware resets the SDD, the SDD becomes locked, and the secure erase fails. To unlock the SDD, run the following command.

```
hdparm --user-master u --security-unlock user123 %diskName%
```

Inventory data is not up to date after adding or replacing cards

For AMD1P and TSM based devices, Lenovo XClarity Administrator might not display correct inventory data, such as FRU and firmware, for newly inserted PCIe cards.

XClarity Administrator automatically fetches inventory data from managed devices every 24 hours. You can either wait for the next inventory collection, or you can manually collect the inventory data by selecting the server on the Server page and then clicking **Actions** → **Inventory** → **Refresh Inventory**.

Chapter 14. Server configuration issues

Use this information to troubleshoot issues with server patterns and profiles.

When creating a pattern from an existing server, an error is encountered

Use this information to troubleshoot issues when creating server patterns from an existing managed server.

1. Ensure that the server status is not Offline. For more information about server patterns, see [Creating a server pattern](#) in the Lenovo XClarity Administrator online documentation.
2. Retry the operation.

When deploying a pattern to a device, an activation error is encountered

An activation error indicates that an issue occurred when deploying the server pattern to a managed device. An activation error can occur for a number of reasons. Use this information to troubleshoot these types of issues.

Review the details of the job from the Jobs page by locating the server-profile activation job with the status “Stopped With Error” and clicking the job. To identify the issue, review the error messages.

- Connectivity or network routing issues between Lenovo XClarity Administrator and the managed device.

These issues might be represented in the job messages as LDAP errors. This indicates that there was an issue related to the device connecting to the virtual appliance over one of the configured network interfaces.

Ensure that the network connection between the XClarity Administrator virtual appliance and the device is operational. If they are on different network segments, ensure that there is network routability between the two segments.

- One or more configuration settings in the server pattern result in a setting change that is not valid on the selected managed device. Consider the following examples.

- The selected UEFI Extended Pattern is not compatible with the selected device.

For example, if a UEFI pattern that is provided with XClarity Administrator for an X6-based server (such as System x3950 X6) is selected and deployed to a System x3650 M4 server, the differences in the processor settings between the two servers might cause the profile activation to fail. To resolve the issue, ensure that the selected Extended UEFI Pattern is compatible with the selected server.

- A Port Pattern for an Ethernet adapter port is assigned to a port that does not support the selected settings.

For example, on Emulex-based adapters, there are settings that are only exposed on the first port of the adapter, specifically Advanced Mode and the Port settings that are used to disable a port. If these settings are assigned to the second port of the adapter, an activation error might occur. These issues might be represented in the job messages as `AdvancedMode is not a setting` or `Port1 is not a setting`. To resolve this issue, ensure that the port pattern that includes these Extended Port Pattern settings for Advanced Mode or Port Enablement is assigned to only the first port of the adapter.

- Some settings are not supported on the selected managed device after a firmware update.

For example, after updating firmware for an I/O adapter, some settings might be removed or renamed by the new firmware, and therefore the setting in the server pattern is not valid on the target server. These issues are represented in the job message as `xxx is not a setting.` To resolve this issue, you can learn a new server pattern from the server, so the new pattern includes all the settings that are

supported with the new firmware. If you need to keep using the old pattern, manually edit the server pattern to remove the invalid settings.

- An error occurs while powering on or restarting the server when Full Activation is selected for the pattern or profile deployment

Ensure that the device power state is stated correctly in XClarity Administrator. If not, refresh the inventory to synchronize the power state:

1. From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).
2. Select the server, and click **All Actions → Refresh Inventory**.

An invalid configuration is deployed to a switch

Use this information to troubleshoot issues when an invalid configuration is deployed to a switch

VLAN IDs must be created before adding a port to a specific VLAN. If a port pattern contains switch inner-port VLANs settings with VLAN IDs that have not been preconfigured for the switch, the profile activation might be successful, but the unapplied and invalid configuration on the switch must be repaired.

To resolve this issue, log in to the switch and manually configure the prerequisites, or back out the changes by deploying a pattern with valid settings.

Chapter 15. Firmware update and repository issues

Use this information to troubleshoot firmware-update issues.


Failed to connect to the Lenovo repository

Lenovo XClarity Administrator v2.8 and earlier use an HTTP connection to the Lenovo Support to refresh the firmware-updates catalog and to download update packages; however, the Lenovo Support now require an HTTPS connection.

Install the latest GAFix on your XClarity Administrator instance, or upgrade to XClarity Administrator v3.0.0 or later.

After successful firmware update, Apply/Activate page does not show updated firmware versions

Use this information to troubleshoot issues with the Firmware Updates: Apply/Activate page.

Ensure that the latest inventory is being compared by clicking the **Refresh** icon () on the Firmware Updates: Apply/Activate page to request a synchronization with the Lenovo XClarity Administrator appliance data.

Cannot connect to fix central to download firmware updates

Use this information to troubleshoot issues when downloading firmware updates from Fix Central.

1. Ensure that Lenovo XClarity Administrator has internet access and is using an open port for downloads. For information about port requirements, see [Port availability](#) in the XClarity Administrator online documentation.
2. Ensure that the XClarity Administrator appliance port (eth0 or eth1) that is configured for management has internet access. For more information about network considerations, see [Network considerations](#) in the XClarity Administrator online documentation.

Cannot update firmware on a device

Use this information to troubleshoot issues when updating firmware on managed devices.

- Review [Firmware update considerations](#) in the XClarity Administrator online documentation, and follow the recommendations provided.
- Ensure that the server status is not Offline and is reachable on the network from Lenovo XClarity Administrator.
- If you encounter a problem updating firmware on an FC5022 switch running FOS v7.4.x and earlier, run the following command from a command-line interface. For more information, see [Tech Tip HT507915](#).
`Seccrypto -- default -type SSH -force`

CMM Firmware Update Hangs

Use this information to troubleshoot issues when updating the CMM firmware, Flex stack release 1.3.2.1 2PET12K through 2PET12Q, that has been running more than three weeks and is part of a dual-CMM configuration.

1. Perform a virtual reset of the CMM. If you have two CMMs in the same chassis, virtually reset both CMMs simultaneously. You can find minimum required firmware levels from the [XClarity Administrator Support – Compatibility webpage](#) by clicking the **Compatibility** tab and then clicking the link for the appropriate device types.
2. Perform the update again from XClarity Administrator.

Firmware is up to date but fails the compliance check

Use this information to troubleshoot compliance issues after a firmware update.

Perform a virtual reset on the device, or run an additional update, such as an HDD update.

Firmware updates to Flex System switches unexpectedly fail

The following topics describe errors that can be found in the jobs log.

To find the messages, click **Monitoring** → **Jobs** from the Lenovo XClarity Administrator menu. The error message can be found by clicking the link for the job in the **Jobs** column to display the job summary and results dialog. Under the Target Results section, the message are listed in the **Message** column and starts with *****ERROR*****.

▼ Target Results: With Errors: 1 Running: 0 Completed: 0	
Target	Message
VDI-5K_CH4-VS: IO Module 03: IO Module Bay 3: IOM	Failed
▼	
Timestamp	Message
April 18, 2016 at 11:47:50	TaskMaanger: IO Module 03 bay 3 (172.16.25.153): IOM: Starting new process for task_id 9.
April 18, 2016 at 11:47:50	IO Module 03 bay 3 (172.16.25.153): IOM TaskType is: IOM : ues = CMMDelay=0, immDelay=0, pciCheck=true
April 18, 2016 at 11:56:19	IO Module 03 bay 3 (172.16.25.153): IOM Reported *** ERROR ***. Firmware download operation failed.
April 18, 2016 at 11:56:21	TaskManager: IO Module 3 bay 3 (172.16.25.153): IOM: Task_id 9 failed. rc=68
April 18, 2016 at 11:56:21	TaskManager: IO Module 03 bay 3 (172.16.25.153): IOM: StopOnError: Canceling the remaining non-required tasks in the job...

Important: Flex switch firmware updates using XClarity Administrator might fail intermittently. If you experience failures, follow suggestions in the following topics. If Flex switch firmware updates continue to fail using XClarity Administrator, update the Flex switches directly from the Flex switch interface.

Note: Firmware updates to a Flex System switch might fail unexpectedly if the switch is not running EHCM L3. For more information, see [Firmware update considerations](#) in the XClarity Administrator online documentation.

Firmware update to Flex switch failed, indicating an error with the message “Firmware download operation failed.”

Use this information to troubleshoot an IOM Reported *****ERROR*** Firmware download operation failed** error message in the jobs log. This might occur on EN4023 and FC5022 switches if you are attempting to perform a disruptive update that requires skipping an earlier firmware-update version and jumping directly to the latest.

To work around this problem, update the Flex switch directly from the Flex switch CLI or web interface.

For FC5022, migrating from FOS v7.3 to v8.0.1-pha is a disruptive update. Migrating from FOS v7.4 to FOS v8.0.1-pha is a non disruptive update.

You can find minimum required firmware levels from the [XClarity Administrator Support – Compatibility webpage](#) by clicking the **Compatibility** tab and then clicking the link for the appropriate device types.

Firmware update to Flex switch failed, indicating an error with the message “DCSS_RC_CDT_FAIL”

Use this information to troubleshoot an IOM: Reported *****ERROR*** DCSS_RC_CDT_FAIL** error message in the jobs log. This indicates that the Flex switch might be powered off or might be experiencing some other communication problem.

Take following actions in this order. After each step, try updating the firmware again.

1. Ensure that the Flex switch is powered on.
2. Ensure that the Flex switch has a valid IP address.
3. Reset the Flex switch.
4. Reset/reboot CMM.

Firmware update to Flex switch failed, indicating an error with the message “time out”

Use this information to troubleshoot an IOM: Reported *****ERROR*** time-out** error message in the jobs log. This might occur if the IP address of switch is not reachable on the network from Lenovo XClarity Administrator.

Take the following actions in this order. After each step, try updating the firmware again.

1. Ensure that the Flex switch has a valid IP address and is reachable on the network from XClarity Administrator.
2. Reset the Flex switch.
3. Reset/reboot CMM.

Firmware update to Flex switch failed, indicating an error with the message “Cannot download the same firmware version. Download another firmware.”

Use this information to troubleshoot an IOM: Reported *****ERROR*** Cannot download the same firmware version. Download another firmware.** error message in the jobs log. This might occur if you are attempting to update the EN4023 to the same level.

The EN4023 does not allow updating firmware to the same level that is already running.

Firmware update to Flex switch failed, indicating an error with the message of failed to contact host

Use this information to troubleshoot an IOM: Reported *****ERROR*** failed to contact host** error message in the jobs log. This might occur if the IP address of switch is not reachable on the network from Lenovo XClarity Administrator.

Take the following actions in this order. After each step, try updating the firmware again.

1. Ensure that the switch has a valid IP address and is reachable on the network from XClarity Administrator.
2. Restart the switch.
3. Restart the CMM.

Firmware update to Flex switch failed, indicating an error with the message “file does not exist”

Use this information to troubleshoot an IOM: Reported *****ERROR*** file does not exist** error message in the jobs log. This might occur if the IP address of the switch is not reachable on the network from Lenovo XClarity Administrator.

Take the following actions in this order. After each step, try updating the firmware again.

1. Ensure that the switch has a valid IP address and is reachable on the network from the XClarity Administrator.
2. Reset the switch.
3. Reset/reboot CMM.

Firmware update to Flex switch failed, indicating an error with the message of “flashing ended with failure”

Use this information to troubleshoot an IOM: Reported *****ERROR*** flashing ended with failure** error message in the jobs log. This might occur if the switch does not have a valid IP address.

Ensure that the switch has a valid IP address and is reachable on the network from the Lenovo XClarity Administrator.

Firmware update to the EN6131 40 Gb Ethernet Switch or the IB6131 InfiniBand Switch fails unexpectedly

Use this information to troubleshoot an unexpected failure when updating the firmware for the EN6131 40 Gb Ethernet Switch or the IB6131 InfiniBand Switch.

1. Check the job log for an error message from the switch, such as Not enough disk space available to download image.

Note: There might be additional information in jobs log. Often, this is in the format of IOM: Reported *****ERROR*** msg**, where *msg* is the specific error for that module.

2. Check your network speed and stability. Updating firmware might fail if the update is not completed within 30 minutes.
3. Free up sufficient disk space on the switch for the update file. The disk space is used when copying update files to the switch. See the [Lenovo Flex System EN6131 40Gb Ethernet Switch in the Flex Systems online documentation](#) for instructions on managing disk space.
4. Perform the update again from Lenovo XClarity Administrator.

Firmware update to the Lenovo EN4091 pass-thru module fails

Use this information to troubleshoot an unexpected failure when updating the firmware for the Lenovo EN4091 pass-thru module.

1. Check the jobs log for an error message from the pass-thru module, such as Firmware image fails data integrity check error or Failed to contact host.

Note: There might be additional information in jobs log. Often, message is in the format of IOM: Reported ***ERROR*** *msg*, where *msg* is the specific error for that module.

2. Perform a virtual reseal of the Lenovo EN4091.
3. Perform the update again from Lenovo XClarity Administrator.

Firmware update to Flex System switch failed, indicating an error with the message of “Host Key Authentication failed”

An error message in the jobs log in the format of “IOM: Reported ***ERROR*** Host Key Authentication failed.” is seen. This happens when the SFTP key has changed on an SFTP server that was used earlier to update the Flex System switch. The effected switches are CN4093, EN2092, EN4091, EN4093, EN4093R, SI4093.

In Lenovo XClarity Administrator, this error can occur if you have already updated firmware on a Flex System switch, and then you install another later version of XClarity Administrator or reboot XClarity Administrator and subsequently attempt to update the switch. This is because installing a new version of XClarity Administrator or rebooting the XClarity Administrator might cause a new SFTP key to be generated.

To resolve this problem, enter the following command from the CLI for a Flex System switch or a Lenovo Flex System switch to clear the SSH keys. Note that if the switch uses the ISCLI, you must be in the Configuration Terminal mode to run this command. You can change to Configuration Terminal mode by running the `enable` command, and then the `configure terminal` command.

```
clear ssh-clienthostkey all
```

Note: If the Flex System switch is in IBMNOS CLI mode, enter the following commands from the switch CLI to clear the SSH keys:

```
maint
clssh
all
exit
```

When performing an update, the system fails to enter Maintenance Mode

Use this information to troubleshoot issues with firmware updates and maintenance mode.

Retry the firmware update.

Restarting a server from the operating system does not activate maintenance mode

When updating firmware with delayed activation on any of the following servers, the update status shows “Pending maintenance mode” even after restarting the server from the operating system.

- Flex System x240 M5, Types 2591 and 9532
- NeXtScale nx360 M5, Type 5465
- System x3250 M6, Types 3633 and 3943
- System x3550 M5, Type 5463

- System x3500 M5, Type 5464
- System x3550 M5, Type 8869
- System x3650 M5, Type 5462
- System x3650 M5, Type 8871

To resolve this issue, restart the server from the management-controller web interface. When the server is back online, the update-activation process resumes.

Server running Red Hat Enterprise Linux (RHEL) does not restart

For Red Hat® Enterprise Linux (RHEL) v7 and later, restarting the operating system from a graphical mode suspends the server by default.

Manually configure the RHEL to change the behavior of the power button to power off. For instructions, see the [Red Hat Data Migration and Administration Guide: Changing behavior when pressing the power button in graphical target mode](#).

Chapter 16. OS device-driver update and repository issues

Use this information to troubleshoot OS device-driver-update issues.

Cannot connect to the Lenovo Support website to download device-driver updates

Use this information to troubleshoot issues when downloading UpdateXpress System Packs (UXSPs) and device drivers from the Lenovo Support website.

- Ensure that the Lenovo XClarity Administrator appliance port (eth0 or eth1) that is configured for management has internet access. For more information about network considerations, see [Network considerations](#) in the XClarity Administrator online documentation.
- Ensure that all required ports and Internet addresses are available before you attempt to update device drivers on a managed server. For more information about ports, see [Port availability](#) and [Firewalls and proxy servers](#) in the XClarity Administrator online documentation.

Cannot update device drivers on a server

Use this information to troubleshoot issues when updating device drivers on managed server.

- Ensure that the server is Online and is reachable on the network from Lenovo XClarity Administrator.
- Review the device-driver update considerations (see [OS device-driver update considerations](#) in the XClarity Administrator online documentation).

Chapter 17. Operating system deployment issues

Use this information to troubleshoot issues that you might encounter when you attempt to deploy operating systems to managed servers from Lenovo XClarity Administrator.

For general issues that are related to operating-system deployment, see [Cannot deploy an operating system](#).

Status reporting issues during OS deployment

Use this information to troubleshoot issues with status reporting by Lenovo XClarity Administrator during operating-system deployment.

- When deploying VMware 6.5 or later using XClarity Administrator v1.4.0 and earlier, the job status might report that deployment is complete before the operating system is ready.

When using scripts to monitor for the completion of OS deployment, add a 10 minute delay to the script after receiving the deployment job status indicating OS deployment is complete.

- When deploying Windows over a network that uses VLAN tagging, status errors might be reported during the *specialize configuration* pass of the deployment.

You can ignore these errors.

Cannot deploy an operating system

Use this information to troubleshoot general issues that you might encounter when you attempt to deploy an operating system to a managed server from Lenovo XClarity Administrator.

In slow network environments, operating-system deployment of SLES 12 and 12.1 in static IP mode might fail because the network delay boot parameter does not take effect in that mode. This issue is fixed in SLES 12.2.

Complete the following steps to resolve the issue:

1. For servers with XCC2 that have System Guard enabled and the action set to **Prevent OS booting**, ensure that System Guard is compliant on the device. If System Guard is not compliant, the devices are prevented from completing the boot process, which causes the OS deployment to fail. To provision these devices, manually respond to the System Guard boot prompt to allow the devices to boot normally.
2. If you see the `https://<management_server_IP>/osdeployment/connection/... Permission denied` message, update the BIOS on the server, and change the date and time setting to the current date and time.
3. Review all requirements for the operating system that is being deployed. See [Supported operating systems](#) in the XClarity Administrator online documentation. For example:
 - An issue can occur with the deployment of VMware ESXi if you do not set the Memory Mapped I/O (MMIO) space to at least 3 GB.
 - If you are deploying Microsoft Windows and joining an Active Directory domain, follow the considerations that are described in [Integrating with Windows Active Directory](#) in the XClarity Administrator online documentation.
4. Review operation-system deployment support limitations for specific I/O adapters. For information about I/O adapter support, see the [XClarity Administrator Support – Compatibility webpage](#).

5. Ensure that you have a stable network connection between XClarity Administrator and the device (managed server) on which the operating system is going to be installed.

Note: When deploying SLES 11 SP4, the deployment might stop and not restart if the network connection is lost between XClarity Administrator and the device. If this occurs, check your network environment, and redeploy the operating system.

6. Ensure that at least one network port on XClarity Administrator is set to manage and deploy operating-system images. You can configure the XClarity Administrator network topology from the Network Access page. For more information about the Network Access page, see [Configuring network access](#) in the XClarity Administrator online documentation.
7. Ensure the XClarity Administrator network port that is being used to attach to the data network is configured to be on the same network as the data network ports on the managed server. The server's port is specified by the MAC Address and is configurable through the Operating Systems -> Network Settings page. For more information about editing network settings, see [Configuring network settings for managed servers](#) in the XClarity Administrator online documentation.
8. Ensure that the target server does not have a deferred or partially activated server pattern. If a server pattern has been deferred or partially activated on the target server, restart the server to apply all configuration settings.
9. View the status of the server from the Deploy OS Images page to ensure that it has a deployment status of "Ready". If the status is "Not Ready", click the status link to determine why the server is not ready for operating-system deployment. For more information about operating-system deployment, see [Deploying an operating-system image](#) in the XClarity Administrator online documentation.
10. Ensure that the device has visibility to the storage location that was selected for operating-system deployment.

Tip: To ensure that operating-system deployments are successful, detach all storage from the server except the storage chosen for the operating-system deployment.

Cannot import a file into the OS-images repository

Use this information section to troubleshoot issues that you might encounter when you attempt to import files into the Lenovo XClarity Administrator image repository.

Complete the following steps to resolve the issue:

- Ensure that the file that is being imported has been verified through the checksum test.
- Ensure the base operating system is supported by XClarity Administrator. See [Supported operating systems](#) in the XClarity Administrator online documentation.
- If you are importing from the local system:
 - Internet Explorer and Microsoft Edge web browsers have an upload limit of 4 GB. If the file that you are importing is greater than 4 GB, consider using another web browser (such as Chrome or Firefox)
- If you are importing from a remote file server:
 - Ensure that the full path to the file matches the actual path on the remote file server.
 - Ensure that the full path to the file contains the correct forward or backward slashes, depending on the operating system that is hosting the remote file server.
 - Ensure that necessary permissions have been granted to the directory on the remote file server.
 - Ensure that there is enough disk space in the OS-images repository to store the file (see [Managing disk space](#) in the XClarity Administrator online documentation).
 - Ensure that you are logged in to the remote file server using the correct credentials.

- Ensure that you have a stable network connection between XClarity Administrator and the remote file server.
- Ensure that the correct trusted certificates have been imported and that the certificates have not been revoked (see [Working with security certificates](#) in the XClarity Administrator online documentation).
- Ensure that the remote server supports at least one algorithm that is supported by XClarity Administrator for each type of algorithm that is required by SSH (see [Implementing a secure environment](#) in the XClarity Administrator online documentation).

OS installer cannot find the disk drive on which you want to install

For servers that include software RAID adapters (such as 110i AnyRAID Adapter, ServeRAID C100 or C105 adapter, and Intel RSTe SATA Software RAID adapter), when the SATA adapter is enabled in the management controller, the SATA mode must be set to “AHCI.” Other modes (such as “RAID” and “IDE”) are not supported for software RAID by RHEL, SUSE, VMware or Windows operating systems.

Note: Each server must have a hardware RAID adapter that is installed and configured. The software RAID that is typically present on the onboard Intel SATA storage adapter is not supported. However, if a hardware RAID adapter is not present, setting the SATA adapter to AHCI SATA mode enabled operating-system deployment might work in some cases.

To modify the SATA mode for ThinkServers, complete the following steps.

1. From the AMI Setup Utility, select the **Advanced Settings** menu.
2. Use the arrow keys to select the **SATA Mode**.
3. Press **+** to change the value to AHCI.
4. Press **F10** to save the change.

To modify the SATA mode for other servers, complete the following steps.

1. From the F1 Setup Utility, select the **System Settings → Devices and I/O Ports → Onboard SATA Mode** menu.
2. Press **+** to change the value to AHCI.
3. Press **F10** to save the change.

OS installer cannot boot on a ThinkServer server

For ThinkServer servers, the Storage OpROM Policy on the ThinkServer Management Module must be set to “UEFI Only” for the OS installer image to boot correctly. If the policy is set to “Legacy Only,” the OS installer will not boot.

To modify the Storage OpROM Policy, complete the following steps.

1. From the AMI Setup Utility, select the **Boot Manager → Miscellaneous Boot Settings** menu.
2. Use the arrow keys to select the **Storage OpROM Policy**.
3. Press **+** to change the value to UEFI Only.
4. Press **F10** to save the change.

For more information, see your ThinkServer documentation.

VMware ESXi deployment issues

Use this information to troubleshoot issues that you might encounter when you attempt to deploy VMware ESXi operating systems to managed servers from Lenovo XClarity Administrator.

VMware deployment causes system hang or restart

During the installation of VMware 5.1u1, 5.1u2, 5.1u3, or 5.5 (any update) onto a managed server, the server might hang or restart.

The hang or restart might occur shortly after the following message:

```
Loading image.pld
```

VMware 5.5 requires Memory Mapped I/O (MMIO) space to be configured within the initial 4 GB of the server. Depending on the configuration, certain servers attempt to use memory higher than 4 GB, which can cause a failure.

Complete the following steps to resolve the issue:

Tip: Instead of setting **MM Config** through the Setup utility that are each server, consider using one of the predefined extended UEFI patterns related to virtualization, which sets the MM Config option to 3 GB and disables the PCI 64-bit resource allocation. For more information about these patterns, see [Defining extended UEFI settings](#) in the XClarity Administrator online documentation .

1. Restart the system. When Press <F1> Setup is displayed, press F1.
2. Select **System Settings → Devices and I/O Ports**.
3. Change the setting for **MM Config** from 2 GB to 3 GB.
4. Ensure that the setting for **PCI 64-Bit Resource** is set to Disable.
5. Attempt to install the VMware image again.

VMware deployment fails with disk errors

During the installation of VMware ESXi, an error that is related to the disk drive might be returned and the deployment does not succeed.

The error message might be similar to the following example:

```
error:/tmp/partitioning:line 2: install requires --disk
or --firstdisk
error:/tmp/partitioning:line 1: clearpart requires
one of the following arguments: --alldrives, --firstdisk,
--ignoredrives=, --drives=
```

This error might occur if the ESXi installer does not detect a SAS configuration that is available for formatting and installation. Typically, this means that the RAID configuration on the server is either inactive or configured incorrectly. Alternatively, this might happen if a server pattern was deployed through the Lenovo XClarity Administrator and **Disable local disk** was selected for the pattern.

Complete the following steps to resolve the issue:

- If a server pattern was deployed to this server and **Disable local disk** was selected, update the server pattern and deploy it again. For more information about configuring local storage using server patterns, see [Defining local storage](#) in the XClarity Administrator online documentation.
- Validate that the RAID configuration is correct on the server:
 1. Restart the server and attempt to boot into a legacy option by pressing F12 (choose something like HD0).
 2. During startup, when you see information about the LSI SAS adapter, press Ctrl-C to change the configuration.
 3. When the user interface displays, select **RAID properties**, and **View Existing Configuration**.
 - If **View Existing Configuration** does not appear, the RAID was not configured.

- If the existing configuration shows a status of “Inactive,” ensure that the RAID is configured correctly.

Operating system does not reboot to complete ESXi deployment on a ThinkServer server

Use this information to troubleshoot issues that you might encounter when you attempt to deploy VMware ESXi operating systems to managed servers from Lenovo XClarity Administrator when PXE is enabled on a network card or bootable devices other than the installation drive is included in the boot-order list..

When deploying ESXi on a ThinkServer server, the operating system does not explicitly move the drive on which the operating system is installed to the top of the boot-order list. If a boot device containing a bootable OS or a PXE server is specified before the boot device containing ESXi, then ESXi does not boot. For ESXi deployment, XClarity Administrator updates the boot-order list for most servers to ensure the ESXi boot device is at the top of the boot-order list; however, ThinkServer servers do not provide a way for XClarity Administrator to update the boot-order list.

If the ThinkServer server has network adapters that are PXE bootable, disable PXE support on the network adapters, redeploy the operating system, and then re-enable PXE support. Press F12 to intercept the boot to get to the PXE settings. For information about changing the PXE boot settings, see your network adapter documentation.

If the ThinkServer server has bootable devices in the boot-order list other than the drive on which the operating system is installed, remove the bootable devices from the boot-order list, redeploy the operating system, and then add the bootable device back to the list. Ensure that the installed drive is at the top of the list. For information about changing the boot-order list, see your ThinkServer documentation.

Red Hat and SUSE Linux deployment issues

Use this information to troubleshoot issues that you might encounter when you attempt to deploy Red Hat and SUSE Linux operating systems to managed servers from Lenovo XClarity Administrator.

Redhat 6.x cannot be deployed on rack-based server with static IP

An issue can occur when attempting to deploy Redhat 6.x to a managed server if that server is connected to a top-of-rack (TOR) switch. If the TOR switch has **spanning tree protocol** enabled and has **forward by default** disabled, the Redhat image might not be downloaded to the server.

Complete the following steps to resolve the issue:

- Ensure that the server is configured to use DHCP (and not a static IP address). Then, attempt to deploy the operating system again.
- Modify the configuration on the top-of-rack (TOR) switch to disable spanning tree protocol *or* enable packet forward by default.

OS deployment fails due to missing drivers

When deploying Red Hat® Enterprise Linux (RHEL) Server or SUSE® Linux Enterprise Server (SLES) to a server, you might see an error message that stops the deployment and the deployment job eventually times out.

This issue can occur when the operating-system image does not contain drivers to support all adapters that are installed in the managed server.

Out-of-box drivers are not preloaded in Lenovo XClarity Administrator for certain Mellanox IB adapters. Therefore, deploying RHEL or SLES to a server with these Mellanox adapters is not supported. For more

information about Mellanox adapter limitations, see the [Lenovo XClarity Administrator Support for Mellanox adapters webpage](#).

Microsoft Windows deployment issues

Use this information to troubleshoot issues that you might encounter when you attempt to deploy Microsoft Windows to managed servers from Lenovo XClarity Administrator.

OS deployment fails due to existing system partitions on an attached disk drive

When deploying Microsoft Windows to a server, attached disk drives must not have existing system partitions. If a partition is detected, the OS deployment fails.

Perform one of the following steps to resolve this issue.

- Disconnect the attached disk drive.
- Manually delete the system partition on the attached disk drive.

Attention: Deleting partitions on a disk drive might result in data loss. Ensure that you back up all data on the disk drive before deleting partitions.

1. From a Windows command prompt, run the `diskpart` utility (see [DiskPart Commands website](#)).
2. Select the disk by entering `select disk <number>`, where `<number>` is the disk number of the disk that contains the partition that you want to delete (see [Select disk website](#)).
3. Select the partition to delete by entering `select partition <number>` where `<number>` is the partition number on the selected disk (see [Select partition website](#)).
4. Delete the partition by entering `delete partition override`. The disk and partition numbers are included in the WinPE error message that appears when a system partition is detected and in the job log. (see [Delete partition website](#))

Chapter 18. Remote control issues

Use this information to solve problems that might occur when you use the remote-control application in Lenovo XClarity Administrator.

Remote-control session does not start

Use this information when you attempt to start the remote-control session from the Lenovo XClarity Administrator web interface or from the shortcut on your system, but it does not start.

To resolve the issue, complete the following steps.

1. Ensure that the server to which you are connecting is managed by XClarity Administrator, and is in the “Online” or “Normal” state. For more information about server status, see [Viewing the status of a managed server](#) in the XClarity Administrator online documentation.
2. Ensure that pop-up dialogs are not disabled in your web browser for the session.
3. Ensure that your web browser has accepted security certificates from XClarity Administrator. Typically, you are prompted to accept the certificate the first time that you access XClarity Administrator from your browser.
4. From the Remote Control window, click **Preferences** → **General** → **Synchronize with management server**, and wait for one minute. Then, open the remote control session again.
5. Ensure that you are using the supported JRE to start the application.
 - In Internet Explorer, click **Tools** → **Internet Options** → **Advanced**. Ensure that the correct JRE is selected (JRE version 7.0, update 18 or later).
 - In Firefox, click **Tools** → **Options** → **Applications**. Ensure that Java Web Start Launcher is associated with the JNLP content type.

Note: Ensure that the **Use SSL 2.0 compatible ClientHello format** option *is not* selected in the in Java Control Panel.

If you are starting the application from the shortcut on your desktop, ensure that your local system has connectivity to XClarity Administrator. The application validates your user ID with the XClarity Administrator authentication server.

6. Clear the Java Web Start cache on the local system. To clear the Java Web Start cache on a system that is running a Windows operating system, run the command `javaws -uninstall`. This can also be done from the Windows Control Panel in the JAVA menu.
7. Remote control requires that a Features on Demand key for ThinkServer System Manager Premium Upgrade is installed on ThinkServer servers. For more information about FoD keys that are installed on your servers, see [Viewing Feature on Demand keys](#) in the XClarity Administrator online documentation.

Remote-control session hangs after login

Use this information to resolve the issue when the remote-control session hangs after login.

If you are not using one of the supported JREs, the remote-control session might hang after login. If the remote-control session appears to hang after you log in, ensure that you are using the supported JRE to start the application:

- Oracle JRE version 6.18 or later

Cannot connect to a server

Use this information to resolve the issue when you cannot establish a remote-control session with a server.

Complete the following steps to resolve this issue.

- Ensure that you have **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin**, or **lxc-hw-manager** privileges.
- Ensure that your local system has network connectivity and that it can connect to Lenovo XClarity Administrator.
- Ensure that the server is being managed by XClarity Administrator by clicking **Hardware → Servers** from the XClarity Administrator menu bar.
- If a firewall is installed on your local system, ensure that the firewall allows connections to the IP address for the managed server.
- Ping the IP address of the managed server to ensure that your local system has connectivity to the managed server. If you are attempting to access a managed server from a local system that has an IP address from an external network, the managed server must also have an IP address that can be accessed externally.
- Ensure that XClarity Administrator tunneling has not been disabled so that XClarity Administrator can tunnel your remote-control requests to the managed server that is network addressable only on the private management network. Tunneling is enabled by default. You can enable XClarity Administrator tunneling from the remote-support Preferences dialog on the **Security** tab. For more information, see [Setting remote-control preferences](#).

Cannot communicate with a Flex System switch after starting a remote-control session

Use this information to resolve the issue when Lenovo XClarity Administrator stops communicating with a Cisco Nexus B22 Fabric Extender network switch after starting a remote-control session.

If the CMM is configured to use autosensing, ensure that the network port on the Cisco Nexus B22 Fabric Extender network switch is configured to use auto-negotiation mode.

Cannot connect to a server in single-user mode

Use this information to resolve the issue when you cannot connect to a server in single-user mode.

When you connect to a server in single-user mode, only one remote-control session can be established to the server at a time.

Complete the following steps to solve the issue.

1. Attempt to connect to the managed server in multi-user mode (if allowed, based on security requirements).
2. Contact other users to determine if anyone else has already established a remote-control session with the managed server. If so, wait until the user ends the remote-control session with the managed server.
3. Attempt to connect to the managed server in single-user mode again.

Remote Control can connect to a server, but no video is available

Use this information to resolve the issue when you are connected to a server from a remote-control session, but the session displays the No video available message.

Ensure that the server is powered on and that the operating system is running a supported resolution and refresh rate.

The following table lists the supported resolutions and refresh rates.

Table 1. Supported resolutions and refresh rates

Resolution	Refresh rates
640 x 480	60, 72, 75, and 85 Hz
800 x 600	60, 72, 75, and 85 Hz
1024 x 768	60, 72, 75, and 85 Hz
1440 x 900	60 Hz
1280 x 1024	60 and 75 Hz
1680 x 1050	60 Hz
1600 x 1200	60 and 75 Hz

A server does not appear in the list for adding a new session

Use this information to resolve the issue when a server does not appear in the list for adding a new session, or a server no longer appears in the thumbnail area.

Complete the following steps to resolve the issue.

1. Ensure that the managed server is being managed by Lenovo XClarity Administrator by clicking **Hardware → Servers** from the XClarity Administrator menu bar.
2. Synchronize the inventory by clicking the **General** tab on the remote-control Preference menu and then clicking **Synchronize with management server**. For more information about remote-control preferences, see [Setting remote-control preferences](#) in the XClarity Administrator online documentation.

State of server in remote-control session does not match state in the Lenovo XClarity Administrator

Use this information to troubleshoot when the state of a managed server in a remote-control session does not match the state of the managed server in Lenovo XClarity Administrator.

Complete the following steps to resolve this issue.

1. Ensure that the server is being managed by XClarity Administrator by clicking **Hardware → Servers** from the XClarity Administrator menu bar.
2. Synchronize the inventory by clicking the **General** tab on the remote-control Preference menu and then clicking **Synchronize with management server**. For more information about remote-control preferences, see [Setting remote-control preferences](#) in the XClarity Administrator online documentation.

A drive or image cannot be mounted to a server

Use this information to troubleshoot when you attempt to mount a drive or image by using remote media, but the drive or image cannot be mounted.

Complete the following steps to resolve the issue.

1. Stop and restart the remote-control session.

2. Set the debug mode to “Full” for the remote-control session. You can set the debug mode from Preferences on the **General** page. When you set debug mode to “Full”, the remote-control session generates diagnostic log files. For more information about the debug mode, [Setting remote-control preferences](#).
3. Contact Lenovo Support and provide the log files. For more information about sending diagnostic data to Lenovo Support, see [Working with service and support](#).

Storage media option is not shown in the list of remote media devices available for mounting

Use this information to troubleshoot when the storage-media option is not shown in the list of remote-media devices that are available for mounting.

If a CD, DVD, or USB device does not appear in the list of available remote-media devices to be mounted to a managed server, click **Relaunch using Administrator account** on the remote-media panel to access more local devices.

Power operation cannot be performed

Use this information to troubleshoot issues when you attempt to perform a power operation on a managed server within a remote-control session and it cannot be performed.

When you attempt to perform a power operation on a managed server from a remote-control session, you might receive a message stating that the power operation failed or that the power operation is not applicable to the current state of the managed server.

Complete the following steps to resolve the issue:

1. Ensure that the server is being managed by Lenovo XClarity Administrator. For more information, see [Viewing the status of a managed server](#) in the XClarity Administrator online documentation.
2. From the Servers page, verify that the status of the server is valid.
3. Ensure that the power operation is valid for the current state of the server. For example, if the server is currently powered off, issuing a power off will not work.
4. Check the jobs log to see if the power operation has completed. It might take some time for the operation to complete, depending on the current load of XClarity Administrator. For more information about viewing the job status, see [Monitoring jobs](#).

Video not available when connecting to Flex System x280 X6, x480 X6, and x880 X6 servers

Use this information to troubleshoot issues when you attempt to start a remote-console session with a Flex System x280 X6, x480 X6, and x880 X6 servers multi-node system or when no video appears in the new tab.

Complete the following steps to resolve the issue.

1. End the connection that you just started if it is still active by closing the new tab.
2. Ensure you start a remote connection with the *primary* server in the multi-node configuration.

Chapter 19. User interface issues

Use this information to troubleshoot user-interface issues.

Menu items, toolbar icons, and buttons are disabled (greyed out)

Use this information to troubleshoot issues when certain actions are disabled in the user interface.

A *role* is used to control user access to resources and limit the actions that users can perform on those resources. A *role group* is a collection of one or more roles and is used to assign those roles to multiple users. The roles that you configure for a role group determine the level of access that is granted to each user that is a member of that role group. Each Lenovo XClarity Administrator user must be a member of at least one role group. For information about roles and privileges, see [Managing roles](#) in the XClarity Administrator online documentation.

Ensure that your user account is assigned to a role group that has privileges that are required to perform the action. For more information, contact your system administrator.

Web browser becomes unresponsive when multiple tabs are open

When multiple tabs containing Lenovo XClarity Administrator pages are open, the web browser might crash or become unresponsive

XClarity Administrator uses client-side JavaScripts that exchange a large amount of data with the management server. When multiple tabs are open, the web browser consumes more memory, processor cycles, and network bandwidth. Several tabs can make some browsers crash or become unresponsive. The effect varies with web browser types and versions.

To resolve this issue, reduce the number of web browser tabs that contain XClarity Administrator pages.

For more information, see [Tip HT504133](#)


JSON response failed, parse error, and other unexpected errors

Use this information to troubleshoot JSON response issues.

Log out of Lenovo XClarity Administrator, and try to log back in.

User interface is not in the preferred language

Use this information to troubleshoot issues with language preferences.

1. Ensure that the web browser is using the locale of your preferred language.
2. From the Lenovo XClarity Administrator title bar, click the user-actions menu ( ADMIN_USER), and then click **Change language**. Select the language that you want to display, and then click **Close**.

Slow or seeming unresponsive load times, long wait to refresh, improper rendering

Use this information to troubleshoot issues with the user interface.

1. Refresh the page with the **Refresh** button on your web browser.
2. Clear the web-browser cache, and reload the page.

Unexpected loss of data

Use this information to troubleshoot data-loss issues in Lenovo XClarity Administrator.

If the host operating system was shut down unexpectedly, restore XClarity Administrator from the last backup (see [Backing up and restoring XClarity Administrator](#) in the XClarity Administrator online documentation).

Device location changes are not reflected in the rack view

Use this information to troubleshoot rack view issues in Lenovo XClarity Administrator.

If you change the location of a device using one of the following REST APIs or using the baseboard management controller after the device is managed by XClarity Administrator, the changes are not reflected in the rack view in the XClarity Administrator user interface. Edit the device properties or the rack in the user interface to reflect the changes made in the API or management controller (see [Modifying the system properties for a server](#), [Viewing the details of a managed chassis](#), and [Managing racks](#) in the XClarity Administrator online documentation).

- [PUT /canisters/<UUID>](#)
- [PUT /chassis/<UUID>](#)
- [PUT /nodes/<UUID>](#)

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

*Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property*

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

LENOVO, SYSTEM, NEXTSCALE, SYSTEM X, THINKSERVER, THINKSYSTEM, and XCLARITY are trademarks of Lenovo.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows, Windows Server, Windows PowerShell, Hyper-V, Internet Explorer, and Active Directory are registered trademarks of the Microsoft group of companies.

Mozilla and Firefox are registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Nutanix is a trademark and brand of Nutanix, Inc. in the United States, other countries, or both.

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.

SUSE is a trademark of SUSE IP Development Limited or its subsidiaries or affiliates.

VMware vSphere is a registered trademark of VMware in the United States, other countries, or both.

All other trademarks are the property of their respective owners.

Lenovo