



Lenovo XClarity Orchestrator User's Guide



Version 2.0.0

Note

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

First Edition (March 2023)

© Copyright Lenovo 2020, 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
---------------------------	----------

Summary of changesiii
-------------------------------------	-------------

Chapter 1. Lenovo XClarity Orchestrator Overview. **1**

Logging in to a local XClarity Orchestrator web interface.	3
User interface tips and techniques	6

Chapter 2. Administering XClarity Orchestrator **11**

Connecting resource managers	11
Discovering and managing devices	14
Device management considerations	15
Configuring global discovery settings	19
Managing servers	20
Managing ThinkEdge Client devices	24
Managing storage devices	27
Managing chassis	30
Using VMwareTools	33
Configuring network settings	33
Configuring the date and time	36
Working with security certificates	38
Adding a trusted certificate for external services	39
Adding a trusted certificate for internal services	40
Installing a trusted, externally-signed XClarity Orchestrator server certificate	41
Regenerating the internally-signed XClarity Orchestrator server certificate	43
Importing the server certificate into a web browser	45
Managing authentication	46
Setting up an external LDAP authentication server	46
Managing users and user sessions	50
Creating users	50
Creating user groups	52
Changing details for your user account	54
Changing details for another user	55
Configuring user security settings	56
Monitoring active user sessions	59
Controlling access to functions	60
Assigning roles to users	62
Controlling access to resources	62
Enabling resource-based access	63

Creating access-control lists	64
Managing disk space	65
Backing up and restoring orchestrator-server data	66
Backing up and restoring orchestrator-server data on a VMware ESXi host	67
Backing up and restoring orchestrator-server data on a Microsoft Hyper-V host	68

Chapter 3. Monitoring resources and activities **71**

Viewing a summary of your environment	71
Viewing resource manager status and details	74
Viewing devices status	75
Viewing device details	78
Viewing infrastructure resources status and details	80
Monitoring jobs	82
Monitoring active alerts	84
Monitoring events	86
Excluding alerts and events	88
Forwarding event, inventory, and metric data	89
Creating data-forwarding filters	90
Forwarding events to SAP Data Intelligence	93
Forwarding events to a REST web service.	95
Forwarding events to an email service using SMTP	97
Forwarding inventory and events to Splunk	102
Forwarding events to a syslog	104
Forwarding metrics data to a Lenovo TruScale Infrastructure Services	106
Forwarding reports	108
Creating forwarder destination configurations	108
Forwarding reports using email	110

Chapter 4. Managing resources. **113**

Creating resource groups	113
Managing devices offline	116
Performing power actions on managed servers	116
Opening a remote-control session for managed servers	118
Opening a remote-control session for ThinkSystem or ThinkAgile servers	118
Opening a remote-control session for ThinkServer servers	119
Opening a remote-control session for System x servers.	119

Chapter 5. Provisioning resources127

Provisioning server configurations 127

- Server-configuration considerations 129
- Learning a server-configuration pattern from an existing server 130
- Assigning and deploying a server-configuration pattern 132
- Maintaining server-configuration compliance. 136

Provisioning operating systems 137

- Operating-system deployment considerations 139
- Supported operating systems 141
- Operating-system image profiles 142
- Port availability for deployed operating systems 145
- Importing operating-system images 146
- Configuring operating-system profiles 148
- Deploying an operating-system image 150

Provisioning updates to managed resources 152

- Update deployment considerations 154
- Downloading and importing updates. 155
- Creating and assigning update-compliance policies 160
- Applying and activating updates to resource managers 163
- Applying and activating updates to managed servers 165

Chapter 6. Analyzing trends and predicting problems169

Creating custom analytics reports. 169

- Creating rules for custom analytics alerts 169

- Creating custom reports (queries) 172
- Analyzing device boot times 175
- Analyzing connectivity issues 175
- Analyzing security fixes. 175
- Analyzing drive health 176
- Analyzing firmware 177
- Analyzing lost events. 177
- Analyzing and predicting resource-manager capacity. 178
- Analyzing and predicting utilization trends 178
- Analyzing performance and usage metrics 179
- Analyzing repeated events 180
- Analyzing unauthorized-access attempts 181
- Analyzing device health. 181
- Analyzing infrastructure-resource health 183
- Analyzing active alerts 184

Chapter 7. Working with service and support187

Sending periodic data to Lenovo 187

- Collecting service data for XClarity Orchestrator 188
- Collecting service data for devices 189
- Importing service data for devices 191
- Creating and assigning contacts for service and support 192
- Automatically opening service tickets using Call Home. 193
- Manually opening a service ticket in the Lenovo Support Center 196
- Viewing service tickets and status. 199
- Viewing warranty information 201

Summary of changes

Follow-on releases of Lenovo XClarity Orchestrator management software support new software enhancements and fixes.

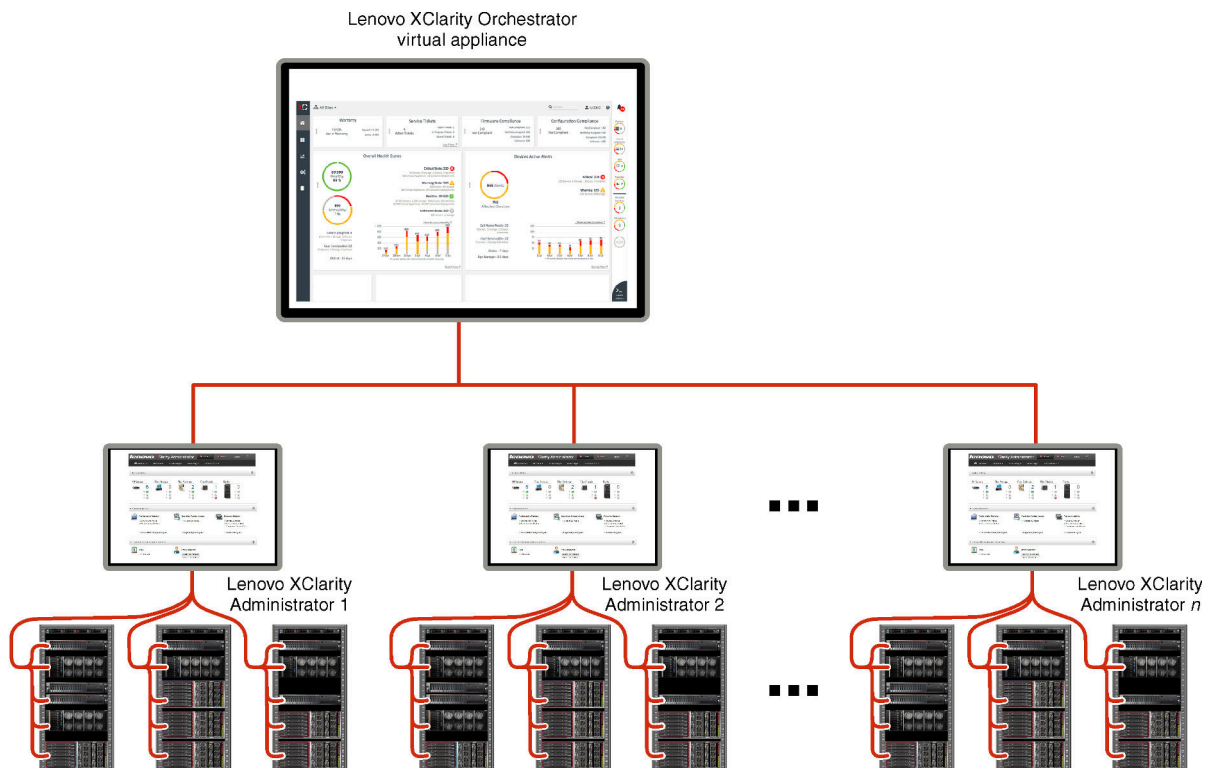
Refer to the change history file (*.chg) that is provided in the update package for information about fixes.

This version supports the following enhancements to the management software. For information about changes in earlier releases, See [What's new](#) in the XClarity Orchestrator online documentation.



Function	Description
Administering	The Configuration Patterns Administrator role and OS Administrator were added to control access to provisioning functions (see Controlling access to functions).
Managing resources	<p>Lenovo XClarity Management Hub is a new resource manager that you can use to manage ThinkEdge Client devices (see Connecting resource managers). You must install a UDC agent on ThinkEdge Client devices before the devices can be discovered and managed by the assigned XClarity Management Hub (see Managing ThinkEdge Client devices).</p> <p>You can manage devices directly from XClarity Orchestrator and assign management of those devices to a specific resource manager. XClarity Management Hub can be used to manage ThinkEdge Client devices. Lenovo XClarity Administrator can be used to manage servers, storage, switches, and chassis. (See Discovering and managing devices).</p> <p>You can unassign devices from a resource manager (see).</p>
Provisioning resources	<p>You can use XClarity Orchestrator to manage the OS-images repository and to deploy operating-systems to managed servers. XClarity Orchestrator sends requests to the applicable resource manager to perform the OS deployment. A dedicated disk is required to store operating system images. You must be a member of a user group to which the predefined OS Administrator role is assigned (see Provisioning operating systems).</p> <p>You can assign update-compliance policies to all or only selected resources without a policy assignment in addition to resources that are compliant and non-compliant with their assigned policy (see Creating and assigning update-compliance policies).</p> <p>You can update BIOS updates on ThinkEdge Client devices running Windows 10 (see Provisioning updates to managed resources).</p>

Chapter 1. Lenovo XClarity Orchestrator Overview

Lenovo XClarity Orchestrator provides centralized monitoring, management, provisioning, and analytics for environments with large numbers of devices. It leverages existing resource managers (such as Lenovo XClarity Administrator and Schneider Electric EcoStruxure IT Expert) across multiple sites to view overall health, collect device inventory and health summaries, drill down into device details, view event and audit logs, and apply updates to managed resources.



Learn more:

-  [XClarity Orchestrator Overview](#)
-  [Management capabilities](#)

Centralized monitoring and management of resources

XClarity Orchestrator provides a single interface to monitor and manage resource managers and the devices that are managed through those resource managers.

- Summary views of the health of your managed resources, including resource managers, devices, and infrastructure resources (such as PDUs and UPSs)
- Summary and detailed views of component health, asset inventory, warranty status, and advisories for devices across multiple sites
- Aggregation of critical alerts and events, creating custom alerts, and forwarding events to external applications
- Life-cycle control for managed devices (including power operations)
- Launch in context to the user interface for resource managers and managed devices from the device summary pages

Provisioning updates

You can use XClarity Orchestrator to maintain current software levels on managed resources. You can use the updates catalog to know what software levels are available, use update-compliance policies to identify which resources need to be updated based on custom criteria, and then deploy the desired updates to those resources. XClarity Orchestrator ensures that software is provisioned on the target resources in the correct order.

XClarity Orchestrator supports the following provisioning operations.

- Deploying updates to Lenovo XClarity Administrator resource managers.
- Deploying firmware updates to devices that are managed by XClarity Administrator.

For more information about provisioning updates, see [Provisioning updates to managed resources](#).

Provisioning server configuration

You can quickly provision managed servers using a consistent configuration. Configuration settings (such as baseboard management controller and UEFI settings) are saved as a pattern that can be applied to multiple servers.

XClarity Orchestrator does not directly deploy configuration patterns to managed servers. Instead, it sends a request to the applicable resource manager to start a job to perform the deployment, and then tracks the progress of the request.

For more information about provisioning server configurations, see [Provisioning server configurations](#).

Provisioning operating systems

You can use XClarity Orchestrator to deploy operating-system images to multiple servers.

XClarity Orchestrator does not directly deploy operating system to managed servers. Instead, it sends a request to the applicable XClarity Administrator resource manager to start a job to perform the update, and then tracks the progress of the request.

Note: The OS deployment feature requires XClarity Administrator v4.0 or later.

For more information about provisioning server configurations, see [Provisioning operating systems](#).

Business intelligence machine learning and predictive analytics

XClarity Orchestrator can connect to third-party services (such as Splunk) for business intelligence machine learning and predictive analytics to:

- Collect and display trend data (such as processor and memory utilization, power consumption, temperature, unauthorized access, repeated and lost events, and mean time between processes like firmware updates and system reboots)
- Uses metric data to predict failures (such as repeated events and health reports)
- Create custom analytics reports based on existing data, including alerts, events, device inventory, and device metrics.
- Define custom alert rules that, when enabled, raise alerts when specific conditions exist in your environment.

Learn more:  [Analytics and predictive capabilities](#)

For more information about predictive analytics, see [Analyzing trends and predicting problems](#).

Service and support

XClarity Orchestrator can be set up to collect and send diagnostic files automatically to Lenovo Support using Call Home when certain serviceable events occur in managed resources. You can also manually collect diagnostic files, open a problem record, and send diagnostic files to the Lenovo Support Center.

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

Documentation

The online documentation is updated regularly in English. See the [XClarity Orchestrator online documentation](#) for the most current information and procedures.

The online documentation is available in the following languages.

- English (en)
- Simplified Chinese (zh_CN)
- Traditional Chinese (zh_TW)
- French (fr)
- German (de)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Brazilian Portuguese (pt_BR)
- Russian (ru)
- Spanish (es)
- Thai (th)

You can change the language of the online documentation in the following ways:

- Change the language setting in your web browser.
- Append `?lang={language_code}` to the end of URL. For example, to display the online documentation in Simplified Chinese, use the following URL.
`http://sysmgmt.lenovofiles.com/help/topic/lxco/lxco-welcome.html?lang=zh_CN`

Logging in to a local XClarity Orchestrator web interface

Log in to a local Lenovo XClarity Orchestrator web interface from a system that has network connectivity to XClarity Orchestrator virtual appliance.

Before you begin

Ensure that you are using one of the following supported web browsers. For more information, see [Supported hardware and software](#) in the XClarity Orchestrator online documentation..

- Chrome 80.0 or later
- Firefox ESR 68.6.0 or later
- Microsoft Edge 40.0 or late
- Safari 13.0.4 or later (running on macOS 10.13 or later)

Access to the web interface is through a secure connection. Ensure that you use **https**.

When using an LDAP user account, you can log in using the user name or `username@domain` (for example, `user1@company.com`).

XClarity Orchestrator automatically logs out user sessions that have been inactive for a certain amount of time and user sessions that have been open for a certain amount of time, regardless of activity. The following default values are set by XClarity Orchestrator.

- If you have not clicked or typed on the user interface for **30 minutes**, your user session is restricted to read-only operations. If you attempt to modify data, the user session is automatically logged out.
- If you have not actively viewed data for **1440 minutes** (24 hours), your user session is automatically logged out.
- After **24 hours**, user sessions are automatically logged out, regardless of user activity.

Procedure

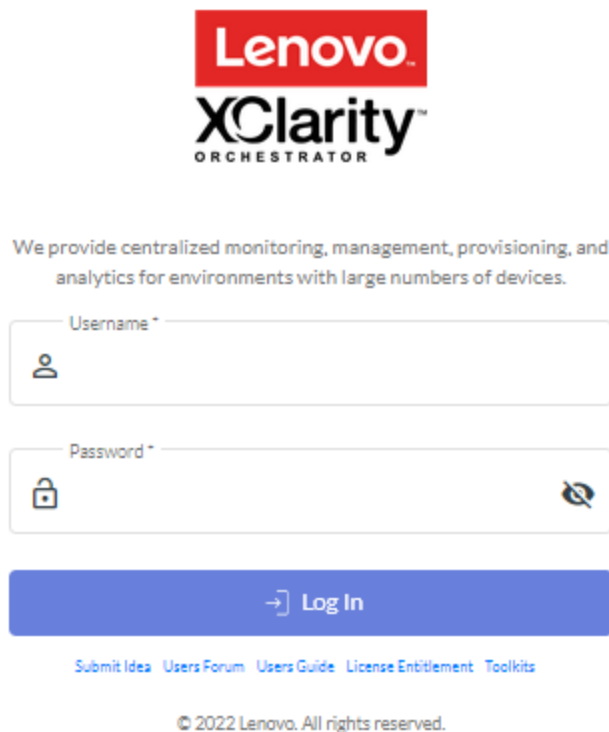
To log in to the XClarity Orchestrator web interface, complete the following steps.

1. Point your browser to the IP address of the XClarity Orchestrator virtual appliance.
 - **Using static an IPv4 address**If you specified an IPv4 address during installation, use that IPv4 address to access the web interface using the following URL.
`https://{IPv4_address}/#/login.html`

 For example:
`https://192.0.2.10/#/login.html`
 - **Using a DHCP server in the same broadcast domain as XClarity Orchestrator**If a DHCP server is set up in the same broadcast domain as XClarity Orchestrator, use the IPv4 address that is displayed in the XClarity Orchestrator virtual-appliance console to access the web interface using the following URL.
`https://{IPv4_address}/#/login.html`

 For example:
`https://192.0.2.10/#/login.html`

The initial login page is displayed.



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

- Submit ideas for XClarity Orchestrator on the [Lenovo XClarity Ideation website](#) or by clicking **Submit idea**.

- Ask questions and find answers on the [Lenovo XClarity Community forum website](#) by clicking **Users Forum**.
 - Find information about how to use XClarity Orchestrator by clicking **Users Guide**.
 - Find and manage all of your Lenovo licenses from the [Features on Demand web portal](#) by clicking **License Entitlement**.
 - Find information about the available APIs by clicking **Toolkits**.
2. Select the desired language from the language drop-down list.

Note: Some configuration settings and data that are provided by the resource managers and managed devices might be available only in English.

3. Enter a valid user ID and password, and click **Log In**. The first time that a specific user account is used to log in to XClarity Orchestrator, you are required to change the password. By default, passwords must contain **8 – 256** characters and must meet the following criteria.

Important: It is recommended that you use strong passwords of 16 or more characters.

- (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed)
- (2) Must contain at least one number
- (3) Must contain at least two of the following characters.
 - Uppercase alphabetic characters (A – Z)
 - Lowercase alphabetic characters (a – z)
 - Special characters ; @ _ ! ' \$ & +
 White space characters are not allowed.
- (4) Must not repeat or reverse the user name
- (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed)

After you finish

The XClarity Orchestrator dashboard is displayed with a summary of resource health and activities in your environment.

You can perform the following actions from the **User-Account** menu () in the upper-right corner of the XClarity Orchestrator web interface.

- Change the password of the current user by clicking **Change password**.
- Log out of the current session by clicking **Log out**. The XClarity Orchestrator log in page is displayed.

From the login page, you can click the **License Entitlement** link to open the [Features on Demand web portal](#), where you can find and manage all your Lenovo product licenses.

- Submit ideas for XClarity Orchestrator on the [Lenovo XClarity Ideation website](#) or by clicking **Submit idea**.
- Ask questions and find answers on the [Lenovo XClarity Community forum website](#) by clicking **Users Forum**.
- Download the XClarity Orchestrator PowerShell (LXCOPSTool) toolkit by clicking **Toolkits**. The LXCOPSTool toolkit provides a library of cmdlets to automate provisioning and resource management from a Microsoft PowerShell session.
- Find information about how to use XClarity Orchestrator using the embedded help system by clicking **Help**.

The online documentation is updated regularly in English. See the [XClarity Orchestrator online documentation](#) for the most current information and procedures.

- View information about the XClarity Orchestrator release by clicking **About**.

From the About dialog, you can find links to view the **End User License Agreement**, **Open Source Licenses**, and the **Lenovo Privacy Statement**.

- Change the language of the user interface by clicking **Change language**. The following languages are supported.
 - English (en)
 - Simplified Chinese (zh_CN)
 - Traditional Chinese (zh_TW)
 - French (fr)
 - German (de)
 - Italian (it)
 - Japanese (ja)
 - Korean (ko)
 - Brazilian Portuguese (pt_BR)
 - Russian (ru)
 - Spanish (es)
 - Thai (th)

User interface tips and techniques

Consider these tips and techniques when using the Lenovo XClarity Orchestrator and Lenovo XClarity Management Hub user interfaces.

Importing files

You can import files by dragging and dropping the files on an Import dialog.

When you import a file, an expandable popup appears on the lower-right corner of the user interface with information about the progress and status of each import process. Icons on the popup help you quickly identify the process status for each import. After an import completes successfully, a job is started to validate the file. If an error occurs during the import process, an error message is listed on the pop-up dialog to help you quickly resolve the issue.

When the popup is collapsed, you can click and hold the **Drag** icon (☰) to move the popup to a different position.

Click **Clear All** to clear the list of completed import processes. If all import processes are complete, the popup is hidden.

Entering text in text fields



The characters that can be entered in some text fields are restricted. The following list describes the characters that are allowed.

- **Names.** Includes all letters and numeric characters in supported languages and special characters @ - _ + / [] , . : and space.
- **Descriptions.** Includes all letters and numeric characters in supported languages and special characters @ - _ % & * + = / () { } [] . , : and space.
- **Passwords.** For local users accounts, passwords can be **8 – 256** characters by default, though 16 or more characters is recommended. There are no character restrictions for passwords. However, passwords require certain types of characters and restrict some sequences for security.
 - (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed)

- (2) Must contain at least one number
- (3) Must contain at least two of the following characters.
 - Uppercase alphabetic characters (A – Z)
 - Lowercase alphabetic characters (a – z)
 - Special characters ; @ _ ! ' \$ & +
 White space characters are not allowed.
- (4) Must not repeat or reverse the user name
- (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed)

Expanding and collapsing the navigation pane

The navigation pane is collapsed by default, showing only icons that represent specific menu items. You can click an icon to temporarily expand the navigation pane and the menu for that icon. When you move the cursor off the navigation pane, the pane collapses so that only the icons are displayed.

To keep the navigation pane permanently expanded, click the **Expand** icon () . You can then collapse the navigation pane by clicking the **Collapse** icon () .

Scoping the user interface

By default, XClarity Orchestrator displays data for *all resources*. You can narrow the scope of data displayed in the current user session to only those resources that are in specific resource managers and groups by using the **Current scope** drop-down menu at the top of the page. From the drop-down menu, you can view the list of resource managers and groups in the current scope under **My Scope List**, click **Change scope** to display a dialog on which you create a custom scope with multiple resource managers and groups, or select **All Resources** to change the scope to view all resources.

The selected scope is persistent only within the current user session. You can open multiple user sessions, each with different views of the dashboard, resources, events, and alerts data.

Note: VMware vRealize Operations Manager resource managers are not included in the list of resource managers, as they do not manage devices in XClarity Orchestrator.

Viewing more data or less data per page

Change the number of rows that are listed in a table per page using the **Rows per page** drop-down list at the bottom of each table. You can display 10, 15, 25 or 50 rows.

Finding data in large lists

There are several ways to display a subset of a large list based on specific criteria.


- Sort the table rows by clicking the column header.
- Narrow the scope of data in the current user session to only those resources that are in a specific resource manager or group by using the **Current scope** drop-down menu at the top of the page (see “Scoping the user interface” above).
- Dynamically create a subset of lists based on data that is found in specific columns by using the **Filters** input fields. You can filter on shown and hidden columns. You can also save filter queries that you want to use regularly.
- Further refine the subset by entering text (such as a name or IP address) in the **Search** field to find data that is found in any available column.

Tip: Separate multiple searches using a comma. For example, “180,190” displays all rows that contain 180 or 190 in any of the available columns.

- Select the checkbox in the table header to select or clear all items that are listed in the table.


Viewing table data

Refresh tables of data by clicking the **Refresh** icon ()

Expand or collapse each row to show or hide subdetails for the tables with expandable rows (such as on the Jobs and Repository Management cards). You can also click the **Collapse All** icon () to hide subdetails for all rows.

If the column size prevents some information from displaying in the table cell (indicated by an ellipsis), you can view the complete information in a popup by hovering over the cell.


Exporting table data

Export the data in the current table to your local system by clicking the **Export data** icon ()

You can choose to export all pages, the current page, or the selected rows, choose the file format (XLSX, CSV, or JSON), and choose whether to include all columns or only visible columns. For CSV format, you can also choose how to separate the data (using a semicolon, tab, or pipe character).

Tip: For JSON format, timestamps in the exported data reflect the time zone that is set for XClarity Orchestrator, not the local system. For CSV and XLSX formats, timestamps are converted to the user's time zone, which is displayed in the web interface.

When you export a data, an expandable popup appears on the lower-right corner of the user interface with information about the progress and status. Icons on the popup help you quickly identify the process status for each export. If an error occurs during the export process, an error message is listed on the pop-up dialog to help you quickly resolve the issue.

When the popup is collapsed, you can click and hold the **Drag** icon () to move the popup to a different position.

Click **Clear All** to clear the list of completed export processes. If all export processes are complete, the popup is hidden.


Configure table columns

Configure tables to show information that is most important to you.

- Choose which columns to show or hide by clicking **All Actions → Toggle Columns**.
- Reorder columns by dragging the column headers to the preferred location.

Changing the language of the user interface


You can change the language of the user interface when you first log in.

After you are logged in, you can change the language by clicking the **User-Account** menu () and then clicking **Change language**.

Note: The help system displays in the same language that is selected for the user interface.

Getting help

There are several ways to get help with the user interface.

- Hover the cursor over a **Help** icon () on some pages to display a pop-up with additional details about a specific field.

- Click the **Learn more** link on some pages to open the help system and get more information in context.
- Get help about how to perform specific actions from the user interface by clicking the **User-Account** menu (👤) and then click **Help**. The online documentation is updated regularly in English. See the [XClarity Orchestrator online documentation](#) for the most current information and procedures.

Chapter 2. Administering XClarity Orchestrator

Several administration activities are available, such as configuring system setting such as date and time and network access, connecting resource managers, managing authentication servers and user access, and managing security certificates.

Connecting resource managers

Lenovo XClarity Orchestrator monitors and manages devices through resource and application managers.

Before you begin

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

XClarity Orchestrator can support an unlimited number of resource managers that collectively manage a maximum of 10,000 devices.

Ensure that the resource managers are supported (see [Supported hardware and software](#) in the XClarity Orchestrator online documentation.).

Ensure that the resource managers are online and reachable on the network from XClarity Orchestrator.

Ensure that the user account that you use to authentication to the resource manager has the correct privileges. For XClarity Administrator, user accounts must be assigned to the **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-hw-admin** or **lxc-recovery** role.

Ensure that the resource manager does not have the maximum number of supported event forwarders. XClarity Orchestrator creates an event forwarder in the resource manager when a connection is created to that resource manager.

When connecting an XClarity Administrator that has an externally signed certificate:

- Ensure that it is an X.509 v3 certificate. XClarity Orchestrator cannot connect to an XClarity Administrator that has an externally signed v1 certificate.
- Ensure that the certificate details include the following requirements.
 - KeyUsage must contain
 - Key Agreement
 - Digital Signature
 - Key Encipherment
 - Enhanced Key Usage must contain
 - Server Authentication (1.3.6.1.5.5.7.3.1)
 - Client Authentication (1.3.6.1.5.5.7.3.2)

About this task

XClarity Orchestrator supports the following resource and application managers.

- **Lenovo XClarity Management Hub.** Manages, monitors, and provisions ThinkEdge Client devices. A UDC agent must be installed on each ThinkEdge Client device to allow communication between the device and XClarity Orchestrator.

Important: The registration process for Lenovo XClarity Management Hub is different than other resource managers. For detailed instructions, see [Connecting Management Hub to XClarity Orchestrator](#) in the XClarity Orchestrator online documentation..

- **Lenovo XClarity Administrator.** Manages, monitors, and provisions Lenovo devices with baseboard management controllers.
- **Schneider Electric EcoStruxure IT Expert.** Manages and monitors infrastructure resources.
- **VMware vRealize Operations Manager.**

When you connect a XClarity Management Hub or XClarity Administrator resource manager, XClarity Orchestrator:

- Retrieves information about all devices that are managed by the resource manager.
- Creates and enables an event forwarder (for a REST web service) in the management server to monitor and forward events to XClarity Orchestrator.

The network address (IP address or hostname) that you provide is used as the manager name.

Procedure

To connect a resource or application manager, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Resources** (🔗) → **Resource Managers** to display the Resource Managers card.

Resource Ma	Health Status	Type	Version	Build	Connected	Drive Analyt	Groups
XClarity...	🟢 No...	XClarity ...	2.0.0	279	Not Availal	Not Availal	Not Availal
host-10-...	🟢 No...	XClarity ...	3.6.0	108	2/16/23, 1	🔗 ⊕	Not Availal

- Step 2. Click the **Connect** icon (⊕) to display the resource manager. The Connect resource manager dialog.

Step 3. Select the type of resource manager, and fill in the required information.

- **XClarity Management Hub**

- Enter the registration key that was generated by the XClarity Management Hub instance, and then click **Connect**. To get the registration request token, log in to the XClarity Management Hub, click **Registration**, and then click **Create registration key**.
- Copy the generated XClarity Orchestrator registration key.
- From the XClarity Management Hub web interface, click **Registration**, and click **Install registration key**, paste the XClarity Orchestrator registration token in the XClarity Management Hub instance, and then click **Connect**.

- **XClarity Administrator**

- Specify the fully-qualified domain name or IP address (IPv4 or IPv6). Using the host name without the domain name is not supported.
- Optionally change the port of the resource manager. The default is 443.
- Specify the user account and password to use to log in to the resource manager.
- Optionally enable **Drive Analytics Data Collection**. When enabled, drive analytics data is collected daily for ThinkSystem and ThinkAgile devices and is used for predictive analytics. Drive analytics data collection is supported only for XClarity Administrator v3.3.0 and later resource managers.

Attention: System performance might be affected when data is collected.

- **EcoStruxure IT Expert**. Specify the name, token key, and URL to use for the connection.

- **vRealize Operations Manager**

- Specify the fully-qualified domain name or IP address (IPv4 or IPv6). Using the host name without the domain name is not supported.
- Optionally change the port of the resource manager. The default is 443.
- Optionally select the authorization source for the users and groups.

- Specify the user account and password to use to log in to vRealize Operations Manager.

Step 4. Click **Connect**.

A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

When a connection is established with the resource manager, the manager is added to the table.

Step 5. If you chose to connect to a XClarity Management Hub, a dialog is displayed with a registration key.

To complete the connection, Click **Copy to Clipboard** to copy the registration key. Then, log in to XClarity Management Hub, click **Administration → Hub Configuration**, and click **Install Registration Key**. Then, paste the registration key, and click **Submit**.

After you finish

You can perform the following actions from the Resource Managers card.

- View the connection status for the resource manager from the **Health Status** column.
- Modify credentials and properties for a selected resource manager by clicking the **Edit** icon (✎). A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)
- Enable or disable drive-analytics-data collection for a selected XClarity Administrator resource manager clicking the **Edit** icon (✎).

Note: The **Drive Analytics Data Collection** toggle is disabled when XClarity Administrator has connectivity or credentials issues (see [Sudden connectivity loss to a resource manager](#) in the XClarity Orchestrator online documentation).

- Disconnect and remove a selected resource manager by clicking the **Delete** icon (🗑️).

Note: If XClarity Orchestrator cannot connect to the resource manager (for example, if credentials are expired or if there are network issues), select **Force disconnect**.

A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

When the resource manager is removed, all devices that are managed by that resource manager are also removed. This includes device inventory, logs, metrics data, and analytic reports.

- Troubleshoot issues when connecting a resource manager (see [Cannot connect a resource manager](#) in the XClarity Orchestrator online documentation).

Discovering and managing devices

You can discover and manage devices using Lenovo XClarity Orchestrator and assign management of those devices to a specific resource manager.

Before you begin

To perform this task, you must be a member of a user group to which the predefined **Supervisor** or **Security Administrator** role is assigned.

About this task

XClarity Orchestrator monitors and manages devices through resource managers. When you connect a resource manager, XClarity Orchestrator manages all devices that are managed by that resource manager.

You can also bring devices into management using XClarity Orchestrator. XClarity Orchestrator lists devices that were already discovered (but not managed) by the resource managers. When you manage discovered devices from XClarity Orchestrator, the devices are managed by resource manager that discovered it. When you manually discover and manage devices using IP addresses, hostnames, or subnets, you choose which resource manager you want to use to manage the devices. XClarity Management Hub can be used to manage ThinkEdge Client devices. Lenovo XClarity Administrator can be used to manage servers, storage, switches, and chassis.

The following devices can be discovered automatically by resource managers using a service discovery protocol.

- ThinkSystem and ThinkAgile servers and appliances
- ThinkEdge Servers (SE350 and SE450)
- Flex System chassis, and ThinkSystem and Flex System devices in a Flex System chassis
- ThinkServer rack and tower servers
- System x, Converged HX, and NeXtScale servers and appliances
- Storage devices

The following devices *cannot* be discovered automatically by resource managers using a service discovery protocol. You must install the UDC agent on these devices before they can be securely discovered and managed.

- ThinkCentre Client
- ThinkEdge Clients

Currently, you cannot bring switches into management from XClarity Orchestrator. You also cannot unmanage Flex System switches from XClarity Orchestrator.

Device management considerations

Before you attempt to discover and manage devices using XClarity Orchestrator, review the following considerations.

- [General considerations](#)
- [Server considerations](#)
- [Storage considerations](#)
- [Switch considerations](#)
- [Chassis considerations](#)
- [Multiple management-tool considerations](#)

General considerations

Ensure that XClarity Orchestrator supports the devices that you want to manage. For information about supported devices, see .

Ensure that the minimum required firmware is installed on each system that you want to manage. For information about firmware requirements, see .

Certain ports must be available to communicate with devices. Ensure that all required ports are available before you attempt to manage servers. For information about ports, see .

XClarity Orchestrator can automatically discover devices in your environment by probing for manageable devices that are on the same IP subnet as XClarity Orchestrator using a service discovery protocol. To discover devices that are in other subnets, you can manually specify IP addresses, host names, range of IP addresses, or subnets.

After the devices are managed by XClarity Orchestrator, XClarity Orchestrator polls each managed storage device periodically to collect information, such as inventory, vital product data, and status.

If the XClarity Orchestrator loses communication with a device (for example, due to power loss or network failure or if the switch is offline) while collecting inventory during the management process, the management completes successfully; however, some inventory information might be incomplete. Either wait for the device to come online and for XClarity Orchestrator to poll the device for inventory or manually collect inventory on the device from the resource-manager web interface by selecting the device and clicking **All Actions → Inventory → Refresh inventory**.

Devices can be managed by only one resource manager (XClarity Orchestrator, XClarity Management Hub, or XClarity Administrator) at a time. If a device is managed by one resource manager, and you want to manage it using another resource manager, you must first unmanage the device from the original resource manager.

If you change the IP address of a device after the device is managed by XClarity Orchestrator recognizes the new IP address and continue to manage the server. However, XClarity Orchestrator does not recognize the IP address change for some servers. If XClarity Orchestrator shows that the server is offline after the IP address was changed, manage the server again using the **Force Management** option.

If you remove, replace, or configure any adapters in a device, restart the device at least once to update the inventory information.

To discover a device that is on a *different* subnet from the resource manager, ensure that one of the following conditions are met:

- Ensure multicast SLP forwarding is enabled on the rack switches and routers in your environment. See the documentation that was provided with your specific switch or router to determine whether multicast SLP forwarding is enabled and to find procedures to enable it if it is disabled.
- If SLP is disabled on the device or on the network, you can use DNS discovery method instead by manually adding a service record (SRV record) to your domain name server (DNS). For example:
`lxco.company.com service = 0 0 443 server1.company.com`
Then, enable DNS discovery on the baseboard management console from the management web interface, by clicking **BMC Configuration → Network**, clicking the **DNS** tab.

Encapsulation considerations

You can choose to enable encapsulation on the chassis and servers during the device management process. When the global encapsulation setting is enabled and the device supports encapsulation, the resource manager communicates with the device during the management process to change the device encapsulation mode to **encapsulationLite** and to change the firewall rules on the device to limit incoming requests to those from only the resource manager (Lenovo XClarity Management Hub or Lenovo XClarity Administrator).

Note: When the management network interface is configured to use the Dynamic Host Configuration Protocol (DHCP), managing devices with encapsulation enabled can take a long time.

The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to **normal** and the firewall rules are not changed during the device management process.

Attention: If the encapsulation mode is **encapsulationLite** on managed devices, the following situations might cause communication and authentication issues between the resource manager and managed devices, rendering the managed devices unreachable. Because the devices are configured to ignore TCP requests from other sources, it is not possible to access those devices through a network interface. In most cases, these devices do not respond to ping, SSH or TELNET requests.

- Network changes on the hypervisor in which the resource manager runs

- Virtual Local Area Networks (VLANs) or VLAN tags changes
- Permanent changes to device IP addresses while encapsulation is enabled
- Force-unmanagement of a device while encapsulation is enabled
- Loss of the resource manager virtual machine
- Loss of TCP communication between the virtual machine and the managed devices
- Other network issues that prevent the resource manager from communicating directly with managed devices while encapsulation mode is enabled

If a permanent problem occurs, complete one of the following actions to recover access to the previously managed devices. For more information, see [Encapsulation management](#), [Recovering management with a CMM after a management server failure](#), and [Recovering management with a CMM after a management server failure](#) in the Lenovo XClarity Administrator online documentation.

- To recover the access to a managed IMM where encapsulation mode is active, the default settings must be loaded from local console through UEFI graphical user interface.
- Use the USB-to-Ethernet bridge to gain in-band access to the management controller, and run the following command:

```
encaps lite -off
```
- To recover access to a managed CMM where encapsulation mode is active, the default settings must be loaded using the rear reset button or by running the following command if the console can still be reached:

```
accesscontrol -off -T mm[p]
```

Server considerations

Ensure that CIM over HTTPS is enabled on the device. Log in to the management web interface for the server using the `RECOVERY_ID` user account. Click **BMC Configuration** → **Security**, and then click **CIM Over HTTPS** tab, and ensure that **Enable CIM Over HTTPS** is selected.

When performing management actions on a server, ensure that the server is either powered off or powered on to the BIOS/UEFI Setup or to a running operating system (see [Performing power actions on managed servers](#).) If the server is powered on without an operating system, the management controller continuously resets the server in an attempt to find an operating system.

Ensure that all `UEFI_Ethernet_*` and `UEFI_Slot_*` settings are enabled in the server UEFI Settings. To verify the settings, restart the server, and when the prompt `<F1> Setup` is displayed, press **F1** to start the Setup utility. Navigate to **System Settings** → **Devices and I/O Ports** → **Enable / Disable Adapter Option ROM Support**, and then locate the **Enable / Disable UEFI Option ROMs** section to verify that the settings are enabled. If supported, you can also use the Remote Console feature in the baseboard management interface to review and modify the settings remotely.

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 Orchestrator trust store (see [Installing a trusted, externally-signed XClarity Orchestrator server certificate](#)).

ThinkEdge Client devices

ThinkEdge Client devices do not have baseboard management controllers and, therefore, are not discoverable using service discovery protocols. You must install a UDC agent on ThinkEdge Client devices before the devices can be securely discovered and managed by the assigned Lenovo XClarity Management Hubresource manager. For more information, see [Managing ThinkEdge Client devices](#).

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 Orchestrator 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 from ThinkSystem

System Manager web interface, click **Settings → IPMI Configuration**. You might need to restart the server to activate the change.

ThinkServer servers

The hostname of the server must be configured using a valid hostname or IP address to automatically discover these servers.

The network configuration must allow SLP traffic between XClarity Orchestrator and the server.

Unicast SLP is required.

To automatically discover ThinkServer servers, multicast SLP is required. In addition, SLP must be enabled on the ThinkServer System Manager (TSM).

If ThinkServer servers are on a different network than XClarity Orchestrator, ensure that the network is configured to allow inbound UDP through port 162 so that XClarity Orchestrator can receive events for those devices.

System x3950 X6 servers

These servers must be managed as two 4U enclosures, each with its own baseboard management controller.

For more information managing servers, see [Managing servers](#) and [Managing ThinkEdge Client devices](#).

Storage considerations

Ensure that the following requirements are met before discovering and managing rack storage devices (other than ThinkSystem DE series).

- The network configuration must allow SLP traffic between the resource manager and the rack storage device.
- Unicast SLP is required.
- Multicast SLP is required if you want XClarity Orchestrator to discover the Lenovo Storage devices automatically. In addition, SLP must be enabled on the rack storage device.

For more information managing storage devices, see [Managing storage devices](#).

Switch considerations

Managing rack switches using XClarity Orchestrator is not currently supported.

Chassis considerations

When you manage a chassis, all devices in the chassis are also managed. You cannot discover and managed components in the chassis independent of the chassis.

Ensure that the number of simultaneous active sessions for LDAP users setting in the CMM is set to 0 (zero) for the chassis. You can verify this setting from the CMM web interface by clicking **BMC Configuration → User Accounts**, click **Global Login Settings**, and then click the **General** tab.

Ensure that there are at least three TCP command-mode sessions set for out-of-band communication with the CMM. For information about setting the number of sessions, see [tcpcmdmode command in the CMM online documentation](#).

Consider implementing either IPv4 or IPv6 addresses for all CMMs and Flex System switches that are managed by XClarity Orchestrator. If you implement IPv4 for some CMMs and Flex switches and IPv6 for others, some events might not be received in the audit log (or as audit traps).

To discover a chassis that is on a *different* subnet from the resource manager, ensure that one of the following conditions are met:

- Ensure multicast SLP forwarding is enabled on the rack switches and routers in your environment. See the documentation that was provided with your specific switch or router to determine whether multicast SLP forwarding is enabled and to find procedures to enable it if it is disabled.
- If SLP is disabled on the device or on the network, you can use DNS discovery method instead by manually adding a service record (SRV record) to your domain name server (DNS). For example:
lxco.company.com service = 0 0 443 cmm1.company.com
Then, enable DNS discovery on the baseboard management console from the management web interface, by clicking **BMC Configuration** → **Network** , clicking the **DNS** tab.

For more information managing chassis, see [Managing chassis](#).

Multiple management-tool considerations

Extra care must be taken when using multiple management tools to manage your devices to prevent unforeseen conflicts. For example, submitting power-state changes using another tool might conflict with configuration or update jobs that are running in XClarity Orchestrator.

ThinkSystem, ThinkServer and System x devices

If you intend to use another management software to monitor your managed devices, create a new local user with the correct SNMP or IPMI settings from the baseboard management controller interface. Ensure that you grant SNMP or IPMI privileges, depending on your needs.

Flex System devices

If you intend to use another management software to monitor your managed devices, and if that management software uses SNMPv3 or IPMI communication, you must prepare your environment by performing the following steps for each managed CMM.

1. Log in to the management controller web interface for the chassis using the RECOVERY_ID user name and password.
2. If the security policy is set to **Secure**, change the user authentication method.
 - a. Click **BMC Configuration** → **User Accounts**.
 - b. Click the **Accounts** tab.
 - c. Click **Global login** settings.
 - d. Click the **General** tab.
 - e. Select **External first, then local authentication** for the user authentication method.
 - f. Click **OK**.
3. Create a new local user with the correct SNMP or IPMI settings from the management controller web interface.
4. If the security policy is set to **Secure**, log out and then log in to the management controller web interface using the new user name and password. When prompted, change the password for the new user.

Configuring global discovery settings

Choose the preferred settings to use when discovering devices.

Procedure

- Step 1. From the XClarity Orchestrator menu bar, click **Resources** (⚙️) → **New Devices** to display the Discover and manage new devices card.
- Step 2. Click the ⚙️ **Configuration** to display the Discovery settings dialog.
- Step 3. Select the preferred discovery settings.

- **SLP Discovery** Indicates whether to automatically discover devices using the service location protocol (SLP).

When enabled, XClarity Orchestrator attempts to discover new devices every 15 minutes and at every user login.

Note: The SLP Discovery setting that you choose in XClarity Orchestrator overrides any SLP discovery setting chosen for Lenovo XClarity Administrator instances that are managed by XClarity Orchestrator. If the SLP Discovery setting is changed in Lenovo XClarity Administrator, it will be synchronized with XClarity Orchestrator.

- **Encapsulation on all future managed devices** Indicates whether encapsulation is enabled during device management.

Encapsulation is disabled by default. When disabled, the device encapsulation mode is set to **normal** and the firewall rules are not changed as part of the management process.

When encapsulation is enabled and a device supports encapsulation, XClarity Orchestrator communicates with the device (through the resource manager) during the management process to change the device encapsulation mode to **encapsulationLite** and to change the firewall rules on the device to limit incoming requests to those only from the resource manager that was chosen to manage the device.

Attention: If encapsulation is enabled and the resource manager that was chosen to manage the device becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with that device.

- **Register request enabled** Indicates whether resource managers (Lenovo XClarity Administrator and Lenovo XClarity Management Hub) accept discovery requests from a baseboard management controller when the management controller uses DNS to find resource-manager instances. When enabled, the management controller can register with resource manager as a discovered device.
- **Offline devices cleanup.** Indicates whether to automatically unmanage devices that are offline for at least the amount of time specified by **Offline devices timeout**. When enabled, XClarity Orchestrator checks for offline devices every hour and each time a user logs in to the portal.
- **Offline devices timeout** Amount of time, in hours, that devices must be offline before they are automatically unmanaged. This value can be from **1 – 24** hours. The default is **24** hours.

Step 4. Click **Save**.

Managing servers

You can use Lenovo XClarity Orchestrator manage several types of servers.

Before you begin

To perform this task, you must be a member of a user group to which the predefined **Supervisor** or **Security Administrator** role is assigned.

Review the management considerations before managing a device (see [Device management considerations](#)).

Review the global discovery settings before managing a device (see [Configuring global discovery settings](#)).

To discover and manage edge devices that do not respond to service discovery protocol, see [Managing ThinkEdge Client devices](#).

About this task

XClarity Orchestrator monitors and manages devices through resource managers. When you connect a resource manager, XClarity Orchestrator manages all devices that are managed by that resource manager.

You can also bring devices into management using XClarity Orchestrator. XClarity Orchestrator lists devices that were already discovered (but not managed) by the resource managers. When you manage discovered devices from XClarity Orchestrator, the devices are managed by resource manager that discovered it. When you manually discover and manage devices using IP addresses, hostnames, or subnets, you choose which resource manager you want to use to manage the devices. XClarity Management Hub can be used to manage ThinkEdge Client devices. Lenovo XClarity Administrator can be used to manage servers, storage, switches, and chassis.

The following servers can be discovered automatically by resource managers using a service discovery protocol.

- ThinkSystem and ThinkAgile servers and appliances
- ThinkEdge Servers (SE350 and SE450)
- Flex System chassis, and ThinkSystem and Flex System devices in a Flex System chassis
- ThinkServer rack and tower servers
- System x, Converged HX, and NeXtScale servers and appliances
- Storage devices

Procedure

To manage your servers, complete one of the following procedures.

- **Manage discovered servers**To manage devices that were automatically discovered, complete the following steps.
 1. From the XClarity Orchestrator menu bar, click **Resources** (🔍) → **New Devices** to display the Discover and manage new devices card.

Discover and manage new devices

Click **Configuration** to define global discovery settings.

Click **UDS Portal Credentials** to set the UDS Portal credentials that are needed to download UDC provisioning packages for devices that do not respond to a service discovery protocol.

If the following list does not contain the device that you expect, use the **Manual Input** option to discover the device. For more information about why a device might not be automatically discovered, see the following help topic: [Cannot discover a device.](#)

⊕ Manual Input ⚙️ Configuration ⊖ UDS Portal Credentials

New Devices

🔄 ⊕ 📄 All Actions ▾ Filters ▾ 🔍 Search ✕

<input type="checkbox"/>	Discovered Device	IP Addresses	Serial Number	Type-Model	Type	Discovered By
<input type="checkbox"/>	G8052-1	10.241.5.1, 10:	Y010CM345...	7309/HC1 (G...	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (G...	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 10	1234567890	7D75/CTO1...	Server	10.241.5.134

0 Selected / 3 Total Rows per page: 10 ▾

2. Click the **All Actions** → **Refresh** to discover all manageable devices in the XClarity Orchestrator domain. Discovery might take several minutes.
3. Select one or more servers that you want to manage.
4. Click the **Manage** icon (⊕) to display the Manage Discovered Devices dialog.
5. Review the list of selected devices to manage, and click **Next**.
6. Specify the username and password for authenticating to the server.

Tip: Consider using a supervisor or administrator account to manage the device. If an account with lower-level authority is used, management might fail, or management might succeed but some features might fail.

7. **Optional:** Select **Create a recovery account and disable all local users**, and then specify the recovery password. When disabled, local user accounts are used for authentication.

When enabled, the assigned resource manager creates a managed-authentication user account and a recovery account (RECOVERY_ID) on the server, and all other local user accounts are disabled. The managed-authentication user account is used to by XClarity Orchestrator and the resource manager for authentication. If there is a problem with XClarity Orchestrator or resource manager, and it stops working for any reason, you *cannot* log in to the baseboard management controller using normal user accounts. However, you can log in using the RECOVERY_ID account.

Important: Ensure that you record the recovery password for future use.

Note: The recovery account is not supported for ThinkServer and System x M4 servers.

8. **Optional:** Enable **Set new password if credentials are expired**, and then specify the new server password. If the current server password has expired, discovery will fail until the password is changed. If you specify a new password, the credentials are changed and the management process can continue. The password is changed only if the current password is expired.
9. Select **Manage**. A job is created to complete the management process in the background. You can monitor the status of the management process from the dialog or from the jobs log by clicking **Monitoring** (📧) → **Jobs** (see [Monitoring jobs](#)).

If management was not successful due to one of the following error conditions, repeat this procedure using the Force management option.

- The resource manager failed and cannot be recovered.

Note: If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

- The resource manager was taken down before the devices were unmanaged.
- Devices were not unmanaged successfully.
- XClarity Orchestrator show a managed device as offline after the device's IP address was changed.

- **Manually discover and manage servers** To manually discover and then manage specific servers, complete the following steps.

1. From the XClarity Orchestrator menu bar, click **Resources** (📧) → **New Devices** to display the Discover and manage new devices card.
2. Click **Manual Input** to display the Discover New Devices dialog.
3. Select **Devices that respond to service discovery protocol**, and then click **Next**.
4. Select **Manual**, and then click **Next**.
5. Choose how you want to discover the devices and then specify the appropriate values.

- **IP Addresses/Hostnames**
 - **IP ranges**
 - **Subnets**
6. Select the Lenovo XClarity Administrator resource manager that you want to use to manage the devices
 7. Click **Discover devices**.
 8. Specify the username and password for authenticating to the server.

Tip: Consider using a supervisor or administrator account to manage the device. If an account with lower-level authority is used, management might fail, or management might succeed but some features might fail.

9. **Optional:** Select **Create a recovery account and disable all local users**, and then specify the recovery password. When disabled, local user accounts are used for authentication.

When enabled, the assigned resource manager creates a managed-authentication user account and a recovery account (RECOVERY_ID) on the server, and all other local user accounts are disabled. The managed-authentication user account is used to by XClarity Orchestrator and the resource manager for authentication. If there is a problem with XClarity Orchestrator or resource manager, and it stops working for any reason, you *cannot* log in to the baseboard management controller using normal user accounts. However, you can log in using the RECOVERY_ID account.

Important: Ensure that you record the recovery password for future use.

Note: The recovery account is not supported for ThinkServer and System x M4 servers.

10. **Optional:** Enable **Set new password if credentials are expired**, and then specify the new server password. If the current server password has expired, discovery will fail until the password is changed. If you specify a new password, the credentials are changed and the management process can continue. The password is changed only if the current password is expired.
11. Select **Manage**. A job is created to complete the management process in the background. You can monitor the status of the management process from the dialog or from the jobs log by clicking **Monitoring** (📊) → **Jobs** (see [Monitoring jobs](#)).

If management was not successful due to one of the following error conditions, repeat this procedure using the Force management option.

- The resource manager failed and cannot be recovered.

Note: If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

- The resource manager was taken down before the devices were unmanaged.
- Devices were not unmanaged successfully.
- XClarity Orchestrator show a managed device as offline after the device's IP address was changed.

After you finish

You can perform the following actions on the managed device.

- Monitor device status and details (see [Viewing devices status](#) and [Viewing device details](#)).
- Unmanage and remove a selected device by clicking click **Resources** (📁) and then click the device type in the left navigation to display a card with a tabular view of all managed devices of that type, select the devices to unmanage, and then click the **Unmanage** icon (🗑️).

Notes:

- Ensure that there are no active jobs running on the device.
- If XClarity Orchestrator cannot connect to the resource manager (for example, if credentials are expired or if there are network issues), select **Force unmanage even if the device is not reachable**.
- For most devices, XClarity Orchestrator and the resource manager retain certain information about the device after it is unmanaged. That information is reapplied when you manage the same device again.
- XClarity Orchestrator automatically unmanage devices that are offline for a 24 hours or more by default (see [Configuring global discovery settings](#)).
- Troubleshoot issues when connecting a resource manager (see and).

Managing ThinkEdge Client devices

ThinkEdge Client devices, do not have baseboard management controllers and, therefore, are not discoverable using service discovery protocols. You must install a Universal Device Client (UDC) agent on ThinkEdge Client devices before the devices can be securely discovered and managed by the assigned Lenovo XClarity Management Hub resource manager. Only Lenovo XClarity Management Hub resource managers can discover and manage these devices.

Before you begin

Review the management considerations before managing a device (see [Device management considerations](#)).

Ensure that at least one Lenovo XClarity Management Hub resource manager is connected to XClarity Orchestrator (see [Connecting resource managers](#)).

To perform this task, you must be a member of a user group to which the predefined **Supervisor** or **Security Administrator** role is assigned.

Ensure that the UDS Portal credentials are configured. The credentials are used to sign the policy that is used in the client provisioning package. The UDS Portal is the trusted source for signing this policy for the UDC agent to work correctly. To configure the credentials, click **Resources** (🔗) → **New Devices** from the menu bar, click **UDS Portal Credentials**, and then enter the client ID and secret. You must request the client ID and secret from Lenovo by sending an email to uedmcredreq@lenovo.com, using “UDS Portal Credentials” in the email description, and include your company name, contact information (email or phone number), and 10-digit Lenovo Customer Number.

Ensure that a UDC agent *is not* currently installed on the ThinkEdge Client device. If a UDC agent is installed, you must uninstall it by running the following commands. You must have elevated privileges to install the UDC agent.

- **Linux**
`sudo apt purge udc-release`
- **Windows**
`PUSHD %windir%\System32\drivers\Lenovo\udc\Data\InfBackup\.\UDCInfInstaller.exe -uninstall`

`POPD`

Ensure that your DNS server is configured to include the following domains, where *(hub-domain)* is the fully-qualified domain name of the XClarity Management Hub resource manager that you want to use to manage the ThinkEdge Client devices.

- `api.(hub-domain)`
- `api-mtls.(hub-domain)`
- `auth.(hub-domain)`

- `mqtt.(hub-domain)`
- `mqtt-mtls.(hub-domain)`
- `s3.(hub-domain)`
- `s3console.(hub-domain)`

About this task

XClarity Orchestrator monitors and manages devices through resource managers. When you connect a resource manager, XClarity Orchestrator manages all devices that are managed by that resource manager.

You can also bring devices into management using XClarity Orchestrator. XClarity Orchestrator lists devices that were already discovered (but not managed) by the resource managers. When you manage discovered devices from XClarity Orchestrator, the devices are managed by resource manager that discovered it. When you manually discover and manage devices using IP addresses, hostnames, or subnets, you choose which resource manager you want to use to manage the devices. XClarity Management Hub can be used to manage ThinkEdge Client devices. Lenovo XClarity Administrator can be used to manage servers, storage, switches, and chassis.

You can find a complete list of supported ThinkEdge Client devices from the [Lenovo XClarity Support website](#) by clicking the **Compatibility** tab and then clicking the link for the appropriate device types.

Note: ThinkEdge Servers (such as SE350, SE360, and SE450) have baseboard management controllers and can be discovered using a service discovery protocol. To manage these devices, see [Managing servers](#).

Procedure

To discover and manage ThinkEdge Client devices, complete the following steps.

1. Install the UDC agent on each ThinkEdge Client device.
 - a. From the XClarity Orchestrator menu bar, click **Resources** (🔗) → **New Devices** to display the Discover and manage new devices card.
 - b. Click **Manual Input** to display the Discover New Devices dialog.
 - c. Select **Devices that do not respond to service discovery protocol**, and then click **Next**.
 - d. Select the IP address of the XClarity Management Hub resource manager that you want to use to manage the ThinkEdge Client devices. Only XClarity Management Hub resource managers in a healthy state can be selected.
 - e. Select the type of operating system that is installed on the server.
 - **Linux ARM**
 - **Linux x86**
 - **Windows**
 - f. Select the number of days before the UDC agent installer becomes unusable after it is downloaded. The default is **30** days.
 - g. Select the number of times that you plan to install the UDC agent on a server. This is typically the number of devices on which you need to install the UDC agent. You can specify up to **1,000,000** usages; the default is **10** usages.
 - h. Click **Download UDC Agent** to download the UDC agent installer to your local system. A job is created to complete the download process in the background. You can monitor the status of the download process from the dialog or from the jobs log by clicking **Monitoring** (📧) → **Jobs** (see [Monitoring jobs](#)).
 - i. Click **Close** to close the dialog.

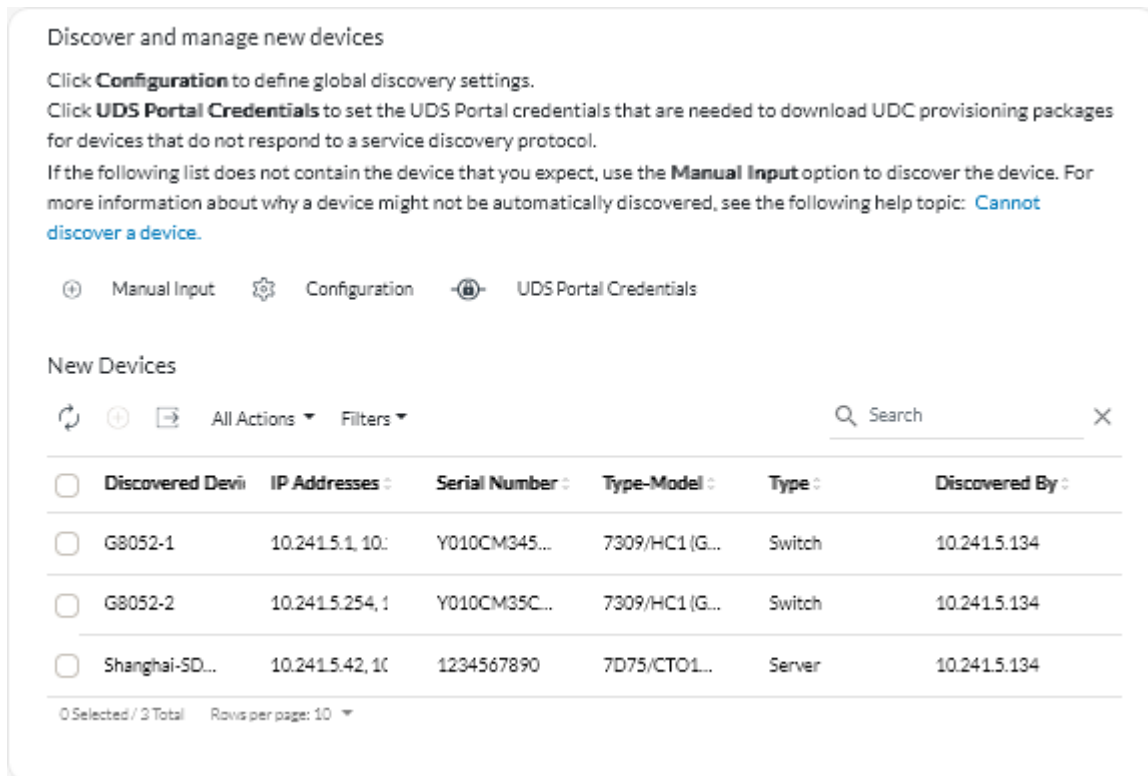
- j. Copy the UDC agent installer to each appropriate ThinkEdge Client device, unpack/unzip the package, and then install the UDC agent on those devices using the following command. You must have **administrator** privileges to install the agent.
 - **Linux** `install.sh`
 - **Windows** `setup.cmd`

After the UDC agent is successfully installed on each ThinkEdge Client device, the devices can be discovered automatically by the selected XClarity Management Hub resource manager.

2. Manage the ThinkEdge Client devices.

- a. From the XClarity Orchestrator menu bar, click **Resources** (⚙️) → **New Devices** to display the Discover and manage new devices card.

Note: It might take a while for IP addresses to appear in the table.



- b. Click the **All Actions** → **Refresh** to discover all manageable devices in the XClarity Orchestrator domain. Discovery might take several minutes.
- c. Select one or more ThinkEdge Client devices that you want to manage.
- d. Click the **Manage** icon (⊕) to display the Manage Discovered Devices dialog.
- e. Review the list of selected devices to manage.
- f. Select **Manage**. A job is created to complete the management process in the background. You can monitor the status of the management process from the dialog or from the jobs log by clicking **Monitoring** (📄) → **Jobs** (see [Monitoring jobs](#)).

If management was not successful due to one of the following error conditions, repeat this procedure using the Force management option.



- The resource manager failed and cannot be recovered.

Note: If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the `RECOVERY_ID` account and password (if applicable) and the **Force management** option.

- The resource manager was taken down before the devices were unmanaged.
- Devices were not unmanaged successfully.
- XClarity Orchestrator show a managed device as offline after the device's IP address was changed.

After you finish

You can perform the following actions on the managed device.

- Monitor device status and details (see [Viewing devices status](#) and [Viewing device details](#)).
- Unmanage and remove a selected device by clicking click **Resources**  and then click the device type in the left navigation to display a card with a tabular view of all managed devices of that type, select the devices to unmanage, and then click the **Unmanage** icon .

Notes:

- Ensure that there are no active jobs running on the device.
 - If XClarity Orchestrator cannot connect to the resource manager (for example, if credentials are expired or if there are network issues), select **Force unmanage even if the device is not reachable**.
 - For most devices, XClarity Orchestrator and the resource manager retain certain information about the device after it is unmanaged. That information is reapplied when you manage the same device again.
 - XClarity Orchestrator automatically unmanage devices that are offline for a 24 hours or more by default (see [Configuring global discovery settings](#)).
- Troubleshoot issues when connecting a resource manager (see and).

Managing storage devices

Lenovo XClarity Orchestrator can manage several types of Lenovo storage appliances, devices, and tape libraries.

Before you begin

To perform this task, you must be a member of a user group to which the predefined **Supervisor** or **Security Administrator** role is assigned.

Review the management considerations before managing a device (see [Device management considerations](#)).

To discover and manage edge devices that do not respond to service discovery protocol, see [Managing ThinkEdge Client devices](#).

About this task

XClarity Orchestrator monitors and manages devices through resource managers. When you connect a resource manager, XClarity Orchestrator manages all devices that are managed by that resource manager.

You can also bring devices into management using XClarity Orchestrator. XClarity Orchestrator lists devices that were already discovered (but not managed) by the resource managers. When you manage discovered devices from XClarity Orchestrator, the devices are managed by resource manager that discovered it. When you manually discover and manage devices using IP addresses, hostnames, or subnets, you choose which

resource manager you want to use to manage the devices. XClarity Management Hub can be used to manage ThinkEdge Client devices. Lenovo XClarity Administrator can be used to manage servers, storage, switches, and chassis.

Procedure

To manage your storage devices, complete one of the following procedures.

- **Manage discovered devices** To manage devices that were automatically discovered, complete the following steps.
 1. From the XClarity Orchestrator menu bar, click **Resources** (🔍) → **New Devices** to display the Discover and manage new devices card.

Discover and manage new devices

Click **Configuration** to define global discovery settings.
 Click **UDS Portal Credentials** to set the UDS Portal credentials that are needed to download UDC provisioning packages for devices that do not respond to a service discovery protocol.
 If the following list does not contain the device that you expect, use the **Manual Input** option to discover the device. For more information about why a device might not be automatically discovered, see the following help topic: [Cannot discover a device.](#)

Manual Input
 Configuration
 UDS Portal Credentials

New Devices

 All Actions ▾
 Filters ▾
 Search
 X

<input type="checkbox"/>	Discovered Device	IP Addresses	Serial Number	Type-Model	Type	Discovered By
<input type="checkbox"/>	G8052-1	10.241.5.1, 10:	Y010CM345...	7309/HC1 (G...	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (G...	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 10	1234567890	7D75/CTO1...	Server	10.241.5.134

0 Selected / 3 Total Rows per page: 10 ▾

2. Click the **All Actions** → **Refresh** to discover all manageable devices in the XClarity Orchestrator domain. Discovery might take several minutes.
3. Select one or more storage devices that you want to manage.
4. Click the **Manage** icon (⊕) to display the Manage Discovered Devices dialog.
5. Review the list of selected devices to manage, and click **Next**.
6. Specify the username and password for authenticating to the server.

Tip: Consider using a supervisor or administrator account to manage the device. If an account with lower-level authority is used, management might fail, or management might succeed but some features might fail.

7. Select **Manage**. A job is created to complete the management process in the background. You can monitor the status of the management process from the dialog or from the jobs log by clicking **Monitoring** (📧) → **Jobs** (see [Monitoring jobs](#)).

If management was not successful due to one of the following error conditions, repeat this procedure using the Force management option.

- The resource manager failed and cannot be recovered.

Note: If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the `RECOVERY_ID` account and password (if applicable) and the **Force management** option.

- The resource manager was taken down before the devices were unmanaged.
- Devices were not unmanaged successfully.
- XClarity Orchestrator show a managed device as offline after the device's IP address was changed.

- **Manually discover and manage devices** To manually discover and then manage specific storage devices, complete the following steps.

1. From the XClarity Orchestrator menu bar, click **Resources** (🔍) → **New Devices** to display the Discover and manage new devices card.
2. Click **Manual Input** to display the Discover New Devices dialog.
3. Select **Devices that respond to service discovery protocol**, and then click **Next**.
4. Select **Manual**, and then click **Next**.
5. Choose how you want to discover the devices and then specify the appropriate values.
 - **IP Addresses/Hostnames**
 - **IP ranges**
 - **Subnets**
6. Select the Lenovo XClarity Administrator resource manager that you want to use to manage the devices
7. Click **Discover devices**.
8. Specify the username and password for authenticating to the server.

Tip: Consider using a supervisor or administrator account to manage the device. If an account with lower-level authority is used, management might fail, or management might succeed but some features might fail.

9. Select **Manage**. A job is created to complete the management process in the background. You can monitor the status of the management process from the dialog or from the jobs log by clicking **Monitoring** (📄) → **Jobs** (see [Monitoring jobs](#)).

If management was not successful due to one of the following error conditions, repeat this procedure using the Force management option.

- The resource manager failed and cannot be recovered.

Note: If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the `RECOVERY_ID` account and password (if applicable) and the **Force management** option.

- The resource manager was taken down before the devices were unmanaged.
- Devices were not unmanaged successfully.
- XClarity Orchestrator show a managed device as offline after the device's IP address was changed.

After you finish

You can perform the following actions on the managed device.

- Monitor device status and details (see [Viewing devices status](#) and [Viewing device details](#)).
- Unmanage and remove a selected device by clicking **Resources** (🔍) and then click the device type in the left navigation to display a card with a tabular view of all managed devices of that type, select the devices to unmanage, and then click the **Unmanage** icon (🗑️).

Notes:

- Ensure that there are no active jobs running on the device.
 - If XClarity Orchestrator cannot connect to the resource manager (for example, if credentials are expired or if there are network issues), select **Force unmanage even if the device is not reachable**.
 - For most devices, XClarity Orchestrator and the resource manager retain certain information about the device after it is unmanaged. That information is reapplied when you manage the same device again.
 - XClarity Orchestrator automatically unmanage devices that are offline for a 24 hours or more by default (see [Configuring global discovery settings](#)).
- Troubleshoot issues when connecting a resource manager (see [and](#)).

Managing chassis

Lenovo XClarity Orchestrator can manage several types of chassis and chassis components.

Before you begin

To perform this task, you must be a member of a user group to which the predefined **Supervisor** or **Security Administrator** role is assigned.

Review the management considerations before managing a device (see [Device management considerations](#)).

To discover and manage edge devices that do not respond to service discovery protocol, see [Managing ThinkEdge Client devices](#).

About this task

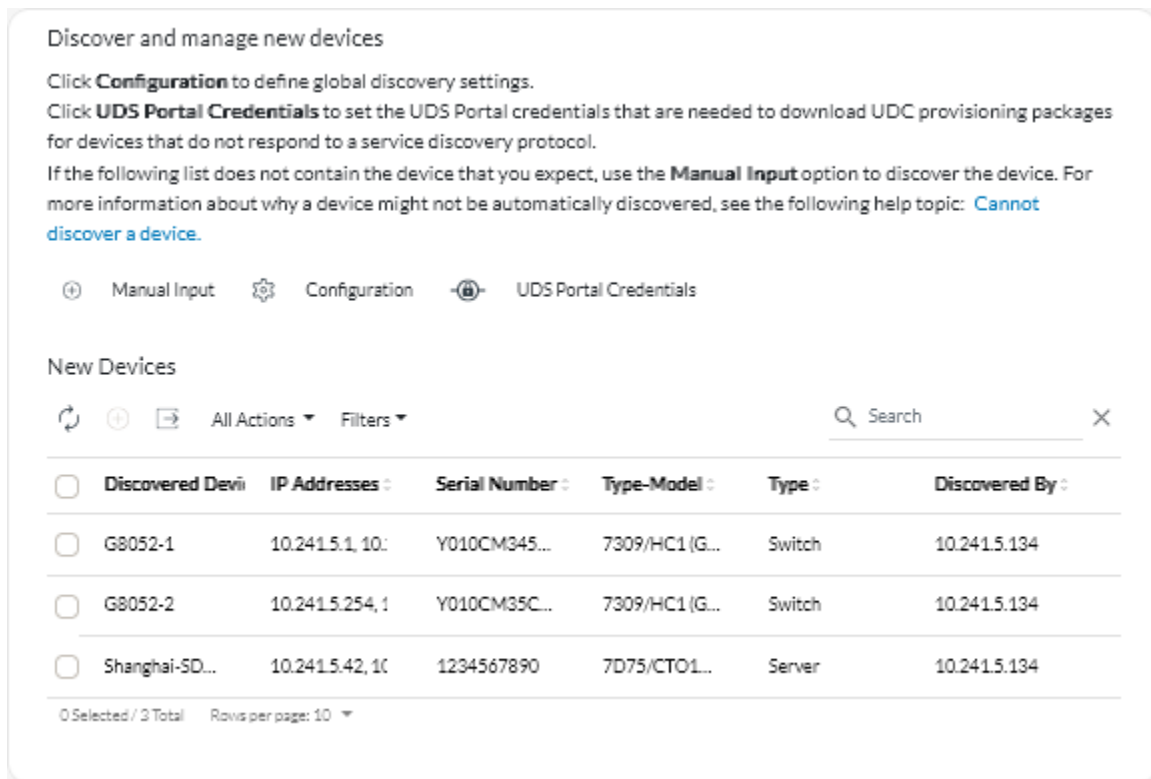
XClarity Orchestrator monitors and manages devices through resource managers. When you connect a resource manager, XClarity Orchestrator manages all devices that are managed by that resource manager.

You can also bring devices into management using XClarity Orchestrator. XClarity Orchestrator lists devices that were already discovered (but not managed) by the resource managers. When you manage discovered devices from XClarity Orchestrator, the devices are managed by resource manager that discovered it. When you manually discover and manage devices using IP addresses, hostnames, or subnets, you choose which resource manager you want to use to manage the devices. XClarity Management Hub can be used to manage ThinkEdge Client devices. Lenovo XClarity Administrator can be used to manage servers, storage, switches, and chassis.

Procedure

To manage your chassis, complete one of the following procedures.

- **Manage discovered devices** To manage devices that were automatically discovered, complete the following steps.
 1. From the XClarity Orchestrator menu bar, click **Resources** (🔍) → **New Devices** to display the Discover and manage new devices card.



2. Click the **All Actions** → **Refresh** to discover all manageable devices in the XClarity Orchestrator domain. Discovery might take several minutes.
3. Select one or more chassis that you want to manage.
4. Click the **Manage** icon (+) to display the Manage Discovered Devices dialog.
5. Review the list of selected devices to manage, and click **Next**.
6. Specify the username and password for authenticating to the server.

Tip: Consider using a supervisor or administrator account to manage the device. If an account with lower-level authority is used, management might fail, or management might succeed but some features might fail.

7. **Optional:** Select **Create a recovery account and disable all local users**, and then specify the recovery password. When disabled, local user accounts are used for authentication.

When enabled, the assigned resource manager creates a managed-authentication user account and a recovery account (RECOVERY_ID) on the server, and all other local user accounts are disabled. The managed-authentication user account is used to by XClarity Orchestrator and the resource manager for authentication. If there is a problem with XClarity Orchestrator or resource manager, and it stops working for any reason, you *cannot* log in to the baseboard management controller using normal user accounts. However, you can log in using the RECOVERY_ID account.

Important: Ensure that you record the recovery password for future use.

Note: The recovery account is not supported for ThinkServer and System x M4 servers.

8. **Optional:** Enable **Set new password if credentials are expired**, and then specify the new server password. If the current server password has expired, discovery will fail until the password is changed. If you specify a new password, the credentials are changed and the management process can continue. The password is changed only if the current password is expired.

9. Select **Manage**. A job is created to complete the management process in the background. You can monitor the status of the management process from the dialog or from the jobs log by clicking **Monitoring** (📄) → **Jobs** (see [Monitoring jobs](#)).

If management was not successful due to one of the following error conditions, repeat this procedure using the Force management option.

- The resource manager failed and cannot be recovered.

Note: If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

- The resource manager was taken down before the devices were unmanaged.
- Devices were not unmanaged successfully.
- XClarity Orchestrator show a managed device as offline after the device's IP address was changed.

- **Manually discover and manage devices** To manually discover and then manage specific chassis, complete the following steps.

1. From the XClarity Orchestrator menu bar, click **Resources** (🔍) → **New Devices** to display the Discover and manage new devices card.
2. Click **Manual Input** to display the Discover New Devices dialog.
3. Select **Devices that respond to service discovery protocol**, and then click **Next**.
4. Select **Manual**, and then click **Next**.
5. Choose how you want to discover the devices and then specify the appropriate values.
 - **IP Addresses/Hostnames**
 - **IP ranges**
 - **Subnets**
6. Select the Lenovo XClarity Administrator resource manager that you want to use to manage the devices
7. Click **Discover devices**.
8. Specify the username and password for authenticating to the server.

Tip: Consider using a supervisor or administrator account to manage the device. If an account with lower-level authority is used, management might fail, or management might succeed but some features might fail.

9. **Optional:** Select **Create a recovery account and disable all local users**, and then specify the recovery password. When disabled, local user accounts are used for authentication.

When enabled, the assigned resource manager creates a managed-authentication user account and a recovery account (RECOVERY_ID) on the server, and all other local user accounts are disabled. The managed-authentication user account is used to by XClarity Orchestrator and the resource manager for authentication. If there is a problem with XClarity Orchestrator or resource manager, and it stops working for any reason, you *cannot* log in to the baseboard management controller using normal user accounts. However, you can log in using the RECOVERY_ID account.

Important: Ensure that you record the recovery password for future use.

Note: The recovery account is not supported for ThinkServer and System x M4 servers.

10. **Optional:** Enable **Set new password if credentials are expired**, and then specify the new server password. If the current server password has expired, discovery will fail until the password is changed. If you specify a new password, the credentials are changed and the management process can continue. The password is changed only if the current password is expired.

11. Select **Manage**. A job is created to complete the management process in the background. You can monitor the status of the management process from the dialog or from the jobs log by clicking **Monitoring** (📊) → **Jobs** (see [Monitoring jobs](#)).

If management was not successful due to one of the following error conditions, repeat this procedure using the Force management option.

- The resource manager failed and cannot be recovered.

Note: If the replacement resource manager instance uses the same IP address as the failed resource manager, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

- The resource manager was taken down before the devices were unmanaged.
- Devices were not unmanaged successfully.
- XClarity Orchestrator show a managed device as offline after the device's IP address was changed.

After you finish

You can perform the following actions on the managed device.

- Monitor device status and details (see [Viewing devices status](#) and [Viewing device details](#)).
- Unmanage and remove a selected device by clicking click **Resources** (📁) and then click the device type in the left navigation to display a card with a tabular view of all managed devices of that type, select the devices to unmanage, and then click the **Unmanage** icon (🗑️).

Notes:

- Ensure that there are no active jobs running on the device.
 - If XClarity Orchestrator cannot connect to the resource manager (for example, if credentials are expired or if there are network issues), select **Force unmanage even if the device is not reachable**.
 - For most devices, XClarity Orchestrator and the resource manager retain certain information about the device after it is unmanaged. That information is reapplied when you manage the same device again.
 - XClarity Orchestrator automatically unmanage devices that are offline for a 24 hours or more by default (see [Configuring global discovery settings](#)).
- Troubleshoot issues when connecting a resource manager (see and).

Using VMwareTools

The VMware Tools package is installed in the virtual machine's guest operating system when you install Lenovo XClarity Orchestrator in VMware ESXi-based environments. This package provides a subset of the VMware tools that support optimized virtual-appliance backup and migration while preserving application state and continuity.

For information about using the VMware Tools, see [Using the VMware Tools Configuration Utility in the VMware vSphere Documentation Center website](#).

Configuring network settings

You can configure a single network interface (using IPv4 and IPv6 settings), Internet routing settings, and proxy settings.

Learn more:  [How to configure networks and set up NTP servers](#)

Before you begin

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

Review the following considerations when choosing the interface.

- The interface must be configured to support discovery and management. It must be able to communicate with the resource managers and the devices that they manage.
- If you intend to manually send collected service data to Lenovo Support or use automatic problem notification (Call Home), the interfaces must be connected to the Internet, preferably through a firewall.

Attention:

- If you change the XClarity Orchestrator virtual-appliance IP address after connecting resource managers, XClarity Orchestrator will lose communication with the managers, and the managers will appear offline. If you need to change the virtual-appliance IP address after XClarity Orchestrator is up and running, ensure that all resource managers are disconnected (deleted) before changing the IP address.
- If the network interface is configured to use the Dynamic Host Configuration Protocol (DHCP), the IP address might change when the DHCP lease expires. If the IP address changes, you must disconnect (delete) the resource managers, and then connect them again. To avoid this problem, either change the network interface to a static IP address, or ensure that the DHCP server is configured such that the DHCP address is based on a MAC address or that the DHCP lease does not expire.
- Network address translation (NAT), which remaps one IP address space into another, is not supported.

Procedure

To configure network settings, click **Administration**  → **Networking** from the XClarity Orchestrator menu bar, and then complete one or more of the following steps.

- **Configure IP settings** You can choose to use IPv4 and IPv6 network settings from the IPv4 Configuration and IPv6 Configuration cards. Enable and modify the applicable IP configuration settings, and then click **Apply**.
 - **IPv4 settings.** You can configure the IP assignment method, IPv4 address, network mask, and default gateway. For the IP assignment method, you can choose to use a statically-assigned IP address or obtain an IP address from a DHCP server. When using a static IP address, you must provide an IP address, network mask, and default gateway. The default gateway must be a valid IP address and must be on the same subnet as network interface.

If DHCP is used to obtain an IP address, the default gateway also uses DHCP.
 - **IPv6 settings.** You can configure the IP assignment method, IPv6 address, prefix length, and default gateway. For the IP assignment method, you can choose to use a statically assigned IP address, stateful address configuration (DHCPv6), or a stateless address auto configuration. When using a static IP address, you must provide an IPv6 address, prefix length and gateway. The gateway must be a valid IP address and must be on the same subnet as network interface.

IPv4 Configuration

Enabled

Method Obtain IP from DHCP	IPv4 Network Mask 255.255.224.0
IPv4 Address 10.243.14.36	IPv4 Default Gateway 10.243.0.1

IPv6 Configuration

Enabled

Method Use stateless address...	IPv6 Prefix Length 64
IPv6 Address fd55:faaf:e1ab:2021:20c:2	IPv6 Default Gateway fe80::5:73ff:fea0:2c

- **Configure Internet routing settings** Optionally configure Domain Name System (DNS) settings from the DNS Configuration card. Then, click **Apply**.

Currently, only IPv4 addresses are supported.

Choose whether to use DHCP to obtain the IP addresses or to specify static IP addresses by enabling or disabling **DHCP DNS**. If you choose to use static IP addresses, specify the IP address for at least one and up to two DNS servers.

Specify the DNS host name and domain name. You can choose to retrieve the domain name from a DHCP server or specify a custom domain name.

Notes:

- If you choose to use a DHCP server to obtain the IP address, any changes that you make to the DNS Server fields are overwritten the next time XClarity Orchestrator renews the DHCP lease.
- When you change any DNS settings, you must manually restart the virtual machine to apply the changes.
- If you change the DNS setting from using from DHCP to a static IP address, ensure that you also change the IP address of the DNS server itself.

DNS Configuration

Preferred DNS address type IPv4 IPv6

Enabled

1st DNS Address: 10.240.0.10

2nd DNS Address: 10.240.0.11

Method: Use domain name o...

Domain Name:

Hostname: lxco

Apply Reset

- **Configure HTTP proxy settings** Optionally enable and specify the proxy server host name, port, and optional credentials from the Proxy Configuration card. Then, click **Apply**.

Notes:

- Ensure that the proxy server is set up to use basic authentication.
- Ensure that the proxy server is set up as a non-terminating proxy.
- Ensure that the proxy server is set up as a forwarding proxy.
- Ensure that load balancers are configured to keep sessions with one proxy server and not switch between them.

Proxy Configuration

Disabled

Proxy Server Host Name

Proxy Server Port

User Name

Password

Apply Reset

Configuring the date and time

You must set up at least one (and up to four) Network Time Protocol (NTP) server to synchronize the timestamps for Lenovo XClarity Orchestrator with events that are received from resource managers.

Before you begin

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

Each NTP server must be accessible over the network. Consider setting up the NTP server on the local system where XClarity Orchestrator is running.

If you change the time on the NTP server, it might take a while for XClarity Orchestrator to synchronize with the new time.

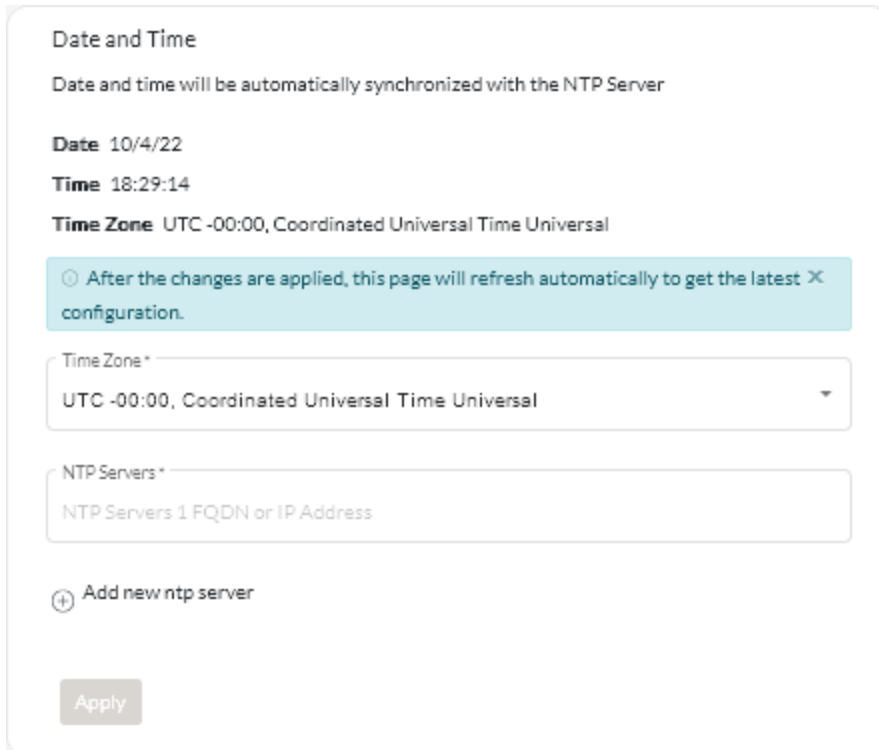
Attention: The XClarity Orchestrator virtual appliance and its host must be set to synchronize to the same time source to prevent inadvertent time mis-synchronization between XClarity Orchestrator and its host. Typically, the host is configured to have its virtual appliances time-sync to it. If XClarity Orchestrator is set to synchronize to a different source than its host, you must disable the host time synchronization between XClarity Orchestrator virtual appliance and its host.

- **ESXi** Follow instructions on the [VMware – Disabling Time Synchronization webpage](#).
- **Hyper-V** From Hyper-V Manager, right-click the XClarity Orchestrator virtual machine, and then click **Settings**. In the dialog, click **Management** → **Integration Services** in the navigation pane, and then clear **Time synchronization**.

Procedure

To set the date and time for XClarity Orchestrator, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Date and Time** to display the Date and Time card.



The screenshot shows the 'Date and Time' configuration page. At the top, it states 'Date and time will be automatically synchronized with the NTP Server'. Below this, the current 'Date' is 10/4/22 and the 'Time' is 18:29:14. The 'Time Zone' is set to 'UTC -00:00, Coordinated Universal Time Universal'. A light blue notification box contains the text: 'After the changes are applied, this page will refresh automatically to get the latest X configuration.' Below the notification, there is a 'Time Zone*' dropdown menu currently showing 'UTC -00:00, Coordinated Universal Time Universal'. Underneath is an 'NTP Servers*' input field with the placeholder text 'NTP Servers 1 FQDN or IP Address'. A plus icon and the text 'Add new ntp server' are located below the input field. At the bottom left of the card is an 'Apply' button.

- Step 2. Choose the time zone where the host for XClarity Orchestrator is located.

If the selected time zone observes daylight saving time (DST), the time is automatically adjusted for DST.

- Step 3. Specify the hostname or IP address for each NTP server within your network. You can define up to four NTP servers.

- Step 4. Click **Apply**.

Working with security certificates

Lenovo XClarity Orchestrator uses SSL certificates to establish secure, trusted communications between XClarity Orchestrator and its managed resource managers (such as Lenovo XClarity Administrator or Schneider Electric EcoStruxure IT Expert) as well as communications with XClarity Orchestrator by users or with different services. By default, XClarity Orchestrator and Lenovo XClarity Administrator use XClarity Orchestrator-generated certificates that are self-signed and issued by an internal certificate authority.

Before you begin

This section is intended for administrators that have a basic understanding of the SSL standard and SSL certificates, including what they are and how to manage them. For general information about public key certificates, see [X.509 webpage in Wikipedia](#) and [Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile \(RFC5280\) webpage](#).

About this task

The default server certificate, which is uniquely generated in every instance of XClarity Orchestrator, provides sufficient security for many environments. You can choose to let XClarity Orchestrator manage certificates for you, or you can take a more active role by customizing and replacing the server certificates. XClarity Orchestrator provides options for customizing certificates for your environment. For example, you can choose to:

- Generate a new pair of keys by regenerating the internal certificate authority and/or the end server certificate that uses values that are specific to your organization.
- Generate a certificate signing request (CSR) that can be sent to your choice of certificate authority to sign a custom certificate that can then be uploaded to XClarity Orchestrator to be used as end-server certificate for all its hosted services.
- Download the server certificate to your local system so that you can import that certificate into your web browser's list of trusted certificates.

XClarity Orchestrator provides several services that accept incoming SSL/TLS connections. When a client, such as a web browser, connects to one of these services, XClarity Orchestrator provides its *server certificate* to be identified by the client attempting the connection. The client should maintain a list of certificates that it trusts. If XClarity Orchestrator server certificate is not included in the client's list, the client disconnects from XClarity Orchestrator to avoid exchanging any security sensitive information with an untrusted source.

XClarity Orchestrator acts as a client when communicating with resource managers and external services. When this occurs, the resource manager or external service provides its server certificate to be verified by XClarity Orchestrator. XClarity Orchestrator maintains a list of certificates that it trusts. If the *trusted certificate* that is provided by the resource manager or external service is not listed, XClarity Orchestrator disconnects from the managed device or external service to avoid exchanging any security sensitive information with an untrusted source.

The following category of certificates is used by XClarity Orchestrator services and are supposed to be trusted by any client connecting to it.

- **Server Certificate.** During the initial boot, a unique key and self-signed certificate are generated. These are used as the default Root Certificate Authority, which can be managed on the Certificate Authority page in the XClarity Orchestrator security settings. It is not necessary to regenerate this root certificate unless the key has been compromised or if your organization has a policy that all certificates must be replaced periodically (see [Regenerating the internally-signed XClarity Orchestrator server certificate](#)). Also during the initial setup, a separate key is generated and a sever certificate is created and signed by the internal

certificate authority. This certificate used as the default XClarity Orchestrator server certificate. It automatically regenerated each time XClarity Orchestrator detects that its networking addresses (IP or DNS addresses) have changed to ensure that the certificate contains the correct addresses for the server. It can be customized and generated on demand (see [Regenerating the internally-signed XClarity Orchestrator server certificate](#)).

You can choose to use an externally-signed server certificate instead of the default self-signed server certificate by generating a certificate signing request (CSR), having the CSR signed by an private or commercial certificate Root Certificate Authority, and then importing the full certificate chain into XClarity Orchestrator (see [Installing a trusted, externally-signed XClarity Orchestrator server certificate](#)

If you choose to use the default self-signed server certificate, it is recommended that you import the server certificate in your web browser as a trusted root authority to avoid certificate error messages in your browser (see [Importing the server certificate into a web browser](#)

The following category (trust stores) of certificates are used by XClarity Orchestrator clients.

- **Trusted Certificates** This trust store manages certificates that are used to establish a secure connection to local resources when XClarity Orchestrator acts as a client. Examples of local resources are managed Resource Managers, local software when forwarding event etc.
- **External-Services Certificates.** This trust store manages certificates that are used to establish a secure connection with external services when XClarity Orchestrator acts as a client. Examples of external services are online Lenovo Support services that are used to retrieve warranty information or create service tickets, external software (such as Splunk) to which events can be forwarded. It contains preconfigured, trusted certificates from Root Certificate Authorities from certain commonly trusted and world-known certificate-authority providers, such as Digicert and Globalsign). When you configure XClarity Orchestrator to use a feature that requires a connection to another external service, refer to the documentation to determine if you need to manually add a certificate to this trust store.

Note that certificates in this trust store are not trusted when establishing connections for other services (such as LDAP) unless you also add them to the main Trusted Certificates trust store. Removing certificates from this trust store prevents successful operation of these services.

Adding a trusted certificate for external services


These certificates are used to establish trust relationships with external services. For example, certificates in this truststore are used when retrieving warranty information from Lenovo, creating tickets, forwarding events to an external application (such as Splunk), and using external LDAP servers.

Before you begin

Certificates in this trust store are not trusted when establishing connections for other services unless you also add them to the main trusted-certificates truststore. Removing certificates from this truststore prevents successful operation of these services.






Procedure

To add a trusted certificate, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Administration**  → **Security**, and then click **External Services Certificates** in the left navigation to display the Trusted Certificates for External Services card.

Trusted Certificates for External Services

Manage certificates that are used to establish trust relationships with external services, for example, when retrieving warranty information from Lenovo, creating tickets, forwarding events to external software, and using external LDAP servers.






 All Actions ▾ Filters ▾ Q Search X

	Subject DN :	Issuer DN :	Not Before :	Not After :	Status :
<input type="radio"/>	C = US, O = DigiC...	C = US, O = DigiC...	Nov 9, 2006, 7:00...	Nov 9, 2031, 7:00...	Active
<input type="radio"/>	OU = GlobalSign...	OU = GlobalSign...	Mar 18, 2009, 6:0...	Mar 18, 2029, 6:0...	Active
<input type="radio"/>	CN = Motorola R...	CN = Motorola R...	Jan 28, 2015, 9:5...	Jan 28, 2035, 10:...	Active
<input type="radio"/>	C = US, ST = Illino...	C = BE, O = Globa...	Nov 14, 2019, 8:5...	Jan 27, 2022, 3:0...	Expired

0 Selected / 4 Total Rows per page: 10 ▾

Step 2. Click the **Add** icon (+) to add a certificate. The Add Certificate dialog is displayed.

Step 3. Copy and paste the certificate data in PEM format.

Step 4. Click **Add**.

After you finish

You can perform the following actions from the Trusted Certificates for External Services card.

- View details of a selected trusted certificate by clicking the **View** icon (🔍).
- Save a selected trusted certificate to the local system by clicking the **View** icon (🔍), and then clicking **Save as pem**.
- Delete a selected trusted certificate by clicking the **Delete** icon (🗑).

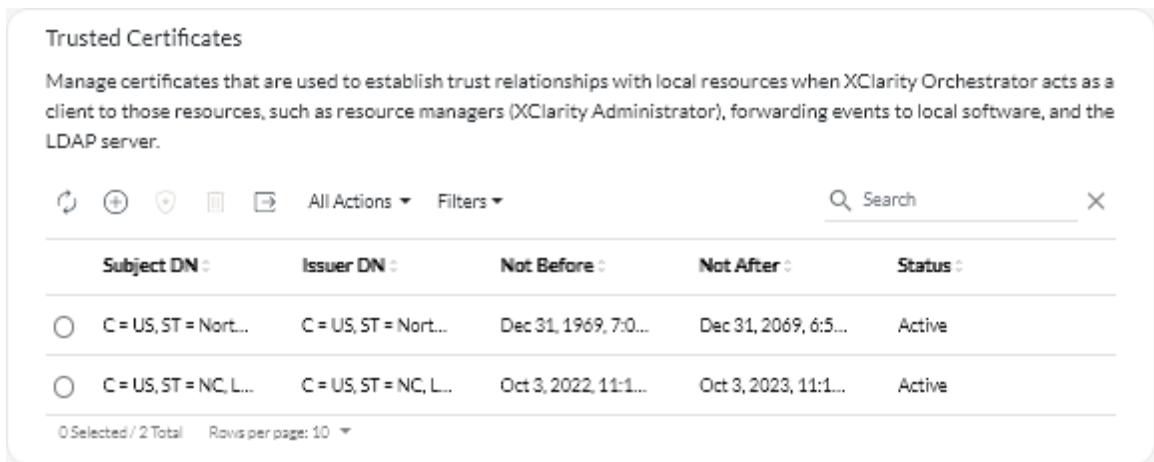
Adding a trusted certificate for internal services

These certificates are used to establish trust relationships with local resources when Lenovo XClarity Orchestrator acts as a client to those resources, such as resource managers, forwarding events to local software, and the embedded LDAP server. Additionally, the internal CA certificate as well as the CA certificate of a customized externally-signed server certificate (if one is installed) are present in this truststore to support internal XClarity Orchestrator communication.

Procedure

To add a trusted certificate, complete the following steps.

Step 1. From the XClarity Orchestrator menu bar, click **Administration** (⚙) → **Security**, and then click **Trusted Certificates** in the left navigation to display the Trusted Certificate card.



- Step 2. Click the **Add** icon (+) to add a certificate. The Add Certificate dialog is displayed.
- Step 3. Copy and paste the certificate data in PEM format.
- Step 4. Click **Add**.

After you finish

You can perform the following actions from the Trusted Certificate card.

- View details of a selected trusted certificate by clicking the **View** icon (*).
- Save a selected trusted certificate to the local system by clicking the **View** icon (*), and then clicking **Save as pem**.
- Delete a selected trusted certificate by clicking the **Delete** icon (III).

Installing a trusted, externally-signed XClarity Orchestrator server certificate

You can choose to use a trusted server certificate that was signed by a private or commercial certificate authority (CA). To use an externally-signed server certificate, generate a certificate signing request (CSR), and then import the resulting server certificate to replace the existing server certificate.

About this task

As a best practice, always use v3 signed certificates.

The externally-signed server certificate must be created from the Certificate Signing Request that was most recently generated using the **Generate CSR File** button.

The externally-signed server certificate content must be a certificate bundle that contains the entire CA signing chain, including the CA's root certificate, any intermediate certificates, and the server certificate.

If the new server certificate was not signed by a trusted third party, the next time that you connect to XClarity Orchestrator, your web browser displays a security message and dialog prompting you to accept the new certificate into the browser. To avoid the security messages, you can import the server certificate into your web browser's list of trusted certificates (see [Importing the server certificate into a web browser](#)).

XClarity Orchestrator begins using the new server certificate without terminating the current session. New sessions are established using the new certificate. To use the new certificate in use, restart your web browser.

Important: When the server certificate is modified, all established user sessions must accept the new certificate by clicking Ctrl+F5 to refresh the web browser and then re-establish their connection to XClarity Orchestrator.

Procedure

To generate and install an externally-signed server certificate, complete the following steps.

Step 1. Create a certificate signing request and save the file to your local system.

1. From the XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Security**, and then click **Server Certificate** in the left navigation to display the Generate Certificate Signing Request card.

Generate Certificate Signing Request (CSR)

Create and save a Certificate Signing Request using user provided values.

Country/Region*
UNITED STATES

Organization*
Lenovo

State/Province*
NC

Organization Unit*
DCG

City*
Raleigh

Common Name*
Generated by Lenovo Management Ecosystem

Subject Alternative Names ⓘ

To add a new Subject Alternative Name, click (+)

Generate CSR File Import Certificate

2. From the Generate Certificate Signing Request (CSR) card, fill in the fields for the request.
 - Two-letter ISO 3166 code for the country or region of origin associated with the certificate organization (for example, US for the United States).
 - Full name of the state or province to be associated with the certificate (for example, California or New Brunswick).
 - Full name of the city to be associated with the certificate (for example, San Jose). The length of the value cannot exceed 50 characters.
 - Organization (company) that is to own the certificate. Typically, this is the legal incorporate name of a company. It should include any suffixes, such as Ltd., Inc., or Corp (for example, ACME International Ltd.). The length of this value cannot exceed 60 characters.
 - (Optional) Organization unit that is to own the certificate (for example, ABC Division). The length of this value cannot exceed 60 characters,
 - Common name of the certificate owner. This must be the hostname of the server that is using the certificate. The length of this value cannot exceed 63 characters.
 - (Optional) Subject alternative names that are added to the X.509 "subjectAltName" extension when the CSR is generated. By default, XClarity Orchestrator automatically defines subject alternative names for the CSR based on the IP address and hostname that are discovered by the network interfaces for the XClarity Orchestrator guest operating system. You can customize, delete, or add to these subject alternative name values.

However, the subject alternative names must have the fully-qualified domain name (FQDN) or IP address of the server, and the subject name be set to the FQDN.

The name that you specify must be valid for the selected type.

- **DNS** (use the FQDN, for example, hostname.labs.company.com)
- **IP address** (for example, 192.0.2.0)
- **email** (for example, example@company.com)

Note: All subject alternative names that are listed in the table are validated, saved, and added to the CSR only after you generate the CSR in the next step.

- Step 2. Provide the CSR to a trusted certificate authority (CA). The CA signs the CSR and returns a server certificate.
- Step 3. Import the externally-signed server certificate and the CA certificate to XClarity Orchestrator, and replace the current server certificate.
 1. From the Generate Certificate Signing Request (CSR) card, click **Import Certificate** to display the Import Certificate dialog.
 2. Copy and paste the server certificate and CA certificate in PEM format. You must provide the entire certificate chain, beginning with the server certificate and ending in the root CA certificate.
 3. Click **Import** to store the server certificate in the XClarity Orchestrator trust store.
- Step 4. Accept the new certificate by pressing Ctrl+F5 to refresh the browser and then re-establishing your connection to the web interface. This must be done by all established user sessions.

Regenerating the internally-signed XClarity Orchestrator server certificate

You can generate a new server certificate to replace the current internally-signed Lenovo XClarity Orchestrator server certificate or to reinstate an XClarity Orchestrator-generated certificate if XClarity Orchestrator currently uses a customized externally-signed server certificate. The new internally-signed server certificate is used by XClarity Orchestrator for HTTPS access.

About this task

The server certificate that is currently in use, whether internally-signed or externally-signed, remains in use until a new server certificate is regenerated and signed.

Important: When the server certificate is modified, all established user sessions must accept the new certificate by clicking Ctrl+F5 to refresh the web browser and then re-establish their connection to XClarity Orchestrator.

Procedure

To generate an internally-signed XClarity Orchestrator server certificate, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Security**, and then click **Server Certificate** in the left navigation to display the Regenerate Server Certificate card.

Regenerate Server Certificate

Generate a new key and certificate using the provided certificate data.

Country/Region* UNITED STATES	Organization* Lenovo
State/Province* NC	Organization Unit* DCG
City* Raleigh	Common Name* Generated by Lenovo Management Ecosystem
Not Valid Before Date Oct/3/2022 13:21	Not Valid After Date* Sep/30/2032 13:21

Regenerate Certificate
Save Certificate
Reset Certificate

Step 2. From the Regenerate Server Certificate card, fill in the fields for the request.

- Two-letter ISO 3166 code for the country or region of origin to associate with the certificate organization (for example, US for the United States)
- Full name of the state or province to associate with the certificate (for example, California or New Brunswick)
- Full name of the city to associate with the certificate (for example, San Jose). The length of the value cannot exceed 50 characters.
- Organization (company) to own the certificate. Typically, this is the legally incorporated name of a company. It should include any suffixes, such as Ltd., Inc., or Corp (for example, ACME International Ltd.). The length of this value cannot exceed 60 characters.
- (Optional) Organization unit to own the certificate (for example, ABC Division). The length of this value cannot exceed 60 characters.
- Common name of the certificate owner. Typically, this is the fully-qualified domain name (FQDN) or IP address of the server that uses the certificate (for example, www.domainname.com or 192.0.2.0). The length of this value cannot exceed 63 characters.
- Date and time when the server certificate is no longer valid.

Note: You cannot change the subject alternative names when regenerating the server certificate.

Step 3. Click **Regenerate Certificate** to regenerate the internally-signed certificate, and then click **Regenerate Certificate** to confirm.

Step 4. Accept the new certificate by pressing Ctrl+F5 to refresh the browser and then re-establishing your connection to the web interface. This must be done by all established user sessions.

After you finish

You can perform the following actions from the Regenerate Server Certificate card.

- Save the current server certificate to your local system in PEM format by clicking **Save Certificate**.
- Regenerate the server certificate using default setting by clicking **Reset Certificate**. When prompted, press Ctrl+F5 to refresh the browser, and then re-establish your connection to the web interface.

Importing the server certificate into a web browser

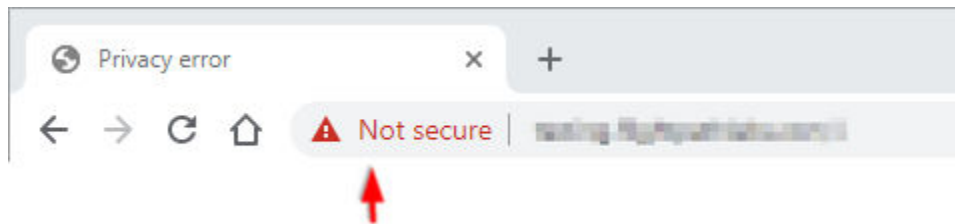
You can save a copy of the current server certificate, in PEM format, to your local system. You can then import the certificate into your web browser's list of trusted certificates or to other applications (such as Lenovo XClarity Mobile or Lenovo XClarity Integrator) to avoid security warning messages from your web browser when you access Lenovo XClarity Orchestrator.

Procedure

To import the server certificate into a web browser, complete the following steps.

• Chrome

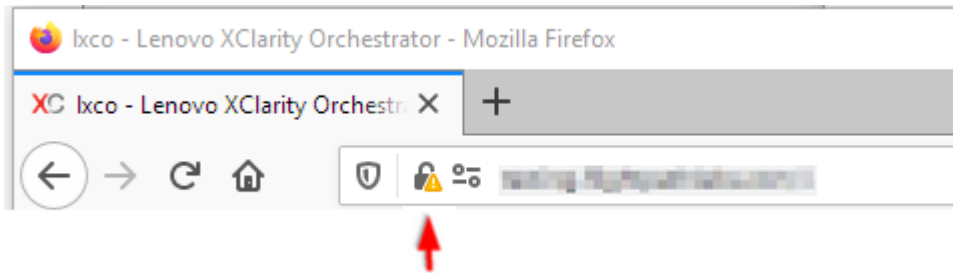
1. Export the XClarity Orchestrator server certificate.
 - a. Click the “Not secure” warning icon in the top address bar, for example:



- b. Click **Certificate (invalid)** to display the Certificate dialog.
 - c. Click the **Details** tab.
 - d. Click **Copy to File** to display the Certificate Export Wizard.
 - e. Select **Cryptographic Message Syntax Standard**, and click **Next**.
 - f. Specify the name and location of the certificate file, and then **Finish** to export the certificate.
 - g. Click **OK** to close the Certificate dialog.
2. Import the XClarity Orchestrator server certificate into the list of trusted root authority certificates for your browser.
 - a. From your Chrome browser, click the three dots in the upper right corner of the window, and then, click **Settings**.
 - b. Scroll to the **Privacy and Security** section, and click **Manage certificates** to display the Certificates dialog.
 - c. Click **Import**, and select the certificate file that you previous exported, and click **Next**.
 - d. Click **Browse** next to **Certificate store**, and select **Trusted Root Certification Authorities**. Then, click **OK**.
 - e. Click **Finish**.
 - f. Close and reopen the Chrome browser, and then open XClarity Orchestrator.

• Firefox

1. Export the XClarity Orchestrator server certificate.
 - a. Click the “Not secure” warning icon in the top address bar, for example:



- b. Expand Connection Not Secured, and then click More Information to display a dialog.
 - c. Click **View certificates**.
 - d. Scroll down to the Download section, and click the **PEM (cert)** link.
 - e. Select **Save File**, and click **OK**.
2. Import the XClarity Orchestrator server certificate into the list of trusted root authority certificates for your browser.
 - a. Open the browser, and click **Tools → Options → Advanced**.
 - b. Click the **Certificates** tab.
 - c. Click **View certificates**.
 - d. Click **Import**, and browse to the location where the certificate was downloaded.
 - e. Select the certificate, and click **Open**.

Managing authentication

You can choose to use the local Lightweight Directory Access Protocol (LDAP) server or another external LDAP server as the authentication server.

The *authentication server* is a user registry that is used to authenticate user credentials. Lenovo XClarity Orchestrator supports two types of authentication servers:

- **Local authentication server.** By default, XClarity Orchestrator is configured to use the local (embedded) LDAP server that resides in the orchestrator server.
- **External LDAP server.** Microsoft Active Directory is supported as an external LDAP server. This server must reside on an outboard Microsoft Windows server that is connected to the management network.

Setting up an external LDAP authentication server

Lenovo XClarity Orchestrator includes a local (embedded) authentication server. You can also choose to use your own external Active Directory LDAP server.

Before you begin

Ensure that all ports that are required for the external authentication server are open on the network and firewalls. For information about port requirements, see [Port availability](#) in the XClarity Orchestrator online documentation.

Only Microsoft Active Directory is supported as an external LDAP server.

XClarity Orchestrator does not automatically clone user groups that are defined in the external LDAP server; however, you can manually clone LDAP user group (see [Creating user groups](#)).

Before an external LDAP user can log in to XClarity Orchestrator, the user must be a direct member of an LDAP user group that is cloned in XClarity Orchestrator (see [Creating user groups](#)). XClarity Orchestrator does not recognize users that are members of user groups that are nested in the cloned LDAP user group defined in the external LDAP server.

About this task

If an external LDAP server is not configured, XClarity Orchestrator always authenticates a user using the local authentication server.

If an external LDAP server is configured, XClarity Orchestrator first attempts to authenticate a user using the local authentication server. If authentication fails, XClarity Orchestrator then attempts to authenticate using the IP address of the first LDAP server. If authentication fails, the LDAP client attempts to authenticate using the IP address of the next LDAP server.

When an external LDAP user logs in to XClarity Orchestrator for the first time, a user account with the name <username>@<domain> is automatically cloned in XClarity Orchestrator. You can add cloned external LDAP users to user groups or use LDAP groups for access control. You can also add supervisor privileges to an external LDAP user.

Procedure

To configure XClarity Orchestrator to use an external LDAP authentication server, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Security**, and then click **LDAP Client** in the left navigation to display the LDAP Client card.

LDAP Client ↻

You can configure XClarity Orchestrator to use external LDAP servers to authenticate users. The local authentication server always performs the authentication first. If authentication fails, the LDAP client attempts to authenticate using the first external LDAP server IP address. If authentication fails, the LDAP client attempts to authenticate using the next server IP address.

Server Information

Domain*

Server Address*

Port*
636

🗑️
⊕
↑
↓

Active Directory Custom LDAP

Configuration

Base distinguished name for users*

Base distinguished name for groups*

LDAP over SSL

Fetch the certificate or paste certificate in PEM format (be sure to include BEGIN and END lines): ⓘ

-----BEGIN CERTIFICATE-----
 certificate contents
 -----END CERTIFICATE-----

Fetch

Binding credentials ⓘ

Binding Method

Configured Credentials

Binding username*

Binding password*

Reset
Apply changes

Step 2. Configure each external LDAP server using the following steps.

1. Click the **Add** icon (⊕) to add an LDAP server.
2. Specify the domain name, IP address, and port for the external LDAP server.

If the port number is *not* explicitly set to 3268 or 3269, the entry is assumed to identify a domain controller.

When the port number is set to 3268 or 3269, the entry is assumed to identify a global catalog. The LDAP client attempts to authenticate using the domain controller for the first configured server IP address. If this fails, the LDAP client attempts to authenticate using the domain controller for the next server IP address.
3. Optionally choose to enable customizing advanced configuration settings. When you choose to use a custom configuration, you can specify the user search filter. If you do not specify a user search filter, (&&(objectClass=user)(|(userPrincipalName={0})(sAMAccountName={0}))) is used by default.

If advanced configuration is disabled, the default Active Directory configuration is used.

4. Specify the fully-qualified LDAP base distinguished name from which the LDAP client initiates the search for user authentication.
5. Specify the fully-qualified LDAP base distinguished name from which LDAP client initiates the search for user groups (for example, `dc=company,dc=com`).
6. Optionally specify credentials to bind XClarity Orchestrator to the external authentication server. You can use one of two binding methods.

- **Configured Credentials.** Use this binding method to use a specific client name and password to bind XClarity Orchestrator to the external authentication server. If the bind fails, the authentication process also fails. Specify the fully-qualified LDAP distinguished name (for example, `cn=somebody,dc=company,dc=com`) or email address (for example, `somebody@company.com`) of the user account, and the password to use for LDAP authentication to bind XClarity Orchestrator to the LDAP server. If the bind fails, the authentication process also fails.

The distinguished name must be a user account within the domain that has at least read-only privileges.

If the LDAP server does not have sub-domains, you can specify the user name without the domain (for example, `user1`). However, if the LDAP server does have sub-domains (for example, sub-domain `new.company.com` in domain `company.com`), then you must specify the username and domain (for example, `user1@company.com`).

Attention: If you change the client password in the external LDAP server, ensure that you also updated the new password in XClarity Orchestrator (see [Cannot log in to XClarity Orchestrator](#) in the XClarity Orchestrator online documentation).



- **Login Credentials.** Use this binding method to use your LDAP XClarity Orchestrator user name and password to bind XClarity Orchestrator to the external authentication server. Specify the fully-qualified LDAP distinguished name of a *test* user account and the password to use for LDAP authentication to validate the connection to the authentication server.

These user credentials are not saved. If successful, all future binds use the user name and password that you used to log in to XClarity Orchestrator. If the bind fails, the authentication process also fails.

Note: You must be logged in to XClarity Orchestrator using a fully-qualified user ID (for example, `administrator@domain.com`).

7. Optionally choose to use secure LDAP by selecting the **LDAP over SSL** toggle and then clicking **Fetch** to retrieve and import the trusted SSL certificate. When the Fetch server certificate dialog is displayed, click **Accept** to use the certificate. If you choose to use LDAP over SSL, XClarity Orchestrator uses the LDAPS protocol to connect securely to the external authentication server. When this option is selected, trusted certificates are used to enable secure LDAP support.

Attention: If you choose to disable LDAP over SSL, XClarity Orchestrator uses an unsecure protocol to connect to the external authentication server. If you choose this setting, your hardware might be vulnerable to security attacks.

8. Optionally reorder the LDAP servers using the **Move Up** icon () and **Move Down** icon (). The LDAP client attempts to authenticate using the first server IP address. If authentication fails, the LDAP client attempts to authenticate using the next server IP address.

Important: For secure LDAP authentication, use the certificate for the root certificate authority (CA) of the LDAP server or one of the intermediate certificates of the server. You can retrieve the root or intermediate CA certificate from a command prompt by running the following


command, where *{FullyQualifiedHostNameOrIpAddress}* is the fully qualified name of the external LDAP server. The root CA certificate or intermediate CA certificate is typically the last certificate in the output, the last BEGIN- -END section.

```
openssl s_client -showcerts -connect {FullyQualifiedHostNameOrIpAddress}:636
```

9. Click **Apply changes**. XClarity Orchestrator attempts to test the the IP address, port, SSL certificates, and binding credentials and validates the LDAP server connection to detect common errors. If the validation passes, user authentication occurs on the external authentication server when a user logs in to XClarity Orchestrator. If the validation fails, error messages are displayed that indicate the source of the errors.

Note: If the validation succeeds and connections to the LDAP server completes successfully, user authentication might fail if the root distinguished name is incorrect.

After you finish

You can remove an LDAP-server configuration by clicking the **Delete** icon () icon next to the configuration. When you delete an LDAP-server configuration, if there are no other LDAP-server configurations in the same domain, the clone users and clone user groups in that domain are also removed.

Managing users and user sessions

User accounts are used to log in and manage Lenovo XClarity Orchestrator.

Creating users

You can manually create user accounts in the local (embedded) authentication server. *Local user accounts* are used to log in to Lenovo XClarity Orchestrator and authorize access to resources.

About this task

Users in an external LDAP server are automatically cloned in the local authentication server with the name *{username}@{domain}* the first time the users log in. This cloned user account can be used only to authorize access to resources. Authentication still occurs through the LDAP authentication server for these users, and changes to the user account (other than description and roles) must be done through LDAP.


XClarity Orchestrator controls access to functions (actions) using roles. You can assign a different role to local and cloned users by adding those users to one or more user groups that are associated with the desired roles. By default, all users are members of the **OperatorGroup** user group (see [Creating user groups](#)).

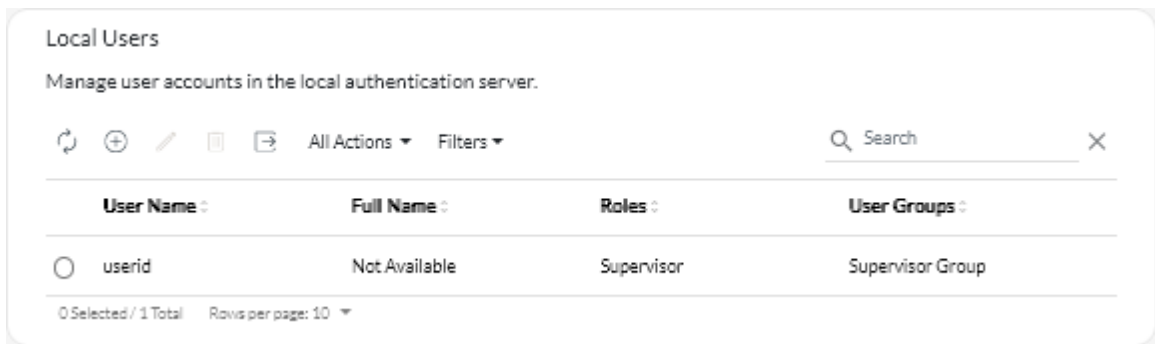
At least one user must be a member of a *local* user group to which the predefined **Supervisor** role is assigned (see [Controlling access to functions](#)).

Attention: Before an external LDAP user can log in to XClarity Orchestrator, the user must be a direct member of an LDAP user group that is cloned in XClarity Orchestrator (see [Creating user groups](#)). XClarity Orchestrator does not recognizes users that are members of user groups that are nested in the cloned LDAP user group defined in the external LDAP server.

Procedure

To create a local user, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Administration** () → **Security**, and then click **Local Users** in the left navigation to display the Local Users card.



Step 2. Click the **Create** icon (+) to create a user. The Create New User dialog is displayed.

Step 3. Fill in the following information in the dialog.

- Enter a unique user name. You can specify up to 32 characters, including alphanumeric, period (.), dash (-), and underscore (_) characters.

Note: User names are not case sensitive.

- Enter the new and confirm passwords. By default, passwords must contain **8 – 256** characters and must meet the following criteria.

Important: It is recommended that you use strong passwords of 16 or more characters.

- (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed)
- (2) Must contain at least one number
- (3) Must contain at least two of the following characters.
 - Uppercase alphabetic characters (A – Z)
 - Lowercase alphabetic characters (a – z)
 - Special characters ; @ _ ! ' \$ & +
 White space characters are not allowed.
- (4) Must not repeat or reverse the user name
- (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed)
- (Optional) Specify contact information for the user account, including the full name, email address, and phone number.

Tip: For the full name, you can specify up to 128 characters, including letters, numbers, spaces, periods, hyphens, apostrophes, and commas.

Step 4. Click the **User Groups** tab, and select the user groups to which this user is to be a member.

Tip: If a user group is not selected, the **OperatorGroup** is assigned by default (see [Creating user groups](#)).

Step 5. Click **Create**.

The user account is added to the table.

After you finish

You can perform the following actions from the Local Users card.

- View user properties by clicking the row in the table for a user to display the User Details dialog.

- Modify the properties of a selected user, including the password and user groups, by clicking the **Edit** icon (✎).
- Delete a selected user by clicking the **Delete** icon (🗑️). You cannot delete the existing LDAP user group from LDAP users
- Export user details, such as user name, first name, and last name by clicking the **Export** icon (📄).

Creating user groups

User groups are used to authorize access to resources.

Learn more:  [How to create a user group](#)

Before you begin

You can manually create user groups in the local repository. Local user groups contain local and cloned users.

You can clone any user groups that are defined in an external LDAP server. The cloned LDAP user group is named `{domain}\{groupName}` in the local repository. This cloned user group can be used only to authorize access to resources. Changes to the group name, description, and membership must be done through LDAP.

Before an external LDAP user can log in to XClarity Orchestrator, the user must be a direct member of an LDAP user group that is cloned in XClarity Orchestrator.

If the LDAP server configuration is setup to use login credentials and if you logged in to XClarity Orchestrator using a local XClarity Orchestrator user ID, you are prompted to provide LDAP user credentials when you clone an LDAP user group. In all other cases, you credentials are not required.

About this task

XClarity Orchestrator provides the following predefined user groups, one for each predefined role. For more information about roles, see [Controlling access to functions](#).

- **Supervisor Group.** Users in this user group are assigned the **Supervisor** role.
- **Hardware Administrator Group.** Users in this user group are assigned the **Hardware Administrator** role.
- **Security Administrator Group.** Users in this user group are assigned the **Security Administrator** role.
- **Reporter Group.** Users in this user group are assigned the **Reporter** role.
- **Updates Administrator Group.** Users in this user group are assigned the **Updates Administrator** role.
- **Operator Group.** Users in this user group are assigned the **Operator** role.
- **Operator Legacy Group.** Users in this user group are assigned the **OperatorLegacy** role. Note that this user group will be deprecated in a future release.

At least one user must be a member of a *local* user group to which the predefined **Supervisor** role is assigned (see [Controlling access to functions](#)).

Before an external LDAP user can log in to XClarity Orchestrator, the user must be a direct member of an LDAP user group that is cloned in XClarity Orchestrator (see [Creating user groups](#)). XClarity Orchestrator does not recognize users that are members of user groups that are nested in the cloned LDAP user group defined in the external LDAP server.

Procedure

To create a user group, complete the following steps.

- **Create a local user group**

1. From the XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Security**, and then click **User Groups** in the left navigation to display the User Groups card.

Name	Description	Roles
<input type="radio"/> Configuration Patterns Administra...	Allows users to configure servers u...	Configuration Patterns Administrato
<input type="radio"/> Hardware Administrator Group	Allows users to view data, manage ...	Hardware Administrator
<input type="radio"/> OS Administrator Group	Allows users to deploy operating s...	OS Administrator
<input type="radio"/> Operator Group	Allows user to only view the orches...	Operator
<input type="radio"/> Operator Legacy Group	Allows user to view the orchestrat...	Operator Legacy
<input type="radio"/> Reporter Group	Allows users to view the orchestrat...	Reporter
<input type="radio"/> Security Administrator Group	Allows user to modify security setti...	Security Administrator
<input type="radio"/> Supervisor Group	Allows user to view data about and...	Supervisor
<input type="radio"/> Updates Administrator Group	Allows user to manage the updates...	Updates Administrator

2. Click the **Create** icon (+) to display the Create group dialog.
3. Select **Local User Group** as the group type.
4. Specify the name and optional description for this user group.
5. Click the **Available Users** tab, and select the users that you want to include in this user group.
6. Click the **Roles** tab, and select the roles that you want to assign in this user group. If a role is not selected, the **Operator** role is assigned by default.
7. Click **Create**.

- **Clone a user group from an external LDAP server**

1. From the XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Security**, and then click **User Groups** in the left navigation to display the User Groups card.
2. Click the **Create** icon (+) to display the Create group dialog.
3. Select **LDAP User Group** as the group type.
4. Optionally specify a description for the group.
5. Select the LDAP configuration for the external LDAP server that contains the user group that you want to add.



Tip: Begin typing to find all group names that contain specified keyword

6. If the external LDAP server is configured using login credentials, specify the username and password to log in to the external LDAP server.

7. Specify a search string (with at least three characters) in the **Search Group** field, and click **Search** to find user groups in the external LDAP server that match the search string. Then, select the group that you want to add.
8. Click the **Roles** tab, and select the roles that you want to assign in this user group. If a role is not selected, the **Operator** role is assigned by default.
9. Click **Create**.

After you finish

You can perform the following actions from the User Groups card.

- Modify the properties, local membership, and roles of a selected user group by clicking the **Edit** icon ().
 - When you add or remove a user from a group, the user is automatically logged out if the roles (permissions) changed after the new groups assignment. When the user logs in again, the user is allowed to perform actions based on the aggregated roles of the assigned user groups.
 - Each user must be a member of at least one user group. If you set this attribute to an empty array or null, **OperatorGroup** is assigned by default.
 - For predefined user groups, you can modify only group membership.
 - For LDAP user group, you can modify only the description and roles. Use the external LDAP server to change other properties and membership.
- Delete a selected user group by clicking the **Delete** icon ().

Note: You cannot delete predefined user groups.
- View the members of a user group by clicking the group name to display the View group dialog and then clicking the **Members Summary** tab.

Changing details for your user account


You can change the password, full name, email address, and phone number for your user account.

About this task

User passwords expire after **0** days, by default.

Procedure

To change your password and other attributes, complete the following steps.

- Step 1. From the XClarity Orchestrator title bar, click the **User-Account** menu () in the upper-right corner, and then click **Change password**. The Change password dialog is displayed.
- Step 2. Enter the current password.
- Step 3. Enter the new and confirm passwords. By default, passwords must contain **8 – 256** characters and must meet the following criteria.
 - (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed)
 - (2) Must contain at least one number
 - (3) Must contain at least two of the following characters.
 - Uppercase alphabetic characters (A – Z)
 - Lowercase alphabetic characters (a – z)
 - Special characters ; @ _ ! ' \$ & +
 White space characters are not allowed.

- (4) Must not repeat or reverse the user name
- (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed)

Step 4. Change your full name, email address, and phone number, if appropriate.

Step 5. Click **Change**.

Changing details for another user

Supervisor users can change details, including the password, for another user.

About this task

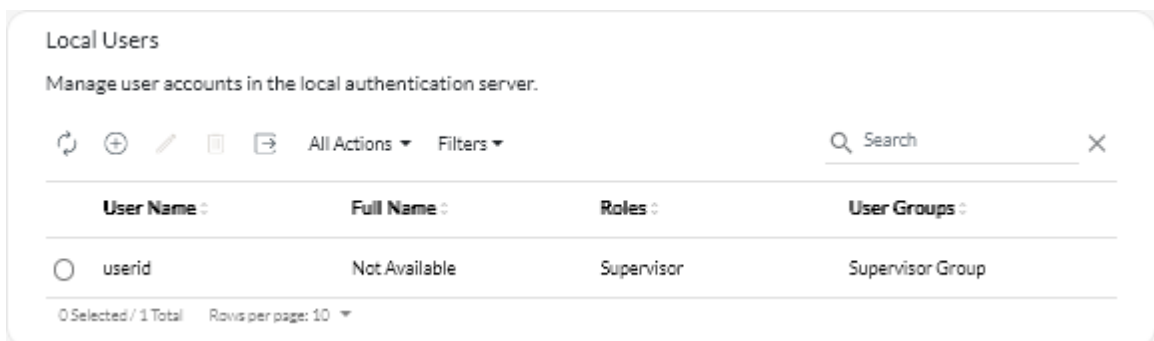
User passwords expire after **0** days, by default.

You can configure the password expiration time and also password complexity rules (see [Configuring user security settings](#)).

Procedure

To create a local user, complete the following steps.

Step 1. From the XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Security**, and then click **Local Users** in the left navigation to display the Local Users card.



Step 2. Select the user account.

Step 3. Click the **Edit** icon (✎) to modify the user’s properties. The Edit User dialog is displayed.

Step 4. Enter the new and confirm passwords. By default, passwords must contain **8 – 256** characters and must meet the following criteria.

- (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed)
- (2) Must contain at least one number
- (3) Must contain at least two of the following characters.
 - Uppercase alphabetic characters (A – Z)
 - Lowercase alphabetic characters (a – z)
 - Special characters ; @ _ ! ' \$ & +
 White space characters are not allowed.
- (4) Must not repeat or reverse the user name
- (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed)

Step 5. Click **Edit**.


Configuring user security settings

The user-account security settings configure the password, login, and user-session settings for local users.

Learn more:  [How to configure user security settings](#)

Procedure

To configure security settings for local users, complete the following steps.

Step 1. From the XClarity Orchestrator menu bar, click **Administration**  → **Security**, and then click **Account Security Settings** in the left navigation to display the Account Security Settings card.

Step 2. Configure the following security settings.

Security setting	Description	Allowed values	Default values
Password expiration period	Amount of time, in days, that a user can use a password before it must be changed Lower values reduce the amount of time that attackers have to guess passwords. If set to 0, passwords never expire.	0 – 365	0
Password expiration warning period	Amount of time, in days, before the password-expiration date when users begin to receive warnings about an impending expiration of the user password If set to 0, users are not warned.	0 – 30	0
Minimum password reuse cycle	Minimum number of times that a unique password must be specified when changing the password before the user can start to reuse passwords If set to 0, users can reuse passwords immediately.	0 – 10	5
Minimum password change interval	Minimum amount of time, in hours, that must elapse before a user can change a password again after it was previously changed The value specified for this setting cannot exceed the value specified for the Password expiration period setting. If set to 0, users can change passwords immediately.	0 – 240	1
Maximum number of login failures	Maximum number of times that a user can attempt to log in with an incorrect password before the user account is locked Note: Consecutive login attempts using the same user name and password count as a single failed login. If set to 0, accounts are never locked.	0 – 10	5

Security setting	Description	Allowed values	Default values
Failed login counter reset	<p>Amount of time since the last failed login attempt before the Maximum number of login failures counter is reset to 0. If set to 0, the counter never resets. For example, if the maximum number of login failures is 2, and you fail your login once, then fail it a second time 24 hours later, the system registers that you have failed your login twice, and your account is locked out.</p> <p>Note: This setting applies only when the Maximum number of login failures setting is set to 1 or greater.</p>	0 – 60	15
Lockout period after maximum login failures	<p>Minimum amount of time, in minutes, after which a locked user can attempt to log back in again</p> <p>A user account that is locked cannot be used to gain access to XClarity Orchestrator even if a valid password is provided.</p> <p>If set to 0, user accounts are never locked.</p> <p>Note: This setting applies only when the Maximum number of login failures setting is set to 1 or greater.</p>	0 – 2880	60
Web inactivity session timeout	<p>Amount of time, in minutes, that a user session established with the orchestrator server can be inactive before the user session expires and the user is automatically logged out. This timeout applies to all actions (such as opening a page, refreshing the current page, or modifying data). This is the primary timeout for the user session.</p> <p>When a session is active, this timer resets every time the user performs any action. After the timeout value is exceeded, the login page is displayed the next time the user attempts to perform an action.</p> <p>If set to 0, this timeout is disabled.</p> <p>Note: Changing this setting immediately affects all user sessions, regardless of authentication type. Existing sessions that have been inactive for longer than the new time-out value are expired.</p>	0, 60 – 1440	1440

Security setting	Description	Allowed values	Default values
Web inactivity timeout for full operations	<p>Amount of time, in minutes, that a user session established with the orchestrator server can be inactive before the actions that modify data (such as creating, updating, or deleting a resource) are disabled</p> <p>This is an optional secondary timeout and is shorter than the primary Web inactivity session timeout value.</p> <p>When a session is active, this timer resets every time the user performs any action. If this timeout value is exceeded but the primary Web inactivity session timeout value <i>is not</i> exceeded, the user is restricted to read-only actions (such as opening or refreshing a page) until the primary Web inactivity session timeout value is exceeded; however, if the user attempts to perform an action that modifies data, the user session expires and the login page is displayed.</p> <p>If set to 0, this timeout is disabled.</p> <p>Note: Changing this setting immediately affects all user sessions, regardless of authentication type. Existing sessions that have been inactive for longer than the new time-out value are expired.</p>	0, 15 – 60	30
Mandatory expiration time of a web-based session	<p>Amount of time, in hours, that a user session established with the orchestrator server can be open before the user is automatically logged out, regardless of user activity</p> <p>Note: Changing this setting immediately affects all user sessions, regardless of authentication type. Existing sessions that have been inactive for longer than the new timeout value are expired.</p>	24 – 240	24
Minimum password length	Minimum number of characters that can be used to specify a valid password	8 – 256	256
Maximum password length	Maximum number of characters that can be used to specify a valid password	8 – 128	128
Maximum active sessions for a specific user	<p>Maximum number of active sessions for a specific user that are allowed at any given time. When the maximum number is reached, the oldest active session for a user (based on the creation timestamp) is removed before a new session is created for that user.</p> <p>If set to 0, an unlimited number of active sessions is allowed for a specific user.</p> <p>Note: Only user sessions that start after the setting is changed are affected.</p>	0 – 20	20

Security setting	Description	Allowed values	Default values
Number of complexity rules that must be followed when creating a new password	<p>Number of complexity rules that must be followed when creating a new password. Rules are enforced starting with rule 1, and up to the number of rules specified. For example, if the password complexity is set to 4, then rules 1, 2, 3 and 4 must be followed. If the password complexity is set to 2, then rules 1 and 2 must be followed.</p> <p>XClarity Orchestrator supports the following password complexity rules.</p> <ul style="list-style-type: none"> • (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed) • (2) Must contain at least one number • (3) Must contain at least two of the following characters. <ul style="list-style-type: none"> – Uppercase alphabetic characters (A – Z) – Lowercase alphabetic characters (a – z) – Special characters ; @ _ ! ' \$ & + White space characters are not allowed. • (4) Must not repeat or reverse the user name • (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed) <p>If set to 0, passwords are not required to comply with any complexity rules.</p>	0 – 5	4
Force user to change password on first access	Indicates whether a user is required to change the password when logging in to XClarity Orchestrator for the first time	Yes or No	Yes

Step 3. Click **Apply**.

After the changes are applied, the new settings take effect immediately. If you change password policies, those policies are enforced the next time a user logs in or changes the password.

After you finish

You can perform the following action from the Account Security Settings card.

- To reset these settings to the default values, click **Restore defaults**.

Monitoring active user sessions

You can determine who is logged in to the XClarity Orchestrator web interface.

Before you begin

By default, user sessions that have no activity for more than 24 hours are logged out automatically. You can configure the Web inactivity session timeout (see [Configuring user security settings](#))

Procedure

To view a list of all active user sessions (including the current session), click **Administration** (⚙️) → **Security** from the XClarity Orchestrator menu bar, and then click **Active Sessions** in the left navigation to display the Active Sessions card.

User Name	IP Address	Last Accessed
userid	Not Available	10/4/22, 3:36 AM
userid	Not Available	10/4/22, 12:55 PM

After you finish

You can perform the following action from the Active Sessions card.

- Disconnect a selected user session by clicking the **Delete** icon (🗑️).

Note: You cannot disconnect the current session.

Controlling access to functions

Lenovo XClarity Orchestrator uses *roles* and *user groups* to determine which functions (actions) a user is allowed to perform.

About this task

A *role* is a set of functions. When a role is assigned to a user group, all users in that group can perform the functions that are included in that role.

XClarity Orchestrator provides the following predefined roles.

- **Supervisor.** Allows users to view data about and perform all available actions on the orchestrator server and all managed resources (resource managers and devices). Users that are assigned this role always have access to all resources (devices and resource managers) and all functions. You cannot restrict access to resources or functions for this role.

You must have supervisor privileges to perform the following actions.

- Performing maintenance tasks, such as installing licenses and updating to a newer version
- Connecting and disconnecting resource managers
- Modifying system settings, such as network preferences and the date and time
- Agreeing to send periodic data to Lenovo

There must be at least one user with supervisor privileges.

Important: When upgrading from XClarity Orchestrator v1.0 to a later release, all users that were created in XClarity Orchestrator v1.0 are given supervisor privileges by default. A supervisor user can remove the supervisor privileges for users that should not have those privileges.

- **Hardware Administrator.** Allows users to view data, manage and deploy configuration patterns, manage and deploy operating systems using OS profiles, view and customize analytics, and perform actions on accessible resources. This role prohibits users from updating software or firmware on managed resources, and from managing resource groups.
- **Server Configuration Administrator.** Allows users to configure servers using configuration patterns, , view predefined analytics, and view data for accessible resources. This role prohibits users from remotely accessing the devices and powering devices on and off.
- **OS Administrator.** Allows users to deploy operating systems using OS profiles, view predefined analytics, and view data for accessible resources. This role prohibits users from remotely accessing the devices and powering devices on and off.
- **Updates Administrator.** Allows users to update firmware on devices and software on resource managers, view data for accessible resources, and view predefined analytics.
- **Security Administrator.** Allows users to modify security settings and perform security-related actions on the orchestrator server, view data for all managed resources, manage resource group, and view predefined analytics. Users that are assigned this role always have access to all resources (devices and resource managers). You cannot restrict access to resources for this role.
- **Reporter.** Allows users to view the orchestrator-server configuration, view data about accessible resources, create queries to generate custom reports, and create data forwarders to schedule and email reports. This role prohibits users from provisioning resources and powering devices on and off.
- **Operator.** Allows users to view the orchestrator server configuration and view data for accessible resources. This role prohibits users from performing actions or modifying configurations settings on the orchestrator server and managed resources, creating and viewing analytics reports, and creating custom alerts.
- **Operator Legacy.** Allows users to view data and perform certain actions on accessible resources, such as managing inventory, alerts and service tickets. This role prohibits users from updating software or firmware on managed resources, creating resource groups, creating and viewing analytics reports, and creating custom alerts.

Attention: When upgrading from XClarity Orchestrator v1.2 to a later release, users that are assigned the **Operator** role are automatically changed to the **Operator Legacy** role and added to the **OperatorLegacyGroup** user group. The **Operator Legacy** role and **OperatorLegacyGroup** user group will be deprecated in a future release.

If a user does is not allowed to perform specific actions, menu items, toolbar icons, and buttons that are used to perform those actions are disabled (greyed out).

Note: Viewing resource-related data is not restricted based on roles. All users can view resource-related data (such as inventory, alerts, jobs, and service tickets) for resources that they can access.

Procedure

To view information about the predefined roles, click **Administration** (⚙️) → **Security** from the XClarity Orchestrator menu bar, and then click **Roles** in the left navigation.

Click the row for any role to display the Roles dialog with information about the role properties, list of functions in the role, and a list of user groups to which the role is assigned.

Assigning roles to users

Lenovo XClarity Orchestrator uses *roles* and *user groups* to determine which functions (actions) a user is allowed to perform.

Before you begin

When roles are changed for a user that is currently logged in to an active session, the user's session is ended automatically, and the user is logged out of the user interface. When the user logs in again, the user can perform the functions based on the new role assignments.

About this task

When you assign multiple roles to a user group, the functions in each role are aggregated.

All users that are members of a user group are allowed to perform the functions that are included in the roles that are assigned to that user group.

You can modify a user's roles by:

- Adding or removing the user from a user group
- Adding or removing roles from a user group of which the user is a member
- Deleting a user group of which the user is a member

Notes:

- When LDAP users are added or removed from LDAP user groups on the LDAP server, the changes to the associations between the LDAP user and LDAP user group are automatically updated in XClarity Orchestrator based on existing cloned LDAP user groups.
- When the roles that are assigned to a user group change, the user must log in again for the roles changes to take effect.

Controlling access to resources

Lenovo XClarity Orchestrator uses *access-control lists* (ACLs) to determine which resources (devices, resource managers, and XClarity Orchestrator) users can access. When a user has access to a specific set of resources, that user can see data (such as inventory, events, alerts, and analytics) that is related to only those resources

About this task

An ACL is a union of user groups and resource groups.

- *User groups* identify the users that are affected by this ACL. The ACL must contain a single user group. Users that are members of a group to which the predefined **Supervisor** role is assigned always have access to all resources. You cannot limit resource access for supervisor users.

When resource-based access is enabled, users that *are not* members of a group to which the predefined **Supervisor** role is assigned do not have access to any resources (devices and resource managers) by default. You must add non-supervisor users to a user group that is part of an access-control list to allow those users to access a specific set of resources.

When resource-based access is disabled, all users have access to all resources (devices and resource managers) by default.

- *Resource groups* identify the resources (devices, resource managers, and XClarity Orchestrator) that can be accessed. The ACL must contain at least one resource group.

Note: A user that has access to a manager group does not automatically get access to all devices that are managed by that resource manager. You must give explicit access to devices using device groups.

Procedure

To control access to resources, complete the following steps.

- Step 1. Create a group of users that can access the resources.
- Step 2. Create one or more groups of resources to which you want to control access.
- Step 3. Create an access-control lists that contains the user group and one or more resource groups.
- Step 4. Enable resource-based access control.

Enabling resource-based access

If you want to limit the resources that users can access, enable resource-based access.

About this task

Users that are members of a group to which the predefined **Supervisor** role is assigned always have access to all resources. You cannot limit resource access for supervisor users.

When resource-based access is enabled, users that *are not* members of a group to which the predefined **Supervisor** role is assigned do not have access to any resources (devices and resource managers) by default. You must add non-supervisor users to a user group that is part of an access-control list to allow those users to access a specific set of resources.

When resource-based access is disabled, all users have access to all resources (devices and resource managers) by default.

Procedure

To enable resource-based access controls, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Security**, and then click **Access Controls** in the left navigation to display the Access Controls card.

Access Control

Access-control lists are used to limit a user's access to resources (devices and resource managers). When a user has access to a specific set of resources, that user can see data (such as inventory, events, alerts, and analytics) that is related to only those resources.

Resource Based Access Enabled

⏪ ⊕ ✎ 🗑️ 🔄 All Actions ▾ Filters ▾ 🔍 Search ✕

Name ▾	Description :
<input type="checkbox"/> ac_1	Not Available

0 Selected / 1 Total Rows per page: 10 ▾

- Step 2. Click the **Resource Based Access** toggle to enable resource access control using access control lists.

Creating access-control lists

Lenovo XClarity Orchestrator uses *access-control lists* (ACLs) to determine which resources (devices, resource managers, and XClarity Orchestrator) users can access. When a user has access to a specific set of resources, that user can see data (such as inventory, events, alerts, and analytics) that is related to only those resources

Learn more:  [How to create access control lists](#)

Before you begin

Ensure that the user groups that you want to associate with the ACL are defined (see [Creating user groups](#)).

Ensure that all resource groups that you want to associate with this ACL are defined (see [Creating resource groups](#)).

About this task

An ACL is a union of user groups and resource groups.

- *User groups* identify the users that are affected by this ACL. The ACL must contain a single user group. Users that are members of a group to which the predefined **Supervisor** role is assigned always have access to all resources. You cannot limit resource access for supervisor users.

When resource-based access is enabled, users that *are not* members of a group to which the predefined **Supervisor** role is assigned do not have access to any resources (devices and resource managers) by default. You must add non-supervisor users to a user group that is part of an access-control list to allow those users to access a specific set of resources.


When resource-based access is disabled, all users have access to all resources (devices and resource managers) by default.

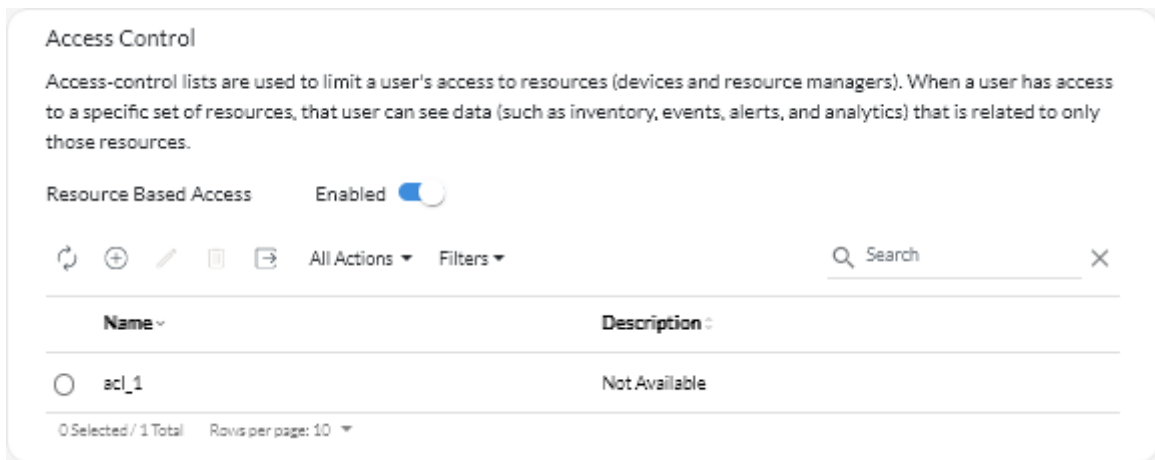
- *Resource groups* identify the resources (devices, resource managers, and XClarity Orchestrator) that can be accessed. The ACL must contain at least one resource group.

Note: A user that has access to a manager group does not automatically get access to all devices that are managed by that resource manager. You must give explicit access to devices using device groups.

Procedure

To create an access-control list, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Administration**  → **Security**, and then click **Access Controls** in the left navigation to display the Access Controls card.



- Step 2. Click the **Add** icon (+) to add an ACL. The Create Access Control dialog is displayed
- Step 3. Specify the name and optional description for the ACL.
- Step 4. Click **User Group**, and select the user group that you want to include in this ACL.
- Step 5. Click **Resource Groups**, and select the resource groups that you want to include in this ACL.
- Step 6. Click **Create**.

The access-control list is added to the table

After you finish

You can perform the following actions on this page.

- View the user group and resources groups in a specific ACL by clicking anywhere in the row for that ACL.
- Modify the properties and membership of a selected ACL by clicking the **Edit** icon (✎).
- Delete a selected ACL by clicking the **Delete** icon (🗑).
- If a user cannot access data for a specific resource or if a user can access data for a specific resource that should not be accessed, identify the access-control lists that are associated with the user and then view the membership of each resource group that is also associated with those access-control lists. Ensure that the resource in question is or is not included in those resource groups.

Managing disk space

You can manage the amount of disk space that is used by Lenovo XClarity Orchestrator by deleting files that are no longer needed

About this task

Procedure

To delete unneeded files, complete one or more of the following procedures.

Device service-data files

1. From the Lenovo XClarity Orchestrator menu bar, click the **Administration** (⚙) → **Service and Support**, and then click **Service Data** tab to display the Device Service Data card.
2. Select one or more service-data files to be deleted, and click the **Delete** icon (🗑).

Operating system images

1. From the Lenovo XClarity Orchestrator menu bar, click the **Administration** (⚙️) → **OS Deployment**, and then click **OS Management** tab to display the OS Images card.
2. Select one or more OS images to be deleted, and click the **Delete** icon (🗑️).

Update payload files

Ensure that the updates are not used in an updates-compliance policy. You can remove an update from a policy from the Apply and Activate card (see [Creating and assigning update-compliance policies](#)).

1. From the XClarity Orchestrator menu bar, click **Provisioning** (🔧) → **Updates**, and then click the **Repository Management** tab to display the Repository Management card.
2. Select one or more update packages or files to be deleted.
3. Click **Delete only payload files** icon (🗑️) to delete only the image (payload) file for each selected update. Information about the update (the XML metadata file) remains in the repository, and the download status changes to “Not downloaded.”

XClarity Orchestrator updates

You can delete orchestrator-server updates that are in the Downloaded state. The **Applied Status** column in the table indicates the status of the update.

1. From the XClarity Orchestrator menu bar, click **Maintenance** (🔧), and then click the **Orchestrator Server Update** tab to display the Orchestrator Server Update card.
2. Select one or more updates to be deleted, and click the **Delete** icon (🗑️). The **Acquired Status** column for the deleted updates changes to “Not downloaded.”

Backing up and restoring orchestrator-server data

Lenovo XClarity Orchestrator does not include built-in backup and restore functions. Instead, use the backup functions that are available based on the virtual-host operating system on which XClarity Orchestrator is installed.

About this task

Always back up XClarity Orchestrator after performing the initial setup and after making significant configuration changes, including:

- Before updating XClarity Orchestrator
- After making any network changes
- After adding users to XClarity Orchestrator local authentication server
- After managing new resource managers

If you have backup and restore procedures in place for virtual hosts, ensure that your procedures include XClarity Orchestrator.

Important:

- Ensure that all running jobs are complete and that XClarity Orchestrator is shut down before you create a backup.
- Ensure that you back up XClarity Orchestrator on a regular basis. If the host operating system shuts down unexpectedly, you might not be able to authenticate with XClarity Orchestrator after the host operating system is restarted. To resolve this problem, restore XClarity Orchestrator from the last backup.

Backing up and restoring orchestrator-server data on a VMware ESXi host

At times, you might need to restore s orchestrator-server data from a backup. Several alternatives are available to backup and restore an XClarity Orchestrator virtual appliance that is running on a VMware ESXi host. The specific process to use to restore from a backup are typically based on the process that was used to create the backup. This topic discusses how to backup and restore using the VMware vSphere Client.

About this task

If VMware vCenter Server is installed, you can use the backup capability that is provided with VMware vCenter to back up XClarity Orchestrator.

If you do not have VMware vCenter Server installed, you can use the VMware vSphere Client to create a backup of the virtual machine by copying the files from the XClarity Orchestrator folder to another folder in the same datastore. You can also copy the files to a different datastore or even a different host for additional backup protection.

Note: VMware vCenter Server is not required to perform a backup using this procedure.

Procedure

- **Backing up XClarity Orchestrator** To create a backup of XClarity Orchestrator using VMware vSphere Client, complete the following steps.
 1. Shutdown XClarity Orchestrator.
 2. Launch the VMware vSphere Client, and connect to the ESXi host on which XClarity Orchestrator is located.
 3. Create a new folder in the same datastore that is used by XClarity Orchestrator.
 - a. Select the ESXi host in the navigation tree, and click the **Configure** tab in the right window.
 - b. Click **Hardware → Storage**.
 - c. Right-click the datastore for XClarity Orchestrator, and click **Browse Datastore**.
 - d. Select the root folder, and then create a new folder to contain a copy of the XClarity Orchestrator files.
 4. Click the XClarity Orchestrator folder.
 5. Select all of the files in the folder, and copy the files to the backup folder that you just created.
 6. Restart XClarity Orchestrator.
- **Restoring XClarity Orchestrator** To restore XClarity Orchestrator using the backup created in the previous procedure, complete the following steps.
 1. Launch the VMware vSphere Client, and connect to the ESXi host on which XClarity Orchestrator is installed.
 2. Right-click XClarity Orchestrator in the left navigation tree, and then click **Power → Power Off**.
 3. Right-click XClarity Orchestrator in the left navigation tree again, and then click **Remove from Inventory**.
 4. Delete the files from the XClarity Orchestrator folder in the datastore that is used by the XClarity Orchestrator.
 - a. Select the ESXi host in the navigation tree, and then click the **Configure** tab in the right window.
 - b. Click **Hardware → Storage**.
 - c. Right-click the datastore for XClarity Orchestrator, and click **Browse Datastore**.
 - d. Select the XClarity Orchestrator folder.

- e. Select all files in the folder, right-click the files, and click **Delete selected items**.
5. Select the folder where the backup files are stored.
6. Select all of the files in the folder, and copy them to the XClarity Orchestrator folder.
7. In the XClarity Orchestrator folder, right-click the VMX file, and click **Add to inventory**.
8. Complete the wizard to add XClarity Orchestrator data.
9. Restart XClarity Orchestrator from VMware vSphere Client.
10. When you are prompted to choose whether the VM was moved or copied, select **moved**.

Important: If you select **copied**, the VM is given a UUID that is different than that of the original VM, which makes the VM act like a new instance and unable to see previously managed devices.

Backing up and restoring orchestrator-server data on a Microsoft Hyper-V host

At times, you might need to restore Lenovo XClarity Orchestrator orchestrator-server data from a backup. Several alternatives are available to backup and restore an XClarity Orchestrator virtual appliance that is running on a Microsoft Hyper-V host. The specific process to use to restore from a backup are typically based on the process that was used to create the backup. This topic discusses how to backup and restore using the Windows Server Backup.

Before you begin

Ensure that Windows Server Backup is set up correctly by completing the following steps.

1. Launch Windows Server Manager.
2. Click **Manage → Add Roles and Features**.
3. Skip through the wizard until you reach the **Select Features** page.
4. Select the **Windows Server Backup** check box.
5. Complete the wizard.

Procedure

- **Backing up XClarity Orchestrator**To create a backup of XClarity Orchestrator using Windows Server Backup, complete the following steps.
 1. Launch Windows Server Backup, and browse to **Local Backup**.
 2. In the Action pane, click **Backup Once** to start the Backup Once Wizard.
 3. On the Backup Options page, click **Different Options**, and then click **Next**.
 4. On the Select Backup Configuration page, click **Custom**, and then click **Next**.
 5. On the Select Items for Backup page, click **Add Items** to display the Select Items window.
 6. Expand the Hyper-V item, click the XClarity Orchestrator virtual machine, and then click **OK**.
 7. Click **Next** to continue.
 8. On the Specify Destination Type page, choose the type of storage for the backup (either a local drive or a remote shared folder), and then click **Next**.
 9. On the Select Backup Destination or Specify Remote Folder page, specify the location to which you want the backup stored, and then click **Next**.
 10. Click **Backup** to start the backup process.
- **Restoring XClarity Orchestrator**To restore XClarity Orchestrator using the backup that was created in the previous procedure, complete the following steps.
 1. Launch Windows Server Backup, and browse to **Local Backup**.
 2. In the Action pane, click **Recover** to start the Recovery Wizard.

3. On the Getting Started page, specify the location where the backup is stored, and click **Next**.
4. On the Select Backup Date page, choose the backup that you want to restore, and click **Next**.
5. On the Select Recovery Type page, select **Hyper-V option**, and click **Next**.
6. On the Select Items to Recover page, expand Hyper-V, and select the XClarity Orchestrator virtual machine. Then, click **Next**.
7. On the Specify Recovery Options page, choose to recover the VM to its original location, and then click **Next**.
8. On the Confirmation page, click **Recover**. The virtual machine is restored and registered in Hyper-V.
9. Restart XClarity Orchestrator from Hyper-V Manager.

Chapter 3. Monitoring resources and activities

You can use Lenovo XClarity Orchestrator to monitor asset inventories, firmware and configuration compliance, health status, and event history of you managed devices.

Viewing a summary of your environment

The dashboard is the hub of Lenovo XClarity Orchestrator, which provides access to information that is important to you. It contains report cards that each summarize the status of resources and activities in your environment, including devices health, compliance, and alerts.

To access the dashboard, click **Dashboard**  from the XClarity Orchestrator menu bar.

You can change the scope of the summary to only those devices that are managed by a specific resource manager or in a specific resource group by using the **Select manager** drop-down menu.

You can click any of the linked statistics on the Dashboard to view a filtered list of data that fits the criteria.

Warranty

The Warranty card summarizes the warranty period for managed devices, including the following data.

- Number of devices for which the warranty is expired
- Number of devices for which the warranty is active
- Number of devices for which warranty data is not available

Service tickets

The Service Tickets card summarizes the managed, including the following data.

- Total number of active service tickets
- Number of service tickets that are open
- Number of service tickets that are in progress
- Number of service tickets that are on hold
- Number of service tickets that are closed
- Number of service tickets in other states

Firmware compliance

The Firmware Compliance card summarizes compliance with the firmware-compliance policy assigned to managed devices in XClarity Orchestrator, including the following data.

- Number of devices that *are not* compliant
- Number of devices that are compliant
- Number of devices that *do not* have an assigned firmware-compliance policy
- Number of devices for which compliance is not supported
- Number of devices for which compliance is being checked against the assigned policy

Note: This data represents firmware compliance based on policies that are assigned by XClarity Orchestrator. It does not represent policies that are assigned by Lenovo XClarity Administrator resource managers.

Configuration compliance

The Configuration Compliance card summarizes compliance with the server-configuration patterns on managed devices, including the following data.

- Number of devices that *are not* compliant with their assigned pattern
- Number of devices that are compliant with their assigned pattern

- Number of devices that *do not* have an assigned pattern
- Number of devices for which a configuration-compliance check is in progress
- Number of devices for which a manual restart is required to complete pattern deployment (pending restart)
- Number of devices for which the last pattern deployment failed

Note: This data represents server-configuration compliance for all devices based on patterns that are assigned by XClarity Orchestrator. It does not represent patterns that are assigned by managed XClarity Administrator resource managers.

Security Fixes

The Security Fixes card summarizes the number of managed devices that have common vulnerabilities and exposures (CVEs) for which a security fix is available, by the highest CVE severity.

- Number of devices that have at least critical vulnerabilities
- Number of devices that have at least one or more high, medium, or low vulnerabilities but no critical vulnerabilities
- Number of devices that have no known vulnerabilities and are protected

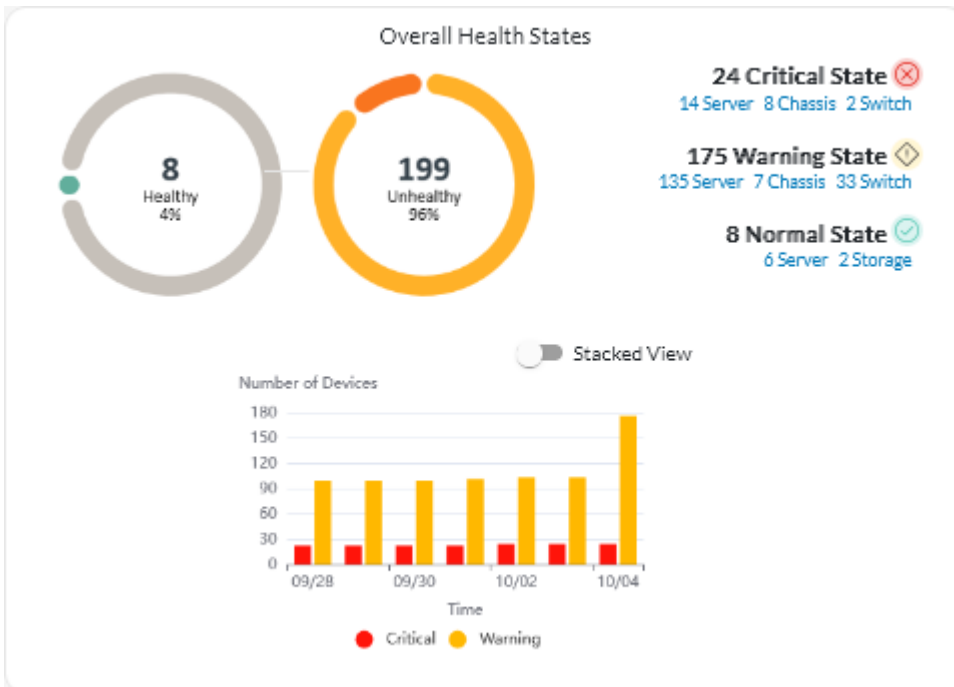
Firmware age

The Firmware Age card summarizes the age of firmware per component type.

- Number of firmware that is more than 2 years old for each component type
- Number of firmware that is between 1 year and 2 years old for each component type
- Number of firmware that is between 6 months and 1 year old for each component type
- Number of firmware that is less than 6 months old for each component type

Overall health status

The Overall Health States card summarizes the managed devices that are currently healthy and unhealthy in your environment.



This card includes the following data.

- A circular graph representing the percent of devices that are in a healthy state (normal) and unhealthy state (critical, warning, and unknown)

Tip: Each colored bar in the circular graph indicates the number of devices in a specific state. You can hover over each colored bar to get more information about the state.

- Total number and percent of devices that are healthy and unhealthy
- Number of devices of each type that are currently in critical, warning, normal and unknown states

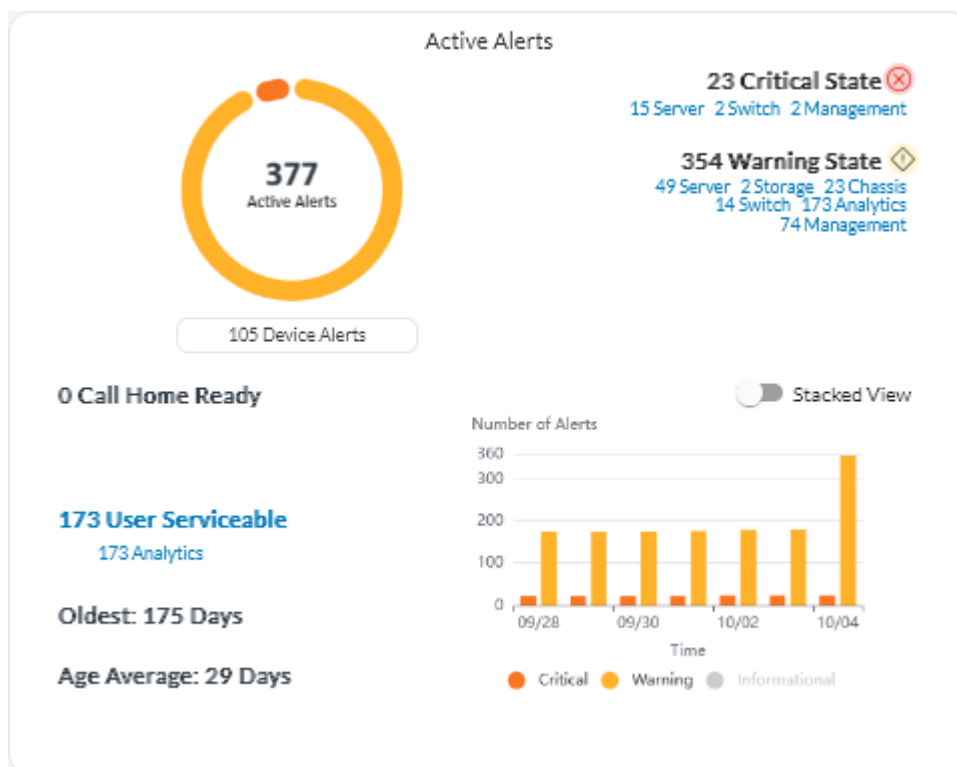
Tip: You can click on the number of devices in a specific state to open a page with a filtered list of devices that match the criteria.

- A line graph representing the number of devices in unhealthy states, over time

Tip: Each colored bar in the bar graph indicates the number of devices in a specific state. You can hover over each colored bar to get more information about the state.

Active alerts

The Devices Active Alerts card summarizes the active alerts were raised by the managed devices.



This card includes the following data.

- A circular graph representing the percent of active alerts for each severity (critical, warning, informational, and unknown)

Tip: Each colored bar in the circular graph indicates the number of alerts with a specific severity. You can hover over each colored bar to get more information about the severity.

- Total number of active alerts
- Number of devices that have active alerts

- Total number of active alerts for each severity, and the number of devices of each type that have active alerts for each severity

Tip: You can click on the number of devices in a specific state to open a page with a filtered list of devices that match the criteria.

- A line graph representing the number of devices in unhealthy states, over time

Tip: Each colored bar in the bar graph indicates the number of alerts with a specific severity. You can hover over each colored bar to get more information about the severity.

- Number of active alerts that opened a service ticket with the Lenovo Support Center (Call Home)
- Total number of active alerts that require user action (user serviceable), and the number of number of devices of each type that have active user-serviceable alerts
- Age of the oldest active alert
- Average age of all active alerts

Viewing resource manager status and details

You can view the type, version, status, and connectivity of each resource manager.

About this task

The **Health Status** column identifies the overall health of a resource manager. The following health states are used.

- (🟢) Normal
- (🟡) Warning
- (🔴) Critical

Procedure

To view the details of resource managers, click **Resources** (⚙️) → **Resource Manager** from the XClarity Orchestrator menu bar to display the Resource Managers card.

Resource Managers

Define the resource managers through which XClarity Orchestrator receives device information and performs management functions.

<input type="checkbox"/>	Resource Ma	Health Status	Type :	Version :	Build :	Connected :	Drive Analyt	Groups :
<input type="checkbox"/>	XClarity...	🟢 No...	XClarity ...	2.0.0	279	Not Availal	Not Availal	Not Availal
<input type="checkbox"/>	host-10-...	🟢 No...	XClarity ...	3.6.0	108	2/16/23, 1	🔴 1	Not Availal

0 Selected / 2 Total Rows per page: 10

After you finish

You can perform the following actions from the Resource Managers card.

- Connect a resource manager by clicking the **Connect** icon (⊕) (see [Connecting resource managers](#)).

- Disconnect and remove a selected resource manager by clicking the **Delete** icon (🗑️).

Note: If XClarity Orchestrator cannot connect to the resource manager (for example, if credentials are expired or if there are network issues), select **Force disconnect**.

A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

When the resource manager is removed, all devices that are managed by that resource manager are also removed. This includes device inventory, logs, metrics data, and analytic reports.

- View a status summary of all resource managers or for a selected resource manager by clicking, click **Dashboard** (📊) from the XClarity Orchestrator menu bar. You can narrow the scope to a single resource manager or resource group by using the **Select manager** drop-down menu.

Viewing devices status

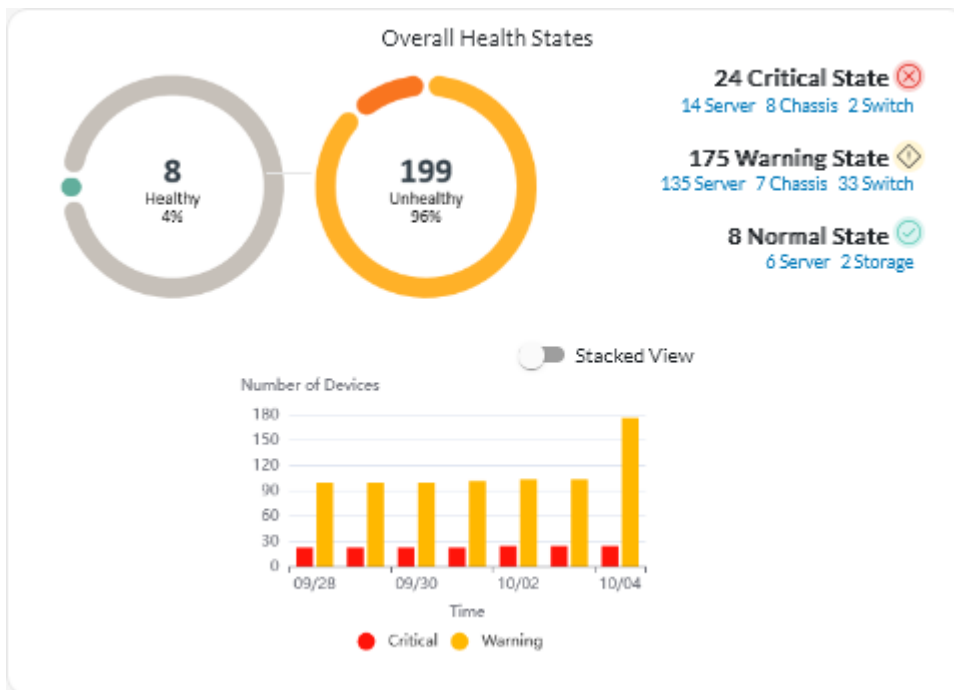
You can view the status of all devices that are managed across all resource managers.

Procedure

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

- **Status summary of all devices** From the XClarity Orchestrator menu bar, click **Dashboard** (📊) to display the dashboard cards with an overview and status of all managed devices and other resources (see [Viewing a summary of your environment](#)).

You can change the scope of the summary to only those devices that are managed by a specific resource manager or in a specific resource group by using the **Select manager** drop-down menu.

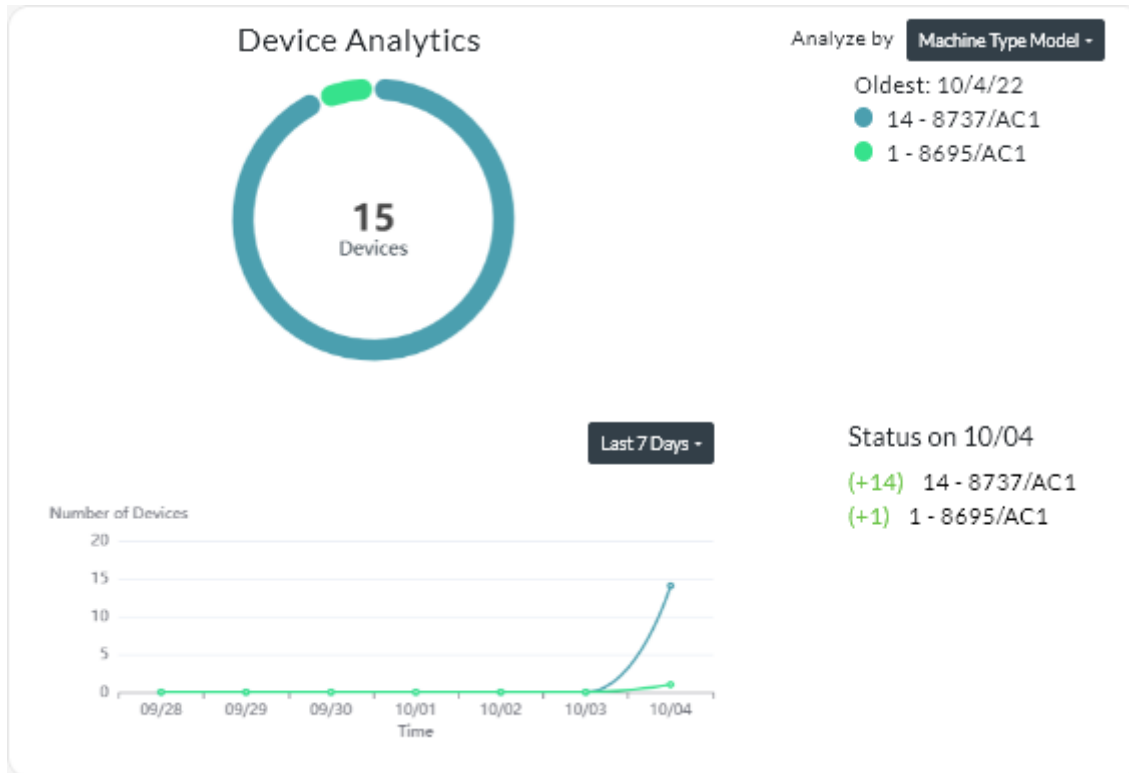


Each colored bar in the circular and bar graphs indicates the number of devices in a specific state. You can hover over each colored bar to get more information about the state. You can also click the number of devices in each state to view a list of all devices that fit the criteria.

- **Status for all devices of a specific type** To view the overall active alert summaries, click **Resources** (🔊) from the XClarity Orchestrator menu bar, and then click the device type to display a card with a tabular view of all devices of that type. For example, if you select **Severs**, a list of all rack, tower, and dense servers and all Flex System and ThinkSystem servers in a chassis is displayed.

You can change the scope of the summary based on device property from the **Analyze by** drop-down list.

- **Machine Type Model.** (default) This report summarizes device health by machine type model (MTM).
- **Machine Type.** This report summarizes device health by machine type.
- **Product Name.** This report summarizes device health by product.



XClarity Orchestrator summarizes device health based on specific criteria. Each summary includes the following information.

- A circular chart that shows the total number of devices that are unhealthy and percentage of devices in each unhealthy state (critical, warning, and unknown).

Each colored bar in the circular graph indicates the number of devices in a specific state. You can hover over each colored bar to get more information about the state.

- A line graph that shows number of devices in each health state per day over the specified number of days.

Each colored bar in the line graph indicates the number of devices in a specific state. You can hover over each colored bar to get more information about the state.

- The number of devices of each type that are unhealthy on a specific day. The current day is shown by default. You can change the day by hovering over each day in the line graph.

- **Status for a specific device** From the XClarity Orchestrator menu bar, click **Resources** (🔊), and then click the device type to display a card with a tabular view of all devices of that type. For example, if you select **Severs**, a list of all rack, tower, and dense servers and all Flex System and ThinkSystem servers in a chassis is displayed.

Servers

Search

<input type="checkbox"/>	Server	Status	Connecti	Power	IP Address	Product	Type-Mo	System F	Advisory	Groups
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	ite-b...				10.24...	Leno...	716...	CGE1f	Not ...	Not Av
<input type="checkbox"/>	Blac...				10.24...	Leno...	716...	A3EGf	Not ...	Not Av
<input type="checkbox"/>	nod...				10.24...	IBM...	791...	Not Av	Not ...	Not Av
<input type="checkbox"/>	Meh...				10.24...	Thin...	7Y4...	ISE13f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Not ...	Not Av

0 Selected / 60 Total Rows per page: 10

The **Status** column identifies the overall health of a device. The following health states are used. If a device is in an unhealthy state, use the alerts log to help identify and resolve the issues (see [Monitoring active alerts](#)).

- Normal
- Warning
- Critical

The **Connectivity** column identifies the connection status between the device and XClarity Orchestrator. The following connectivity states are used.

- Offline
- Offline Managed
- Online
- Partial
- Pending

The **Power** column identifies the power status. The following power states are used.

- On
- Off

The **Advisory** column identifies the number of online customer advisories (technical tips) that are related to each server. Click the number to display the Advisory card on the device details page to display a list of

online customer advisories, including the abstract and link for each advisory. Click a link to open a webpage with details for that advisory.

After you finish

You can perform the following action from the device cards.

- Add a selected device to a group by clicking **All Actions** → **Add items to Group**.
- Forward reports about specific device types on a reoccurring basis to one or more email addresses by clicking the **Create Report Forwarder** icon (⊕). The report is sent using the data filters that are currently applied to the table. All shown and hidden table columns are included in the report. For more information, see [Forwarding reports](#).
- Add a report about a specific device type to a specific report forwarder using the data filters that are currently applied to the table by clicking the **Add to Report Forwarder** icon (↗). If the report forwarder already includes a report for that device type, the report is updated to use the current data filters.

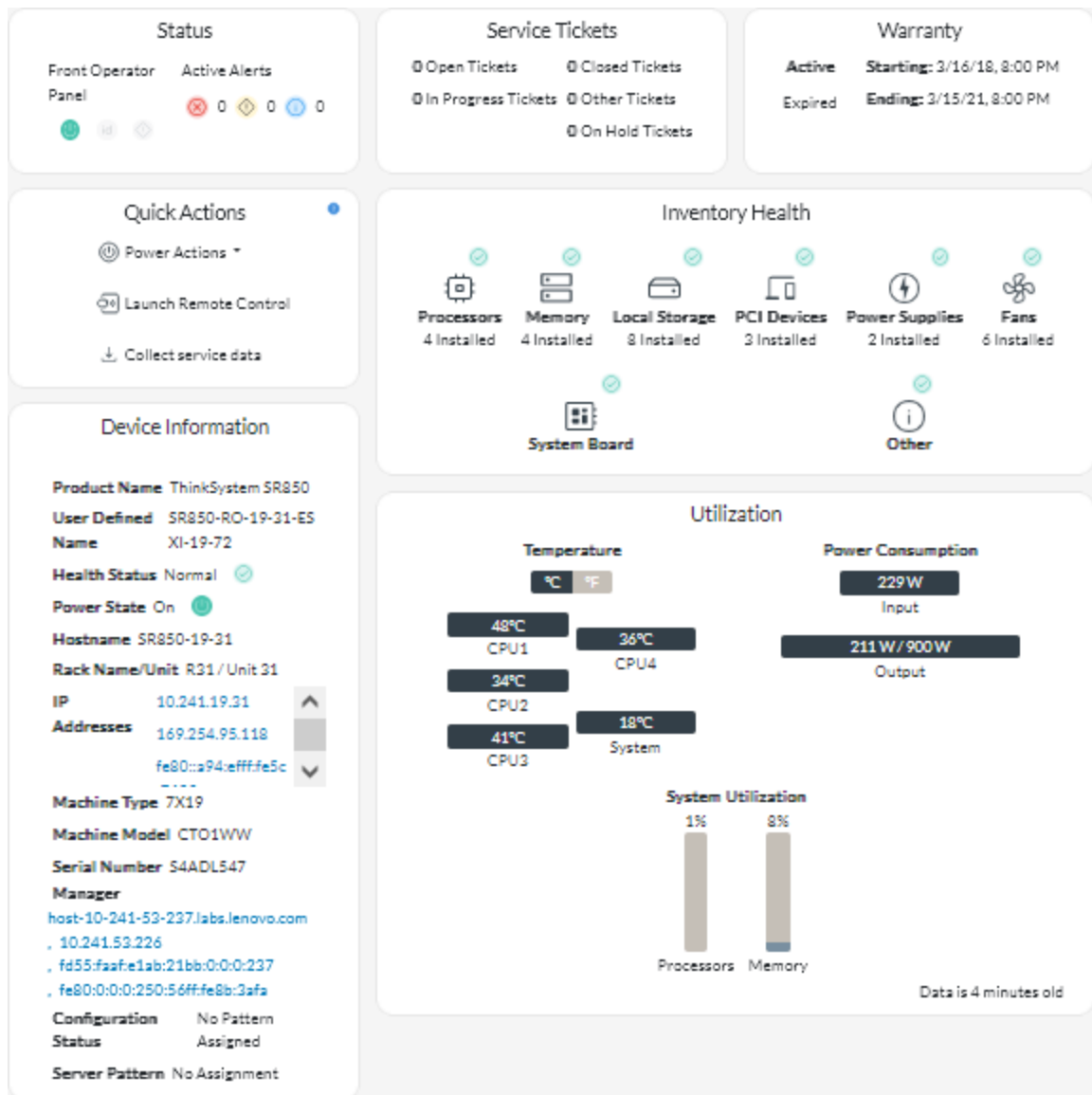
Viewing device details

You can view detailed information about each device, including the overall summary of device health and status, inventory, alerts and events, system metrics, and firmware.

Procedure

To view the details for a device, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Resources** (⊙), and then click the device type to display a card with a tabular view of all managed devices of that type.
- Step 2. Click the row for the device to display the device summary cards for that device.



Step 3. Complete one or more of the following actions.

The details on each card might vary depending on the device type.




- Click **Summary** to view an overall summary of the device, including device information, inventory, health, OS information, system metrics, service tickets, and warranty. This page also includes the **Quick Actions** card that lists actions that you can perform on the device (such as performing power actions, collect service data, and launching a remote-control session). This page displays the state of each LED on the front operator panel.

– **Power LED**

- **On** (🟢). The device is powered on.
- **Off** (🔴). The device is powered off.

– **Location LED**

- **On** (🟦). The Location LED on the control panel is lit.
- **Blinking** (🟦). The Location LED on the control panel is lit or blinking.

- **Off** (). The Location LED on the control panel is not lit.
- **Fault LED**
 - **On** (). The fault LED on the control panel is lit.
 - **Off** (). The Fault LED on the control panel is not lit.
- Click **Inventory** to view details about hardware components in the device (such as processors, memory modules, drives, power supplies, fans, PCI devices, and system board).

Notes:

- Inventory *is not* supported for these storage devices: ThinkSystem DS2200, Lenovo Storage S2200 and S3200, and Flex System V7000 Storage Node.
- Firmware details *are not* available for these storage devices: ThinkSystem DS4200 and DS6200, and Lenovo Storage DX8200C, DX8200D, and DX8200N.
- Click **Alerts Log** to display the list of active alerts and alert statistics for the device (see [Monitoring active alerts](#)).
- Click **Events Log** to display the list of events for the device (see [Monitoring events](#)).
- Click **Firmware** to display a list of current firmware levels for the device and device components.
- Click **Service** to display information about service-data archives and service tickets for the device.
- Click **Utilization** to display system utilization, temperature, and power metrics over time for ThinkAgile and ThinkSystem devices.
- Click **Advisory** to display a list of online customer advisories, including the abstract and link for each advisory. Click a link to open a webpage with details for that advisory.

After you finish

In addition to displaying summary and detailed information about a device, you can perform the following actions on a device from this page.




- Launch the web interface for the baseboard management controller from the **Summary** tab by clicking the main IP address for the device.
- Launch the web interface for the device from the **Summary** tab by clicking the IP address.
- Launch the web interface for the resource manager that manages the device from the **Summary** tab by clicking the resource manager name or IP address.

Viewing infrastructure resources status and details

You can view status and detailed information for datacenter infrastructure resources (such as PDUs and UPSs) that are managed through a Schneider Electric EcoStruxure IT Expert resource manager.

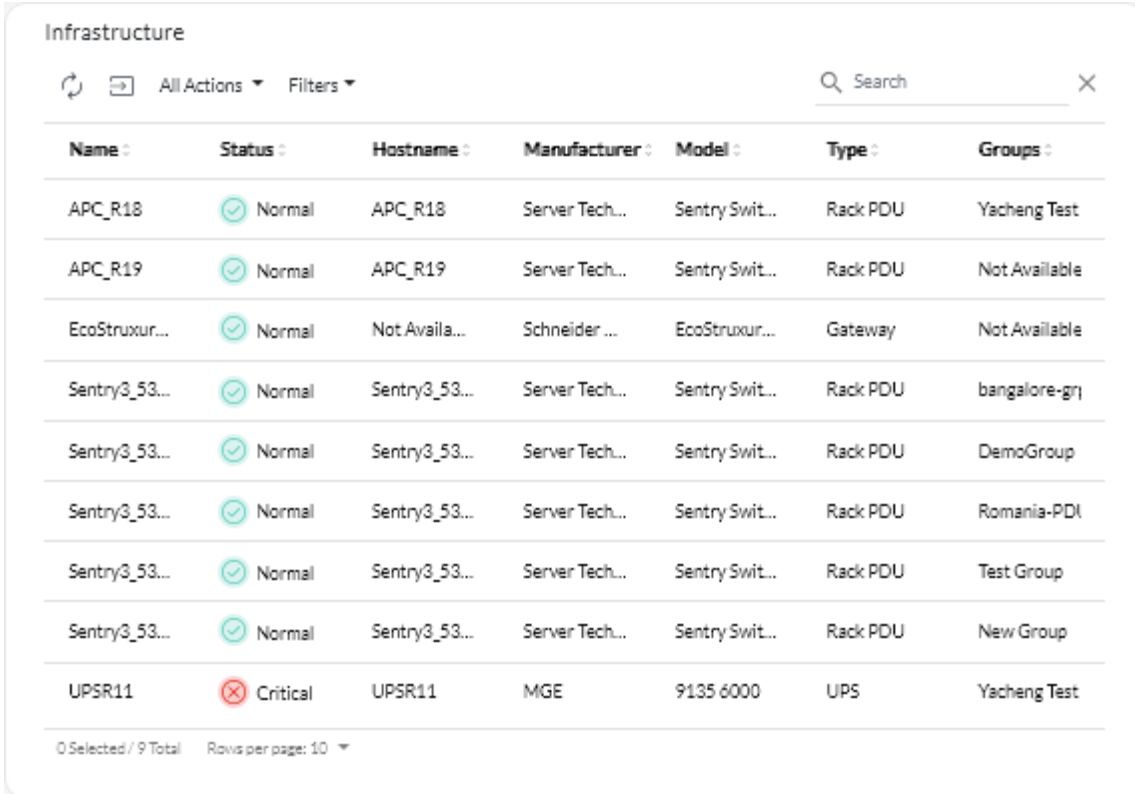
Before you begin

The **Status** column identifies the overall health of an infrastructure resource. The following health states are used. If an infrastructure resources is in an unhealthy state, use the alerts log to help identify and resolve the issues (see [Monitoring active alerts](#)).

- () Normal
- () Warning
- () Critical

Procedure

- **Status for a specific infrastructure resource** To view the status of infrastructure resources, click **Resources** (🔗) → **Infrastructure** from the XClarity Orchestrator menu bar to display the Infrastructure card. If an infrastructure resource is in an unhealthy state, use the alerts log to help identify and resolve the issues (see [Monitoring active alerts](#)).



The screenshot shows the 'Infrastructure' card in the XClarity Orchestrator. It features a table with columns for Name, Status, Hostname, Manufacturer, Model, Type, and Groups. The table lists nine resources, with the last one, UPSR11, in a 'Critical' state. The interface includes a search bar, a refresh button, and a filter dropdown.

Name	Status	Hostname	Manufacturer	Model	Type	Groups
APC_R18	Normal	APC_R18	Server Tech...	Sentry Swit...	Rack PDU	Yacheng Test
APC_R19	Normal	APC_R19	Server Tech...	Sentry Swit...	Rack PDU	Not Available
EcoStruxur...	Normal	Not Availa...	Schneider ...	EcoStruxur...	Gateway	Not Available
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	bangalore-grj
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	DemoGroup
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	Romania-PDI
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	Test Group
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	New Group
UPSR11	Critical	UPSR11	MGE	9135 6000	UPS	Yacheng Test

- **Details for a specific infrastructure resource**

1. From the XClarity Orchestrator menu bar, click **Resources** (🔗) → **Infrastructure** to display the Infrastructure card.
2. Click the row for the infrastructure resource to display the summary card for that resource.
3. Complete one or more of the following actions.
 - Click **Summary** to view an overall summary of the resource, including device information, and status.
 - Click **Alerts Log** to display the list of active alerts and alert statistics for the resource (see [Monitoring active alerts](#)).
 - Click **Events Log** to display the list of events for the resource (see [Monitoring events](#)).
 - Click **Sensors** to display the list of sensors in the resource. You can determine the latest measurement of sensor from the Sensors card, or you can select one or more sensors and then click the **Graph** icon (📊) to view line graphs over time for each selected sensor. Sensors with the same unit (such as watts or amps) are plotted on the same graph.

Note: Schneider Electric EcoStruxure IT Expert collects sensor data every 5 minutes, and XClarity Orchestrator synchronizes this data every hour. Currently, XClarity Orchestrator saves only the last 60 minutes of data.

After you finish

In addition to displaying summary and detailed information about an infrastructure resource, you can perform the following actions from this page.

- Launch the web interface for certain infrastructure resources from the **Summary** tab by clicking the IP address for the resource.

Monitoring jobs

Jobs are long-running tasks that run in the background. You can view a log of all jobs that are started by Lenovo XClarity Orchestrator.

About this task


If a long-running task targets multiple resources, a separate job is created for each resource.

You can see the status and details about each job in the jobs log. The jobs 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.

Note: Jobs that are running for more than 24 hours are stopped and placed in the Expired state.




Procedure

To view jobs, complete one or more of the following steps.

- **View all jobs** Click **Monitoring**  → **Jobs** from the XClarity Orchestrator menu bar to display the Jobs card. This card lists information about each job, including the status, progress, start and end timestamps, and target resource.

Jobs

Jobs are longer running tasks performed against one or more target systems. You can choose to delete a job or view its details.




 All Actions ▾ Filters ▾ Q Search

<input type="checkbox"/>	Job name	Status	Progress	Start time	Complete t	Target	Category	Created by
<input type="checkbox"/>	Assign po	✓ Comple	100%	Oct 5, 20	Oct 5, 20	Not Av...	Updates	Orches...
<input type="checkbox"/>	Assign po	✓ Comple	100%	Oct 5, 20	Oct 5, 20	Not Av...	Updates	Orches...
<input type="checkbox"/>	Assign po	✓ Comple	100%	Oct 5, 20	Oct 5, 20	Not Av...	Updates	Orches...
<input type="checkbox"/>	Assign po	✓ Comple	100%	Oct 5, 20	Oct 5, 20	Not Av...	Updates	Orches...
<input type="checkbox"/>	Assign po	✓ Comple	100%	Oct 5, 20	Oct 5, 20	Not Av...	Updates	Orches...
<input type="checkbox"/>	Process s	✗ Aborted	100%	Oct 5, 20	Oct 5, 20	SN#Y0...	Service	Orches...
<input type="checkbox"/>	Process s	✗ Aborted	100%	Oct 4, 20	Oct 4, 20	SN#Y0...	Service	Orches...
<input type="checkbox"/>	Process s	✗ Aborted	100%	Oct 4, 20	Oct 4, 20	SN#Y0...	Service	Orches...
<input type="checkbox"/>	Process s	✗ Aborted	100%	Oct 4, 20	Oct 4, 20	SN#Y0...	Service	Orches...
<input type="checkbox"/>	Downloa	✓ Comple	100%	Oct 4, 20	Oct 4, 20	XClarit...	Updates	Orches...

0 Selected / 15 Total Rows per page: 10 ⏪ < 1 2 > ⏩

To view detailed information about a job, click the row for that job in the table. Cards are displayed that lists information about each subtask in the job (including the status, progress, start and end timestamps, target devices, and jobs log).

Import OS Image VMware-ESXi-8.0.0-20037389-LNV-20220711.iso

🔄 ☰ 📄 All Actions ▾ Filters ▾ 🔍 Search ✕

Job name	Status	Progress	Start time	Complete time	Target
Import OS Image	● Stopped Wit	<div style="width: 100%; background-color: #007bff; height: 10px;"></div> 100%	Oct 5, 2022, 10:1	Oct 5, 2022, 10:1	XClarity Orche...

1 Total Rows per page: 10 ▾

Logs for Import OS Image VMware-ESXi-8.0.0-20037389-LNV-20220711.iso

🔄 ☰ All Actions ▾ Filters ▾ 🔍 Search ✕

Message	Severity	Timestamp
Validating the payload file	i Informational	Oct 5, 2022, 10:18:02 AM
Checking if the payload file already exis...	i Informational	Oct 5, 2022, 10:18:02 AM
Checking if the payload file is a support...	i Informational	Oct 5, 2022, 10:18:02 AM
An error occurred during the execution...	i Informational	Oct 5, 2022, 10:18:03 AM

4 Total Rows per page: 10 ▾

After you finish

You can perform the following actions from the Jobs card.

- Delete a *completed* or *expired* job or subtask from the jobs log by selecting the job or subtask and clicking the **Delete** (🗑️) icon.

Monitoring active alerts

Alerts are hardware or orchestrator event that require investigation and user action. Lenovo XClarity Orchestrator polls the resource managers asynchronously and displays alerts that are received from those managers.

About this task

There is no limit to the number of active alerts that are stored in the local repository.

From the Alerts card, you can view a list of all active alerts.

Alerts

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

All Actions ▾ Filters ▾ X

	Date and Ti	Severity	Alert	Resource	Serviceabili	Resource T ₁	Source Type	Groups
<input type="checkbox"/>	10/5/2...	W...	Hot air ex	SN#Y0...	No...	Chassis	Device	Not Availi
<input type="checkbox"/>	10/5/2...	W...	The conn	XClarit...	No...	Chassis	Manage...	Not Availi
<input type="checkbox"/>	10/5/2...	W...	The conn	XClarit...	No...	Chassis	Manage...	Not Availi
<input type="checkbox"/>	10/5/2...	W...	The conn	XClarit...	No...	Switch	Manage...	Not Availi
<input type="checkbox"/>	10/5/2...	W...	The conn	XClarit...	No...	Switch	Manage...	Not Availi
<input type="checkbox"/>	10/5/2...	W...	The conn	XClarit...	No...	Switch	Manage...	Not Availi
<input type="checkbox"/>	10/5/2...	W...	The conn	XClarit...	No...	Switch	Manage...	Not Availi
<input type="checkbox"/>	10/5/2...	W...	The conn	XClarit...	No...	Switch	Manage...	Not Availi
<input type="checkbox"/>	10/5/2...	W...	The conn	XClarit...	No...	Switch	Manage...	Not Availi
<input type="checkbox"/>	10/5/2...	W...	The conn	XClarit...	No...	Switch	Manage...	Not Availi

352 Total Rows per page: 10 ▾ 1 2 3 4 5 >

The **Severity** column identifies the severity of the alert. The following severities are used.

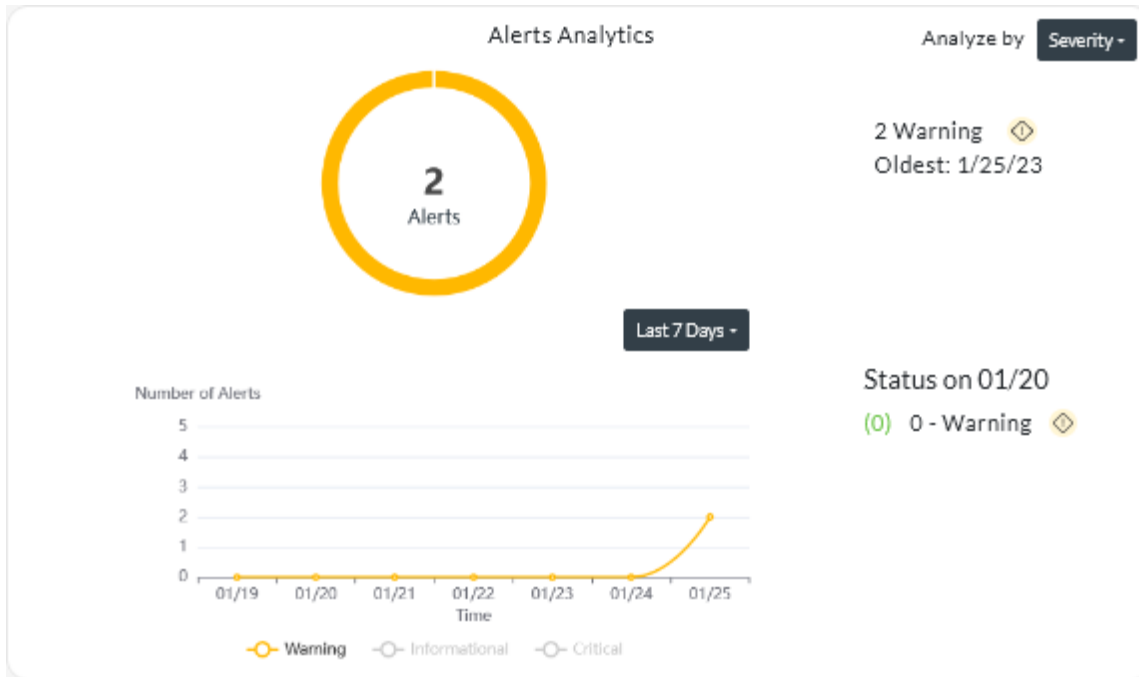
- **Informational**. No action is required.
- **Warning**. Action can be deferred, or no action is required.
- **Critical**. Immediate action is required.

The **Serviceability** column identifies whether the device requires service and who typically performs that service. The following serviceability types are used.

- **None**. The alert is informational and does not require service.
- **User**. Take appropriate recovery action to resolve the issue.
- **Support**. If Call Home is enabled for XClarity Orchestrator or for the resource manager that manages the associated device, the alert is typically submitted to Lenovo Support Center unless an open service ticket for the same alert ID already exists for the device (see [Setting up automatic problem notification to Lenovo Support \(Call Home\)](#) in the XClarity Orchestrator online documentation).

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

If active alerts exist, alert statistics are displayed in the Alerts Analytics card. You can view alert statistics by severity, source, resource, and serviceability for the current day and over a specific period of time (see [Analyzing active alerts](#)).



Procedure

To view active alerts, complete one or more of the following steps.

- **View all active alerts** Click **Monitoring** (📊) → **Alerts** from the XClarity Orchestrator menu bar to display the Alerts card.

To view information about a specific alert, click the description in the **Alert** column. A pop-up is displayed with information about the source of the alert, explanation, and recovery actions.

- **View active alerts for a specific device**
 1. From the XClarity Orchestrator menu bar, click **Resources** (📁) and then click the device type to display a card with a tabular view of all managed devices of that type.
 2. Click the row for a device to display the device summary cards for that device.
 3. Click **Alerts Log** to display the list of active alerts for the device on the Alerts Analytics card. To view information about a specific alert, click the description in the **Alert** column. A pop-up is displayed with information about the source of the alert, explanation, and recovery actions.

Monitoring events

From Lenovo XClarity Orchestrator, you have access to a historical list of all resource and audit events.

Learn more:  [How to monitor specific device events](#)

About this task

A *resource event* identifies a hardware or orchestrator condition that occurred on a managed device, resource manager, or XClarity Orchestrator. You can use these events to track and analyze hardware and orchestrator-server related issues.

An *audit event* is a record of user activities that were performed from a resource manager or XClarity Orchestrator. You can use these audit events to track and analyze authentication-related issues.

The event log contains both resource and audit events. It can contain a maximum of 100,000 events from all sources. A maximum of 50,000 events can be from a single resource manager and its managed devices. A maximum of 1,000 events can be from a single managed device. When the maximum number of events is reached, the oldest event is discarded when the next event is received.

The **Severity** column identifies the severity of the event. The following severities are used.

- (i) **Informational**. No action is required.
- (⚠) **Warning**. Action can be deferred, or no action is required.
- (⊗) **Critical**. Immediate action is required.

The **Serviceability** column identifies whether the device requires service and who typically performs that service. The following serviceability types are used.

- **None**. The alert is informational and does not require service.
- (👤) **User**. Take appropriate recovery action to resolve the issue.
- (🛠) **Support**. If Call Home is enabled for XClarity Orchestrator or for the resource manager that manages the associated device, the alert is typically submitted to Lenovo Support Center unless an open service ticket for the same alert ID already exists for the device (see [Setting up automatic problem notification to Lenovo Support \(Call Home\)](#) in the XClarity Orchestrator online documentation).

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

Procedure

To view events, complete one or more of the following steps.

- **View all resource or audit events** Click **Monitoring** (📁) → **Events** from the XClarity Orchestrator menu bar to display the Events card. Then, click the **Resource Events** or **Audit Events** tab to the view log entries.

Events

The Event log provides a history of hardware and management conditions that have been detected (resource events) and an audit trail of user actions (audit events).

Resource Events **Audit Events**

All Actions ▾ Filters ▾

	Date and Tim	Severity :	Event :	Resource :	Serviceability	Resource Typ	Groups :
	10/5/22, ...	Info...	Power supp	SN#Y031Bf	None	Chassis	Not Availab
	10/5/22, ...	Info...	Failed to dis	IO Module :	None	Switch	Not Availab
	10/5/22, ...	Warn...	The device l	Not Availab	None	Not Availab	Not Availab
	10/5/22, ...	Warn...	A warning a	Not Availab	None	Not Availab	Not Availab
	10/5/22, ...	Warn...	Power supp	SN#Y031Bf	Servi...	Chassis	Not Availab
	10/5/22, ...	Info...	Power supp	SN#Y031Bf	None	Chassis	Not Availab
	10/5/22, ...	Warn...	Power supp	SN#Y031Bf	Servi...	Chassis	Not Availab
	10/5/22, ...	Info...	Failed to dis	IO Module :	None	Switch	Not Availab
	10/5/22, ...	Warn...	The device l	Not Availab	None	Not Availab	Not Availab
	10/5/22, ...	Warn...	A warning a	Not Availab	None	Not Availab	Not Availab

13908 Total Rows per page: 10 ▾ 1 2 3 4 5

- **View resource or audit events for a specific device**

1. Click **Resources** (🔍) from the XClarity Orchestrator menu bar, and then click the device type to display a card with a tabular view of all managed devices of that type.
2. Click the row for a device to display the device summary cards for that device.
3. Click the **Events log** tab to display the Events page for that device.

Excluding alerts and events

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

About this task

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

When you exclude an event that has an associated alert, that alert is also excluded.

Procedure

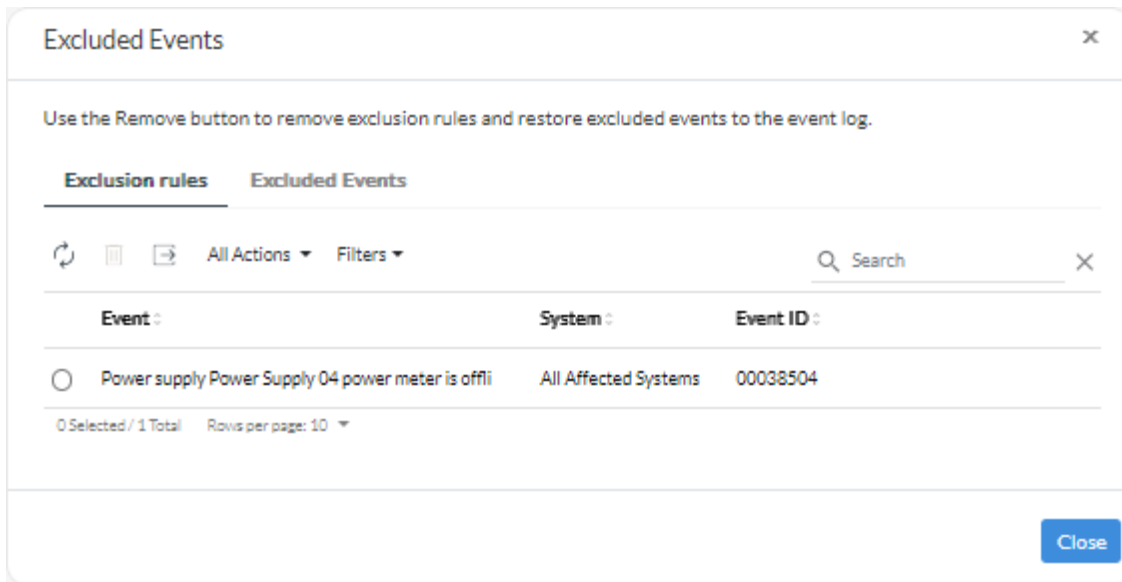
Complete the following steps to exclude alerts and events.

- Step 1. From the XClarity Orchestrator menu bar, click **Monitoring** (📊) → **Alerts** or **Monitoring** (📊) → **Events** to display the Alerts or Events card.
- Step 2. Select the alerts or events to be excluded, and click the **Exclude** icon (🗑️). The Exclude alerts or Exclude events dialog is displayed.
- Step 3. Select one of the following options.
 - **Exclude selected events from all devices.** Excludes the selected events from all managed devices.
 - **Exclude events only from devices 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, XClarity Orchestrator creates exclusion rules based on information that you provide.

- View a list of exclusion rules and excluded events and alerts by clicking the Show **View Exclusions** icon (🗑️) to display the Excluded alerts or Excluded events dialog. Click the **Exclusion Rules** tab to view the exclusion rules, or click the **Excluded alerts** or **Excluded Events** tab to view excluded alerts or events.



- Restore events that have been excluded in the logs by removing the appropriate exclusion rule. To remove an exclusion rule, click the **View Exclusions** icon (🗑️) to display the Excluded alerts or Excluded events dialog, select the exclusion rules to restore, and click the **Delete** icon (🗑️).

Forwarding event, inventory, and metric data

You can forward event, inventory, and metric data from Lenovo XClarity Orchestrator to external applications, which you can use to monitor and analyze data.

About this task

Events data

XClarity Orchestrator can forward events that occur in your environment to external tools, based on criteria (filters) that you specify. Every generated event is monitored to see if it matches the criteria. If it matches, the event is forwarded to the specified location using the indicated protocol.

XClarity Orchestrator supports forwarding event data to the following external tools.

- **Email.** Event data is forwarded to one or more email addresses using SMTP.
- **Intelligent Insights.** Event data is forwarded in a predefined format to SAP Data Intelligence. You can then use SAP Data Intelligence for managing and monitoring the event data.
- **REST.** Event data is forwarded over the network to a REST Web Service.
- **Syslog.** Event data is forwarded over the network to a central log server where native tools can be used to monitor the syslog.

XClarity Orchestrator uses *global filters* to define the scope of event data to be forwarded. You can create event filters to forward only events with specific properties, including event codes, event classes, event severities, and service types. You can also create device filters forward only events that are generated by specific devices.

Inventory and events data

XClarity Orchestrator can forward all inventory and event data for all devices to external applications, which you can use to monitor and analyze data.

- **Splunk.** Event data is forwarded in a predefined format to a Splunk application. You can then use Splunk to create graphs and charts based on event data. You can define multiple Splunk configurations; however, XClarity Orchestrator can forward events to only one Splunk configuration. Therefore, only one Splunk configuration can be enabled at a time.

Metrics data

XClarity Orchestrator can forward metric data that it collects about managed devices to the following external tool.

- **TruScale Infrastructure Services.** Metric data is forwarded in a predefined format to the Lenovo TruScale Infrastructure Services. You can then use TruScale Infrastructure Services for managing and monitoring the metric data.

Attention: Information about TruScale Infrastructure Services forwarder is intended only for Lenovo Service representatives.

You can define multiple TruScale Infrastructure Services forwarders; however, XClarity Orchestrator can forward metric data to only one TruScale Infrastructure Services forwarder. Therefore, only one TruScale Infrastructure Services forwarder can be enabled at a time.

Learn more:  [Get to Know Lenovo TruScale Infrastructure Services](#)

Creating data-forwarding filters

You can define common *data-forwarding filters* that can be used by multiple forwarders to trigger forwarding data that match specific criteria.

About this task

You can create the following types of filters.

- *Events filters* forward events that match specific event codes or properties (such as event classes, event severities, and service types)
 - All codes and properties apply to all event sources.
 - If no class properties are selected, all class properties are matched.
 - If no serviceable properties are selected, all serviceable properties are matched.

- If no severity properties are selected, all severity properties are matched.
- If no event code is specified, all event codes are matched.
- *Resource filters* forward data that is generated by specific resources (XClarity Orchestrator, resource managers, and devices). You can choose a subset of resources by selecting one or more resource groups.
 - If a resource type is disabled, no data from that resource type is forwarded.
 - If a resource type is enabled, and no groups are selected, all data from that resource type is forwarded.
 - If a resource type is enabled, and one or more groups are selected, only data that is generated by the resources in selected groups are forwarded.

You can reuse event and resource filters in multiple forwarders; however, you can add at most one event filter and one resource filter to each forwarder.

Procedure

To create a data-forwarding filter, complete one of the following steps depending on the type of filter that you want to create.

- **Event filters**

1. From the XClarity Orchestrator menu bar, click **Monitoring** (📊) → **Forwarding**, and then click **Data Forwarder Filters** in the left navigation to display the Data Forwarder Filters card.

Name ~	Creator :	Privacy :	Type :	Description :
<input type="radio"/> Email_forwarder	userid	Private	Resource Filter	Not Available

0 Selected / 1 Total Rows per page: 10 ▾

2. Click the **Create** icon (⊕) to display the Create Data Forwarder Filter dialog.

3. Specify the filter name and optional description.
4. Select **Event filter** as the filter type.
5. Select the privacy type.
 - **Private**. Only the user that created the filter can use the filter.
 - **Public**. Any user can use the filter.
6. Choose event properties or event codes as criteria for this filter.
7. Click **Rules**, and select the criteria for this filter based on the criteria type that you selected in the previous step.
 - **Match events by properties**. Select one or more severity, serviceability, and class properties. Only events that match the selected properties are forwarded. For example, if you choose warning and critical severities, and adapter and memory classes, then event data is forwarded for only warning memory events, critical memory events, warning adapter events, and critical adapter events, regardless of the serviceability of the event. If you select only user serviceability, then event data is forwarded for only events that are user serviceable, regardless of the severity or class.

Notes:

- If you do not select a class property, all class properties are matched.
- If you do not select a serviceable property, all serviceable properties are matched
- If you do not select a severity property, all severity properties are matched.
- **Match events by code**. Enter an event code that you want to filter, and then click the **Add** icon (+) to add the event code to the list. Repeat for each event code that you want to add. You can delete an event code by clicking the **Delete** icon (🗑️) next to the specific code. Only events that match one of the listed event codes are forwarded.



You can specify a full or partial event code. For example, FQXXOCO0001I matches the specific event, FQXXOSE matches all XClarity Orchestrator security events, and CO001 matches all events that contain those characters.


If you do not specify an event code, all event codes are matched.

To find a list of available event codes, see [Event and alert messages](#) in the XClarity Orchestrator online documentation.


8. Click **Create** to create the filter. The filter is added to the table.

- **Resource filters**

1. From the XClarity Orchestrator menu bar, click **Monitoring**  → **Forwarding**, and then click **Data Forwarder Filters** in the left navigation to display the Data Forwarder Filters card.
2. Click the **Create** icon  to display the Create Data Forwarder Filter dialog.
3. Specify the filter name and optional description.
4. Select **Resource filter** as the filter type.
5. Select the privacy type.
 - **Private**. Only the user that created the filter can use the filter.
 - **Public**. Any user can use the filter.
6. Click **Resources**, and select the source of events for this filter.
 - **Match any XClarity Orchestrator events**. Forwards events that are generated by this XClarity Orchestrator. This option is disabled by default.
 - **Match any resource manager events**. Forwards events that are generated by a resource manager. This option is disabled by default.
 - If you disable this option, events are not forwarded from any resource managers.
 - If you enable this option but do not select any manager groups, events that are generated by all resource managers are forwarded.
 - If you enable this option and select one or more manager groups, events that are generated by only resource managers in the selected groups are forwarded.

Tip: You can create manager groups from this card by clicking the **Create** icon .


- **Match any device events**. Forwards events that are generated by a device. This option is enabled by default.
 - If you disable this option, events are not forwarded from any devices.
 - If you enable this option but do not select any device groups, events that are generated by all devices are forwarded.
 - If you enable this option and select one or more device groups, events that are generated by only devices in the selected groups are forwarded.

Tip: You can create device groups from this card by clicking the **Create** icon .

7. Click **Create** to create the filter. The filter is added to the table.

After you finish

You can perform the following action from the Data Forwarder Filters card.

- Remove a selected filter by clicking the **Delete** icon . You cannot delete a filter that is assigned to a forwarder.

Forwarding events to SAP Data Intelligence

You can configure Lenovo XClarity Orchestrator to forward events to SAP Data Intelligence (Intelligent Insights).

Before you begin

Attention: The connection between XClarity Orchestrator and SAP Data Intelligence uses encrypted transport but does not verify the TLS certificate of the remote system.

About this task

If resource-based access control is enabled, data is forwarded for only those resources that you can access using access-control lists. If you are not a member of a group to which the predefined **Supervisor** role is assigned, you must assign one or more access-control lists to the forwarders that you create. If you want to send data for all resources that you can access, select all access-control lists that are associated that are available to you. If you are a member of a group to which the predefined **Supervisor** role is assigned, you can choose to send data for all resources, or you can choose to assign access control lists to limit the resources.

You cannot filter data that is forwarded to SAP Data Intelligence.

The following example shows the default format for data that is forwarded to SAP Data Intelligence. Words between double square brackets are attributes that are replaced with actual values when data is forwarded.

```
{ "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]" }
```

Procedure

To forward event data to SAP Data Intelligence, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Monitoring** (🔍) → **Forwarding**, and then click **Data Forwarders** in the left navigation to display the Data Forwarders card.
- Step 2. Click the **Create** icon (+) to display the Create Data Forwarder dialog.
- Step 3. Specify the forwarder name and optional description.
- Step 4. Choose to enable or disable the forwarder by clicking the **State** toggle.
- Step 5. Select **Intelligent Insights** as the forwarder type.
- Step 6. Click **Configuration**, and fill in the protocol-specific information.
 - Enter the hostname or IP address of SAP Data Intelligence.
 - Enter the port to use for forwarding events. The default is 443.
 - Enter the resource path on which the forwarder is to post the events (for example, /rest/test).
 - Select the REST method. This can be one of the following values.
 - **PUT**
 - **POST**
 - Select the protocol to use for forwarding events. This can be one of the following values.
 - **HTTP**
 - **HTTPS**
 - Enter the time-out period (in seconds) for the request. Default is 30 seconds.

- If authentication is required, select one of the following authentication types.
 - **Basic.** Authenticates to the specified server using the specified tenant, user ID, and password.
 - **Token.** Authenticates to the specified server using the specified token header name and value

Step 7. Click **Access Control Lists**, and select one or more access-control lists that you want to associated with this forwarder.

If resource-based access is enabled, you must select at least one access-control list.

Tip: Users that are members of a group to which the predefined **Supervisor** role is assigned can optionally select **Match Everything** instead of selecting an access control lists so that forwarded data is not restricted.

Step 8. Click **Create** to create the forwarder.

After you finish

You can perform the following actions from the Data Forwarders card.

- Enable or disable a selected forwarder by selecting the toggle in the **State** column
- Modify a selected forwarder by clicking the **Edit** icon (✎).
- Remove a selected forwarder by clicking the **Delete** icon (🗑).

Forwarding events to a REST web service

You can configure Lenovo XClarity Orchestrator to forward specific events to a REST web service.

Before you begin

Attention: A secure connection is not established when forwarding data to this service. Data is sent over a clear text protocol.

About this task

If resource-based access control is enabled, data is forwarded for only those resources that you can access using access-control lists. If you are not a member of a group to which the predefined **Supervisor** role is assigned, you must assign one or more access-control lists to the forwarders that you create. If you want to send data for all resources that you can access, select all access-control lists that are associated that are available to you. If you are a member of a group to which the predefined **Supervisor** role is assigned, you can choose to send data for all resources, or you can choose to assign access control lists to limit the resources.

Common *data-forwarding filters* are used to define the scope of events that you want to forward, based on event codes, event classes, event severities, service types, and resource that generated the event. Ensure that the event and resource filters that you want to use for this forwarder are already created (see [Creating data-forwarding filters](#)).



The following example shows the default format for data that is forwarded to a REST web service. Words between double square brackets are attributes that are replaced with actual values when data is forwarded.

```
{ "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]]\\"}"
```

Procedure

To forward data to a REST web service, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Monitoring**  → **Forwarding**, and then click **Data Forwarders** in the left navigation to display the Data Forwarders card.
- Step 2. Click the **Create** icon  to display the Create Data Forwarder dialog.
- Step 3. Specify the forwarder name and optional description.
- Step 4. Choose to enable or disable the forwarder by clicking the **State** toggle.
- Step 5. Select **REST** as the forwarder type.
- Step 6. Click **Configuration**, and fill in the protocol-specific information.
 - Enter the hostname or IP address of the REST server.
 - Enter the port to use for forwarding events. The default is 80.
 - Enter the resource path on which the forwarder is to post the events (for example, /rest/test).
 - Select the REST method. This can be one of the following values.
 - **PUT**
 - **POST**
 - Select the protocol to use for forwarding events. This can be one of the following values.
 - **HTTP**
 - **HTTPS**
 - Enter the time-out period (in seconds) for the request. Default is 30 seconds.
 - If authentication is required, select one of the following authentication types.
 - **Basic**. Authenticates to the specified server using the specified user ID and password.
 - **Token**. Authenticates to the specified server using the specified token header name and value.
- Step 7. Click **Filters**, and optionally select the filters that you want to use for this forwarder.

You can select at most one event filter and one resource filter.

If you do not select a filter, data is forwarded for all events that are generated by all resources (devices, resource managers, and XClarity Orchestrator).

From this tab, you can also choose to forward excluded event by setting the **Excluded Events** toggle to **Yes**.

- Step 8. Click **Access Control Lists**, and select one or more access-control lists that you want to associated with this forwarder.

If resource-based access is enabled, you must select at least one access-control list.

Tip: Users that are members of a group to which the predefined **Supervisor** role is assigned can optionally select **Match Everything** instead of selecting an access control lists so that forwarded data is not restricted.

Step 9. Click **Create** to create the forwarder.

After you finish

You can perform the following actions from the Data Forwarders card.

- Enable or disable a selected forwarder by selecting the toggle in the **State** column
- Modify a selected forwarder by clicking the **Edit** icon (✎).
- Remove a selected forwarder by clicking the **Delete** icon (🗑).

Forwarding events to an email service using SMTP

You can configure Lenovo XClarity Orchestrator to forward specific events to one or more email addresses using SMTP.

Before you begin

Attention: A secure connection is not established when forwarding data to this service. Data is sent over a clear text protocol.

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 [Forwarding events to a Gmail SMTP service](#).

About this task

If resource-based access control is enabled, data is forwarded for only those resources that you can access using access-control lists. If you are not a member of a group to which the predefined **Supervisor** role is assigned, you must assign one or more access-control lists to the forwarders that you create. If you want to send data for all resources that you can access, select all access-control lists that are associated that are available to you. If you are a member of a group to which the predefined **Supervisor** role is assigned, you can choose to send data for all resources, or you can choose to assign access control lists to limit the resources.

Common *data-forwarding filters* are used to define the scope of events that you want to forward, based on event codes, event classes, event severities, service types, and resource that generated the event. Ensure that the event and resource filters that you want to use for this forwarder are already created (see [Creating data-forwarding filters](#)).

The following example shows the default format for data that is forwarded to an email service. Words between double square brackets are attributes that are replaced with actual values when data is forwarded.

Email subject

Event Forwarding

Email body

```
{
  "groups": [],
  "acts": [],
  "local": null,
  "eventID": "FQXHMEMO216I",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
```

```

"msg": "The event forwarder destination cannot be reached. Therefore new events are not being
        forwarded.",
"description": "The event forwarder destination cannot be reached. Therefore new events are not
        being forwarded.",
"userAction": "Look in the online documentation to determinate more information about this event
        based on the eventID. At the moment the orchestrator server can not offer more
        information.",
"recoveryURL": null,
"flags": [],
"userid": null,
"action": "None",
"eventClass": "System",
"args": [],
"service": "None",
"xcaUUID": "23C87F0A2CB6491097489193447A655C",
"managerID": "23C87F0A2CB6491097489193447A655C",
"failFRUNumbers": null,
"failFRUSNs": null,
"failFRUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
"msgID": null,
"timeStamp": "2021-03-12T18:32:14.000Z",
"eventDate": "2021-03-12T18:32:14Z",
"commonEventID": "FQXHMEM0216I",
"sequenceNumber": "17934247",
"details": null,
"device": {
    "name": "xhmc194.labs.lenovo.com",
    "mtm": null,
    "serialNumber": null
},
"resourceType": "XClarity Administrator",
"componentType": "XClarity Administrator",
"sourceType": "Management",
"resourceName": "xhmc194.labs.lenovo.com",
"fruType": "other",
"ipAddress": "10.243.2.107",
"_id": 252349
}

```

Procedure

To forward data to an email service using SMTP, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Monitoring** (🔍) → **Forwarding**, and then click **Data Forwarders** in the left navigation to display the Data Forwarders card.
- Step 2. Click the **Create** icon (+) to display the Create Data Forwarder dialog.
- Step 3. Specify the forwarder name and optional description.
- Step 4. Choose to enable or disable the forwarder by clicking the **State** toggle.
- Step 5. Select **Email** as the forwarder type.
- Step 6. Click **Configuration**, and fill in the protocol-specific information.
 - Enter the hostname or IP address of the SMTP server.
 - 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.

- **Optional:** Enter the email address for the sender of the email (for example, john@company.com) and the sender domain. If you do not specify an email address, the sender address is LXCO.
<source_identifier>@<smtp_host> by default.

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

Notes:

- If you set up your SMTP server to require a hostname to forward email, and you do not set up a hostname for XClarity Orchestrator, it is possible that the SMTP server might reject forwarded events. If XClarity Orchestrator 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 (LXCO.<source_identifier>@{smtp_host}) is rejected. In this case, you must specify at least a domain name in the **From User** field.
- To establish a secure connection to the SMTP server, select one of the following connection types.
 - **SSL.** Uses the SSL protocol to form a secure communication.
 - **STARTTLS.** Uses the TLS protocol to form a secure communication over an unsecure channel.

If one of these connection types is selected, XClarity Orchestrator attempts to download and import the SMTP server’s certificate to the XClarity Orchestrator truststore. You are prompted to accept this certificate.
- 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.
 - **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 7. Click **Filters**, and optionally select the filters that you want to use for this forwarder.

You can select at most one event filter and one resource filter.

If you do not select a filter, data is forwarded for all events that are generated by all resources (devices, resource managers, and XClarity Orchestrator).

From this tab, you can also choose to forward excluded event by setting the **Excluded Events** toggle to **Yes**.

Step 8. Click **Access Control Lists**, and select one or more access-control lists that you want to associated with this forwarder.

If resource-based access is enabled, you must select at least one access-control list.

Tip: Users that are members of a group to which the predefined **Supervisor** role is assigned can optionally select **Match Everything** instead of selecting an access control lists so that forwarded data is not restricted.

Step 9. Click **Create** to create the forwarder.

After you finish

You can perform the following actions from the Data Forwarders card.

- Enable or disable a selected forwarder by selecting the toggle in the **State** column
- Modify a selected forwarder by clicking the **Edit** icon (✎).
- Remove a selected forwarder by clicking the **Delete** icon (🗑).

Forwarding events to a Gmail SMTP service

You can setup Lenovo XClarity Orchestrator to forward 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.” Click **GMAIL API** in the search results.
 - e. Click on **Enable**.
 - f. Click the **Credentials** tab.
 - g. Click **OAuth consent screen**.
 - h. Type a name in the **Product name shown to users** field, and click **Save**.
 - i. Click **Create credentials** → **OAuth client ID**.
 - j. Select **Other**, and enter a name.
 - k. Click **Create**. The OAuth client dialog is displayed with your client ID and client secret.
 - l. Record the client ID and client secret for later use.
 - m. 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=884243132302-458elfqjiebpvdmvdackp6elip8kl63.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=884243132302-458elfqjbiepudmvdackp6elip8kl63.apps.googleusercontent.com&redirect_uri=urn%3Aietf%3Awww%3Aoauth%3A2.0%3Ahttps%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.CjHXAsyoH9GuCZutgIDxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_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 Orchestrator with the new token.

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

Parameter	Value
Host	smtp.gmail.com
Port	587
SSL	Clear
STARTTLS	Select
Authentication	OAuth2
User	Valid Gmail email address
Token	Security token
From Address	(optional)

Forwarding inventory and events to Splunk

You can configure Lenovo XClarity Orchestrator to forward inventory and events in a predefined format to a Splunk application. You can then use Splunk to create graphs and charts based on that data to help analyze conditions and predict problems in your environment.

Before you begin

Attention: A secure connection is not established when forwarding data to this service. Data is sent over a clear text protocol.

About this task

Splunk is a tool for data-center operators to track and analyze event logs and other data. Lenovo provides an XClarity Orchestrator app for Splunk that analyzes events that are forwarded by XClarity Orchestrator and presents the analysis in a set of dashboards. You can monitor the dashboards in this app as an aid to find potential problems in your environment so that you can react before serious issues occur. For more information, see [XClarity Orchestrator app for Splunk User's Guide](#) in the XClarity Orchestrator online documentation.

You can define multiple Splunk configurations; however, XClarity Orchestrator can forward events to only one Splunk instance. Therefore, only one Splunk configuration can be enabled at a time.

If resource-based access control is enabled, data is forwarded for only those resources that you can access using access-control lists. If you are not a member of a group to which the predefined **Supervisor** role is assigned, you must assign one or more access-control lists to the forwarders that you create. If you want to send data for all resources that you can access, select all access-control lists that are associated that are available to you. If you are a member of a group to which the predefined **Supervisor** role is assigned, you can choose to send data for all resources, or you can choose to assign access control lists to limit the resources.

You cannot filter data that is forwarded to Splunk applications.

Procedure

To forward inventory and event data to a Splunk application, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Monitoring** (📊) → **Forwarding**, and then click **Data Forwarders** in the left navigation to display the Data Forwarders card.
- Step 2. Click the **Create** icon (+) to display the Create Data Forwarder dialog.
- Step 3. Specify the forwarder name and optional description.
- Step 4. Choose to enable or disable the forwarder by clicking the **State** toggle.
- Step 5. Select **Splunk** as the forwarder type.
- Step 6. Click **Configuration**, and fill in the protocol-specific information.
 - Enter the hostname or IP address of the Splunk application.
 - Specify the user account and password to use to log in to the Splunk service.
 - Specify the REST API and data port numbers to use to connect to the Splunk service.
 - Specify one or more HTTP event-collector indices. The default index is **lxco**.
 - Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- Step 7. Click **Access Control Lists**, and select one or more access-control lists that you want to associated with this forwarder.

If resource-based access is enabled, you must select at least one access-control list.

Tip: Users that are members of a group to which the predefined **Supervisor** role is assigned can optionally select **Match Everything** instead of selecting an access control lists so that forwarded data is not restricted.

- Step 8. Click **Create** to create the forwarder.

After you finish

You can perform the following actions from the Data Forwarders card.

- Enable or disable a selected forwarder by selecting the toggle in the **State** column

- Modify a selected forwarder by clicking the **Edit** icon (✎).
- Remove a selected forwarder by clicking the **Delete** icon (🗑).

Forwarding events to a syslog

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

Before you begin

Attention: A secure connection is not established when forwarding data to this service. Data is sent over a clear text protocol.

About this task

If resource-based access control is enabled, data is forwarded for only those resources that you can access using access-control lists. If you are not a member of a group to which the predefined **Supervisor** role is assigned, you must assign one or more access-control lists to the forwarders that you create. If you want to send data for all resources that you can access, select all access-control lists that are associated that are available to you. If you are a member of a group to which the predefined **Supervisor** role is assigned, you can choose to send data for all resources, or you can choose to assign access control lists to limit the resources.

Common *data-forwarding filters* are used to define the scope of events that you want to forward, based on event codes, event classes, event severities, service types, and resource that generated the event. Ensure that the event and resource filters that you want to use for this forwarder are already created (see [Creating data-forwarding filters](#)).

The following example shows the default format for data that is forwarded to a syslog. Words between double square brackets are attributes that are replaced with actual values when data is forwarded.

```
{
  "appl": "LXCO",
  "groups": [],
  "acls": [],
  "local": null,
  "eventID": "FQXHMEM0216I",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "msg": "The event forwarder destination cannot be reached. Therefore new events are not being
        forwarded.",
  "description": "The event forwarder destination cannot be reached. Therefore new events are not
                being forwarded.",
  "userAction": "Look in the online documentation to determinate more information about this event
                based on the eventID. At the moment the orchestrator server can not offer more
                information.",
  "recoveryURL": null,
  "flags": [],
  "userid": null,
  "action": "None",
  "eventClass": "System",
  "args": [],
  "service": "None",
  "lxcaUUID": "23C87F0A2CB6491097489193447A655C",
  "managerID": "23C87F0A2CB6491097489193447A655C",
  "failFRUNumbers": null,
  "failFRUSNs": null,
  "failFRUUUDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]"
}
```

```

"msgID": null,
"timeStamp": "2021-03-12T18:32:14.000Z",
"eventDate": "2021-03-12T18:32:14Z",
"commonEventID": "FQXHMEM0216I",
"sequenceNumber": "17934247",
"details": null,
"device": {
  "name": "xhmc194.labs.lenovo.com",
  "mtm": null,
  "serialNumber": null
},
"resourceType": "XClarity Administrator",
"componentType": "XClarity Administrator",
"sourceType": "Management",
"resourceName": "xhmc194.labs.lenovo.com",
"fruType": "other",
"ipAddress": "10.243.2.107",
"_id": 252349
}

```

Procedure

To forward data to syslog, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Monitoring** (📄) → **Forwarding**, and then click **Data Forwarders** in the left navigation to display the Data Forwarders card.
- Step 2. Click the **Create** icon (+) to display the Create Data Forwarder dialog.
- Step 3. Specify the forwarder name and optional description.
- Step 4. Choose to enable or disable the forwarder by clicking the **State** toggle.
- Step 5. Select **Syslog** as the forwarder type.
- Step 6. Click **Configuration**, and fill in the protocol-specific information.
 - Enter the hostname or IP address of the syslog.
 - 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.
 - **Optional:** 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 7. Click **Filters**, and optionally select the filters that you want to use for this forwarder.

You can select at most one event filter and one resource filter.

If you do not select a filter, data is forwarded for all events that are generated by all resources (devices, resource managers, and XClarity Orchestrator).

From this tab, you can also choose to forward excluded event by setting the **Excluded Events** toggle to **Yes**.

- Step 8. Click **Access Control Lists**, and select one or more access-control lists that you want to associated with this forwarder.

If resource-based access is enabled, you must select at least one access-control list.

Tip: Users that are members of a group to which the predefined **Supervisor** role is assigned can optionally select **Match Everything** instead of selecting an access control lists so that forwarded data is not restricted.

Step 9. Click **Create** to create the forwarder.

After you finish

You can perform the following actions from the Data Forwarders card.

- Enable or disable a selected forwarder by selecting the toggle in the **State** column
- Modify a selected forwarder by clicking the **Edit** icon (✎).
- Remove a selected forwarder by clicking the **Delete** icon (🗑).

Forwarding metrics data to a Lenovo TruScale Infrastructure Services

You can configure Lenovo XClarity Orchestrator to forward metrics (telemetry) data to a Lenovo TruScale Infrastructure Services.

Learn more:  [Get to Know Lenovo TruScale Infrastructure Services](#)

Before you begin

Attention: These configuration steps are intended only for Lenovo Service representatives.

A secure connection is established when forwarding data to TruScale Infrastructure Services.

Ensure that the XClarity Orchestrator is running v1.2.0 or later.

Ensure that the Lenovo XClarity Administrator resource managers that manage the devices for which you want to forward metrics data are running v3.0.0 plus the fix pack or later.

Ensure that the appropriate XClarity Administrator resource managers are connected to XClarity Orchestrator (see [Connecting resource managers](#)).

Ensure that the devices for which you want to forward metrics data are running the latest Lenovo XClarity Controller firmware (see [Applying and activating updates to resource managers](#)).

Ensure that the data and time settings are configured correctly in the following resources.

- XClarity Orchestrator (see [Configuring the date and time](#))
- XClarity Administrator resource manager (see [Setting date and time](#) in the XClarity Administrator online documentation)
- Baseboard management controllers in each device (see [Setting XClarity Controller date and time](#) in the Lenovo XClarity Controller online documentation)

Ensure that the networking settings in XClarity Orchestrator are configured correctly (see [Configuring network settings](#)).

Ensure that metrics data is being collected for the managed devices by viewing the utilization graphs on the device summary page (see [Viewing device details](#)). If metrics data is not displayed, see .

To learn more about Lenovo TruScale Infrastructure Services, see the [TruScale Infrastructure Services website](#).

About this task

You can define multiple Lenovo TruScale Infrastructure Services configurations; however, XClarity Orchestrator can forward events to only one Lenovo TruScale Infrastructure Services instance. Therefore, only one Lenovo TruScale Infrastructure Services configuration can be enabled at a time.

If resource-based access control is enabled, data is forwarded for only those resources that you can access using access-control lists. If you are not a member of a group to which the predefined **Supervisor** role is assigned, you must assign one or more access-control lists to the forwarders that you create. If you want to send data for all resources that you can access, select all access-control lists that are associated that are available to you. If you are a member of a group to which the predefined **Supervisor** role is assigned, you can choose to send data for all resources, or you can choose to assign access control lists to limit the resources.

You cannot filter data that is forwarded to a Lenovo TruScale Infrastructure Services.

The following example shows the default format for data that is forwarded to a Lenovo TruScale Infrastructure Services. Words between double square brackets are attributes that are replaced with actual values when data is forwarded.

```
{ "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]" }
```

Procedure

To forward data to a Lenovo TruScale Infrastructure Services, complete the following steps.

Step 1. Add the trusted SSL certificates that is provided by the Lenovo TruScale Infrastructure Services.

1. From the XClarity Orchestrator menu bar, click XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Security**, and then click **Trusted Certificates** in the left navigation to display the Trusted Certificates card.
2. Click the **Add** icon (⊕) to add a certificate. The Add Certificate dialog is displayed.
3. Copy and paste the certificate data in PEM format.
4. Click **Add**.

Step 2. From the XClarity Orchestrator menu bar, click **Monitoring** (📊) → **Forwarding**, and then click **Data Forwarders** in the left navigation to display the Data Forwarders card.

Step 3. Click the **Create** icon (⊕) to display the Create Data Forwarder dialog.

Step 4. Specify the forwarder name and optional description.

Step 5. Choose to enable or disable the forwarder by clicking the **State** toggle.

Step 6. Select **TruScale Infrastructure Services** as the forwarder type.

Step 7. Click **Configuration**, and fill in the protocol-specific information.

- Enter the hostname or IP address of the TruScale Infrastructure Service.

- Enter the port to use for forwarding events. The default is 9092.
- Optionally enter the frequency, in minutes, when data is pushed. The default is 60 minutes.
- Enter the topic name.
- Enter the time-out period (in seconds) for the request. Default is 300 seconds.

Step 8. Click **Validate Connection** to ensure that a connection can be established based on the configuration.

Attention: Validating the connection might take several minutes to complete. You can close the pop-up message and continue creating the forwarder without disrupting the validation process. When the validation completes, another popup message is displayed to notify you whether the connection is successful.

Step 9. Click **Access Control Lists**, and select one or more access-control lists that you want to associated with this forwarder.

If resource-based access is enabled, you must select at least one access-control list.

Tip: Users that are members of a group to which the predefined **Supervisor** role is assigned can optionally select **Match Everything** instead of selecting an access control lists so that forwarded data is not restricted.

Step 10. Click **Create** to create the forwarder.

After you finish

You can perform the following actions from the Data Forwarders card.

- Enable or disable a selected forwarder by selecting the toggle in the **State** column
- Modify a selected forwarder by clicking the **Edit** icon (✎).
- Remove a selected forwarder by clicking the **Delete** icon (🗑).

Forwarding reports

You can forward reports on a reoccurring basis to one or more email addresses using an SMTP web service.

About this task

A *report* is any data that is presented in tabular form in the user interface. The following reports are currently support.

- Active alerts
- Resource and audit events
- Managed devices (servers, storage, switches, and chassis)
- Device firmware compliance
- Server configuration compliance
- Warranty status for servers
- Active service tickets

Creating forwarder destination configurations

You can define common destination configurations that can be used by multiple report forwarders. The destination identifies where the reports are to be sent.

Procedure

To create a destination configuration for report forwarders, complete the following steps.

Step 1. From the XClarity Orchestrator menu bar, click **Monitoring** (🔍) → **Forwarding**, and then click **Forwarder Destinations** in the left navigation to display the Forwarder Destinations card.

Step 2. Click the **Create** icon (+) to display the Create Forwarder Destinations dialog.

Step 3. Specify the report forwarder name and optional description

Step 4. Select **SMTP** as the destination type.

Step 5. Click **Configuration**, and fill in the protocol-specific information.

- Enter the hostname or IP address of the SMTP (email) server.
- Enter the port to use for the destination. 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.
- **Optional:** Enter the email address for the sender of the email (for example, john@company.com) and the sender domain. If you do not specify an email address, the sender address is LXCO. *{source_identifier}@{smtp_host}* by default.

If you specify only the sender domain, the format of the sender address is *{LXCO_host_name}@{sender_domain}* (for example, XClarity1@company.com).

Notes:

- If you set up your SMTP server to require a hostname to forward email, and you do not set up a hostname for XClarity Orchestrator, it is possible that the SMTP server might reject the email. If XClarity Orchestrator does not have a hostname, the email 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 email.
- If you specify the sender domain, the source does not identify in the sender address. Instead, information about the data source is included in the body of the email, including system name, IP address, machine type/model, and serial number.
- If the SMTP server accepts only emails that are sent by a registered user, the default sender address (LXCO.<source_identifier>@{smtp_host}) is rejected. In this case, you must specify at least a domain name in the **From User** field.
- To establish a secure connection to the SMTP server, select one of the following connection types.
 - **SSL.** Uses the SSL protocol to form a secure communication.
 - **STARTTLS.** Uses the TLS protocol to form a secure communication over an unsecure channel.If one of these connection types is selected, XClarity Orchestrator attempts to download and import the SMTP server’s certificate to the XClarity Orchestrator truststore. You are prompted to accept this certificate.
- 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.
 - **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 6. Click **Create** to create the destination configuration.

After you finish

You can perform the following actions from the Forwarder Destinations card.

- Modify a selected destination by clicking the **Edit** icon (✎).
- Remove a selected destination by clicking the **Delete** icon (🗑️). You cannot delete a destination that is assigned to a forwarder

Forwarding reports using email

You can forward reports on a reoccurring basis to one or more email addresses using an SMTP web service.

About this task

A *report* is any data that is presented in tabular form in the user interface. The following reports are currently supported.

- Active alerts
- Resource and audit events
- Managed devices (servers, storage, switches, and chassis)
- Device firmware compliance
- Server configuration compliance
- Warranty status for servers
- Active service tickets

Each report forwarder can include only one report of each type.

The report is created as archive file and saved on the orchestrator server host. If the file is 10 MB or less, the file forwarded as an email attachment. If the file is greater than 10MB, the email includes the location of the files. You can also download the archive file by clicking **Reports History** and clicking **Download** in the row for the report.

Lenovo XClarity Orchestrator stores a maximum of 100 reports. If the maximum number of reports is reached, XClarity Orchestrator deletes the oldest report before generating a new one.

Procedure

To forward a report though email, complete one of the following steps.

- **Send unfiltered data**
 1. From the XClarity Orchestrator menu bar, click **Monitoring** (📧) → **Forwarding**, and then click **Report Forwarders** in the left navigation to display the Reports card.
 2. Click the **Create** icon (⊕) to display the Create Report dialog.
 3. Specify the report forwarder name and optional description.
 4. Choose to enable or disable the report forwarder by clicking the **State** toggle.
 5. Click **Content List**, and select one or more reports that you want to forward.
 6. Click **Forwarder Destination**, and select the destination (see [Creating forwarder destination configurations](#)).
 7. Click **Schedules**, and specify the week day, time, duration (start and end date) when you want reports to be sent. The report is sent at the same day and time each week during the specified duration.

8. Click **Create** to create the forwarder.

- **Send filtered data**

1. From the XClarity Orchestrator menu bar, open the card that contains the report that you want to send. The following reports are supported.
 - Device data (click **Resources** (🔍) → {device_type})
 - Active alert data (click **Monitoring** (📧) → **Alerts**)
 - Resource and audit event data (click **Monitoring** (📧) → **Events**)
 - Firmware compliance (click **Provisioning** (🔧) → **Updates** → **Apply and Activate** → **Devices**)
 - Server-configuration compliance (click **Provisioning** (🔧) → **Server Configuration** → **Assign and Deploy**)
 - Device warranty data (click **Administration** (⚙️) → **Service and support** → **Warranty**)
 - Active service tickets (click **Administration** (⚙️) → **Service and support** → **Service Tickets**)
2. Optionally refine the data set to only the information that interests you, by narrowing the scope of data to only those resources that are in specific resource managers and groups, and using filters and search to include data that matches specific criteria (see [User interface tips and techniques](#)).
3. Click the **All Actions** → **Create Report Forwarder** to display the Create Report Forwarder dialog.
4. Specify the report forwarder name and optional description.
5. Choose to enable or disable the report forwarder by clicking the **State** toggle.
6. Click **Forwarder Destination**, and select the destination (see [Creating forwarder destination configurations](#)).
7. Click **Schedules**, and specify the week day, time, duration (start and end date) when you want reports to be sent. The report is sent at the same day and time each week during the specified duration.
8. Click **Create** to create the forwarder.

After you finish

You can perform the following actions from the Report Forwarder card.

- Enable or disable a selected report forwarder by selecting the toggle in the **State** column.
- Modify a selected report forwarder by clicking the **Edit** icon (✎).
- Remove a selected report forwarder by clicking the **Delete** icon (🗑).
- Save reports to your local system by clicking the **Reports History** tab and then clicking **Download** in the row for each report.

You can add a report to an existing report forwarder from any supported report card using the data filters that are currently applied to the table by clicking **All Actions** → **Add content to existing Report Forwarder** from that card. If the report forwarder already includes a report of that type, the report is updated to use the current data filters.

Chapter 4. Managing resources

You can use Lenovo XClarity Orchestrator to manage resources, including viewing offline-devices details.

Creating resource groups

A *resource group* is a set of resource that you can view and act upon collectively in Lenovo XClarity Orchestrator. Several types of resource groups are supported.

Learn more:  [How to create a resource group](#)

About this task

Several types of resource groups are supported.

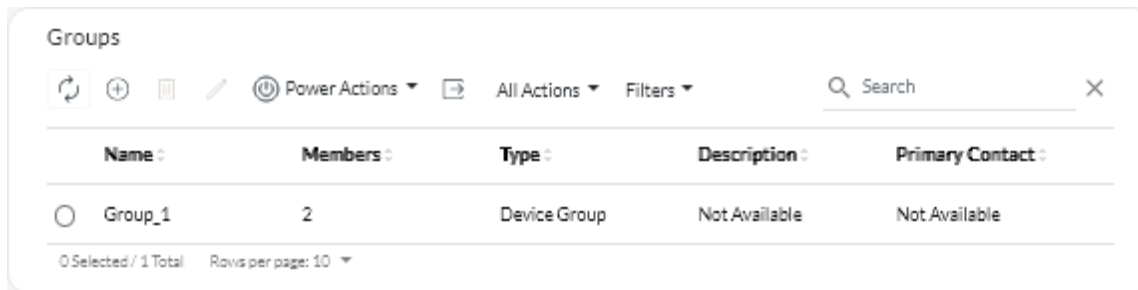
- *Dynamic device groups* contain a dynamic set of devices based on specific criteria.
- *Device groups* contain a static set of specific devices.
- *Manager groups* contain a static set of specific resource managers and XClarity Orchestrator itself.
- *Infrastructure groups* contains a set of network devices. When you manage a Schneider Electric EcoStruxure IT Expert resource manager, XClarity Orchestrator automatically clones “group” collections that are defined in a managed EcoStruxure IT Expert. The cloned group is named *{domain}\{groupName}* in the local repository. Note that location-type collections (site, building, room, row, or rack) are not cloned.

Note: You cannot create a resource group with a mix of devices, resource managers, and infrastructure resources.

Procedure

To create a resource group and manage membership, complete the following steps.

- **Create a dynamic device group and add devices.**
 1. From the XClarity Orchestrator menu bar, click **Resources** (🔍) → **Groups** to display the Groups card.



2. Click the **Create** icon (+) to display the Create group dialog.
3. Select the **Dynamic Device Group** as the group type.
4. Specify the name and optional description for the group.
5. Click **Group Criteria**, and select rules to use for group membership.

- Choose whether a device must match **any** (one or more) or **all** rules from the **Criteria** match drop down.
 - Specify the attribute, operator, and value for each rule. Click **Add Criteria** to add another rule.
 - 6. Click **Contact Information**, and optionally select a primary support contacts (in the **Primary Contacts** column) and one or more secondary contacts (in the **Secondary Contacts** column) to assign to all devices in the group.
 - 7. Click **Create**The group is added to the table.
- **Create a static resource group and add resources.**
 1. From the XClarity Orchestrator menu bar, click **Resources** (⊙) → **Groups** to display the Groups card.
 2. Click the **Create** icon (⊕) to display the Create group dialog.
 3. Select **Device Group** or **Manager Group** as group type.
 4. Specify the name and optional description for the group.
 5. Click **Available Devices** or **Available Resource Managers**, depending on the group type, and select the resources that you want to include in the group.
 6. Click **Contact Information**, and optionally select a primary support contacts (in the **Primary Contacts** column) and one or more secondary contacts (in the **Secondary Contacts** column) to assign to all devices in the group.
 7. Click **Create**.The group is added to the table.
 - **Add devices to a static device group.**
 1. From the XClarity Orchestrator menu bar, click **Resources** (⊙) and then click the device type (such as Servers or Switches) to display a card listing all devices of that type.

Servers

Search X

All Actions ▾ Filters ▾

<input type="checkbox"/>	Server	Status	Connecti	Power	IP Addre	Product	Type-Mo	System F	Advisory	Groups
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	ite-b...				10.24	Leno...	716...	CGE1f	Not ...	Not Av
<input type="checkbox"/>	Blac...				10.24	Leno...	716...	A3EGf	Not ...	Not Av
<input type="checkbox"/>	nod...				10.24	IBM ...	791...	Not Av	Not ...	Not Av
<input type="checkbox"/>	Meh...				10.24	Thin...	7Y4...	ISE13f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Not ...	Not Av
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Not ...	Not Av

0 Selected / 60 Total Rows per page: 10 ▾

2. Select one or more devices to add to a group.

3. Click the **Add item to group** icon ().

4. Select an existing the group or specify a name and optional description to create a new group, and click **Apply**.

- **Add resource managers to a static manager group.**

1. From the XClarity Orchestrator menu bar, click **Resources** () → **Resource Managers** to display the Resource Managers card.

2. Select one or more resource managers to add to a group.

3. Click the **Add item to group** icon ().

4. Select an existing group or specify a name and optional description to create a new group, and click **Apply**.

After you finish

You can perform the following actions from the Groups card.

- Modify the properties and membership of a selected group by clicking the **Edit** icon ().

Note: For infrastructure groups that were cloned from Schneider Electric EcoStruxure IT Expert, use Schneider Electric EcoStruxure IT Expert to change the group name, description, and membership.

- Delete a selected group by clicking the **Delete** icon ().

- View the members of a resource group by clicking the group name to display the View group dialog and then clicking the **Members Summary** tab.

Managing devices offline

If a device is not currently managed by a resource manager, you can use Lenovo XClarity Orchestrator to manage the devices in *offline mode* by importing a service-data archive that is associated with that device.

About this task

Only servers with IMM2 or XCC baseboard management controllers can be managed offline. These devices are identified in the web interface using the “Offline Managed” connectivity status.

You can perform the following actions on devices that are managed offline. All other actions are disabled.

- View device inventory
- Exclude alerts and events
- Manage service data
- Open service tickets in the Lenovo Support Center using Call Home, and manage those service tickets
- Retrieve warranty information
- Analytics functions to predict and analyze problems with those devices

Important: XClarity Orchestrator does not communicate with offline devices to retrieve up to date data.

Procedure

To manage offline devices, complete the following steps.

- Step 1. From the Lenovo XClarity Orchestrator menu bar, click **Resources** (⚙️) → **Servers**. The Servers page is displayed.
- Step 2. Click the **Import** icon (📁) to import service-data archives.
- Step 3. Drag and drop one or more service-data archives (in .gz, .tzz, or .tgz format) to the Import dialog, or click **Browser** to locate the archive.
- Step 4. Optionally enable **Add the server in the service data to the inventory for view only** to manage the applicable server in offline-management mode (see [Managing devices offline](#)).
- Step 5. Click **Import** to import and parse the archive. When parsing is complete, the **Parse Status** for the imported archive changes to “Parsed.”

You can monitor the status of the import and parsing process from the jobs log ([Monitoring jobs](#)).

After you finish

You can unmanage a selected device that is managed offline by clicking the **Unmanage** icon (🗑️).

Performing power actions on managed servers

You can use Lenovo XClarity Orchestrator to power on, power off, and restart managed servers.

Before you begin








You must be a member of a user group to which the predefined **Supervisor** or **Hardware Administrator** role is assigned.

ThinkSystem servers require an operating system to perform power operations.


Ensure that the operating system on the server is Advanced Configuration and Power Interface (ACPI) compliant and is configured to allow shutdown operations.

About this task

XClarity Orchestrator supports the following power actions.

-  **Power On.** Powers on selected servers that are currently powered off.
-  **Power Off Normally.** Shuts down the operating system and powers off selected servers that are currently powered on.
-  **Power Off Immediately.** Powers off selected servers that are currently powered on.
-  **Restart Normally.** Shuts down the operating system and restarts the selected servers that are currently powered on.
-  **Restart Immediately.** Restarts selected servers that are currently powered on.
-  **Restart to System Setup.** Restarts to BIOS/UEFI (F1) Setup for selected servers.
-  **Restart Management Controller.** Restarts the baseboard management controller for selected servers.

Notes:


- For ThinkEdge Client devices, only  **Restart Normally** is supported.
- The connectivity status of the server must be online. You cannot perform power actions on devices that are offline, including Offline Managed devices.

You can perform power actions on a maximum of 25 devices at one time.


• Procedure

To power on, power off or restart servers, complete the following steps

For a single server

- a. From the XClarity Orchestrator menu, click **Resources**  → **Servers**. The Servers card is displayed with a tabular view of all managed servers.
- b. Click the row for the server to display the server summary cards for that server.
- c. From the Quick Actions card, click **Power Actions**, and then click the desired power action.
- d. Click **Confirm**.


For multiple servers

- a. From the XClarity Orchestrator menu, click **Resources**  → **Servers**. The Servers card is displayed with a tabular view of all managed servers.
- b. Select one or more servers. You can select a maximum of 25 servers.
- c. Click **Power Actions**, and then click the desired power action.

A dialog is displayed with a list of selected devices. Note that devices that are not applicable (that do not support power actions) are grey out.

- d. Click **Confirm**.

For all servers in a group

- a. From the XClarity Orchestrator menu, click **Resources**  → **Groups**. The Groups card is displayed with a tabular view of all groups.
- b. Select a group of servers.
- c. From the Quick Actions card, click **Power Actions**, and then click the desired power action.

A dialog is displayed with a list of selected devices. Note that devices that are not applicable (that do not support power actions) are grey out.

- d. Select the specific servers in the group to act on. You can select a maximum of 25 servers.
- e. Click **Confirm**.

A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring (📊)** → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

Opening a remote-control session for managed servers

You can open a remote-control session to a managed server as if you were at a local console. You can then use the remote-control session to perform operations such as powering on or off the server, and logically mounting a local or remote drive.

Opening a remote-control session for ThinkSystem or ThinkAgile servers

You can open a remote-control session to a managed ThinkSystem or ThinkAgile server as if you were at a local console. You can then use the remote-control session to perform management operations.

Before you begin

You must be a member of a user group to which the predefined **Supervisor** or **Hardware Administrator** role is assigned.

The managed server must have a Normal health state and Online connectivity state. For more information about viewing the server status, see [Viewing device details](#).

Review the following considerations for ThinkSystem SR635 and SR655 servers.

- Baseboard management controller firmware v2.94 or later is required.
- Only multiple-user mode is supported; single-user mode is not supported.
- Internet Explorer 11 is not supported.
- You cannot power on or power off a server from a remote-control session.

About this task

You can launch a remote-control session to a single ThinkSystem or ThinkAgile server.

For more information about using the remote console and media features, see your ThinkSystem or ThinkAgile server documentation.

Note: For the ThinkSystem and ThinkAgile servers, a Java Runtime Environment (JRE) with Java WebStart support is not required.

Procedure

To open a remote-control session for a ThinkSystem or ThinkAgile server, complete the following steps.

- Step 1. From the XClarity Orchestrator menu, click **Resources (📊)** → **Servers**. The Servers card is displayed with a tabular view of all managed servers.
- Step 2. Select the server to remotely control.
- Step 3. Click the **Launch Remote Control** icon (🖥️).
- Step 4. Accept any security warnings from your web browser.

After you finish

If the remote-control session does not open successfully, see [Remote control issues](#) in the XClarity Orchestrator online documentation..

Opening a remote-control session for ThinkServer servers

You can open a remote-control session to managed ThinkServer servers as if you were at a local console. You can then use the remote-control session to perform power and reset operations, logically mount a local or network drive on the server, capture screen shots, and record video.

Before you begin

You must be a member of a user group to which the predefined **Supervisor** or **Hardware Administrator** role is assigned.

The managed server must have a Normal health state and Online connectivity state. For more information about viewing the server status, see [Viewing device details](#).

The Features on Demand key for ThinkServer System Manager Premium Upgrade must be installed on managed server. For more information about FoD keys that are installed on your servers, see [Viewing Features on Demand keys](#) in the Lenovo XClarity Administrator online documentation.

A Java Runtime Environment (JRE) with Java WebStart support (such as Adopt OpenJDK 8 with the IcedTea-Web v1.8 plugin) must be installed on the local server.



About this task

You can open a remote-control session to only a single ThinkServer server.

For more information about using the ThinkServer remote console and media features, see your ThinkServer server documentation.

Procedure

To open a remote-control session for a ThinkSystem or ThinkAgile server, complete the following steps.

- Step 1. From the XClarity Orchestrator menu, click **Resources**  **Servers**. The Servers card is displayed with a tabular view of all managed servers.
- Step 2. Select the server to remotely control.
- Step 3. Click the **Launch Remote Control** icon .
- Step 4. Accept any security warnings from your web browser.

After you finish

If the remote-control session does not open successfully, see [Remote control issues](#) in the XClarity Orchestrator online documentation..

Opening a remote-control session for System x servers

You can open a remote-control session to managed System x servers as if you were at a local console. You can then use the remote-control session to perform power and reset operations, logically mount a local or network drive on the server, capture screen shots, and record video.

Before you begin

Review the security, performance, and keyboard considerations before opening a remote-control session. For more information about these considerations, see [Remote control considerations](#).

You must be a member of a user group to which the predefined **Supervisor** or **Hardware Administrator** role is assigned.

The managed server must have a Normal health state and Online connectivity state. For more information about viewing the server status, see [Viewing device details](#).

Use your Lenovo XClarity Orchestrator user account to log in to the remote-control session. The user account must have sufficient user authority to access and manage a server.

A Java Runtime Environment (JRE) with Java WebStart support (such as Adopt OpenJDK 8 with the IcedTea-Web v1.8 plugin) must be installed on the local server.

The Features on Demand key for remote presence must be installed and enabled on managed server. You can determine whether remote presence is enabled or disabled from the Servers page and clicking **Filters** → **Remote Presence**. If disabled:

- Ensure that the server is in a Normal health status and Online connectivity state.
- Ensure that the XClarity Controller Enterprise level or MM Advanced Upgrade for is enabled for servers that do not come with these features already activated by default.

The remote-control session uses the locale and display language settings that are defined for the operating system on your local system.

About this task

You can start multiple remote-control sessions. Each session can manage multiple servers.

Note: For Flex System x280, x480, and x880 server, you can start a remote-control session to only the primary node. If you attempt to start a remote-control session to a non-primary node in a multi-node system, the remote-control dialog starts, but no video is displayed.

Procedure

To open a remote-control session for a System x server, complete the following steps.

Step 1. From the XClarity Orchestrator menu, click **Resources** (🔍) → **Servers**. The Servers card is displayed with a tabular view of all managed servers.

Step 2. Optional: Select the server to remotely control.

If you do not select a server, an untargeted remote-control session is opened.

Step 3. Click the **Launch Remote Control** icon (🔗).

Step 4. Accept any security warnings from your web browser.

Step 5. When you are prompted, select one of the following connection modes:

- **Single-user mode.** Establishes an exclusive remote-control session with the server. All other remote-control sessions to that server are blocked until you disconnect from the server. This option is available only if there are no other remote-control sessions established to the server.
- **Multi-user mode.** Allows multiple remote-control sessions to be established with the same server. XClarity Orchestrator supports up to six concurrent remote-control sessions to a single server.

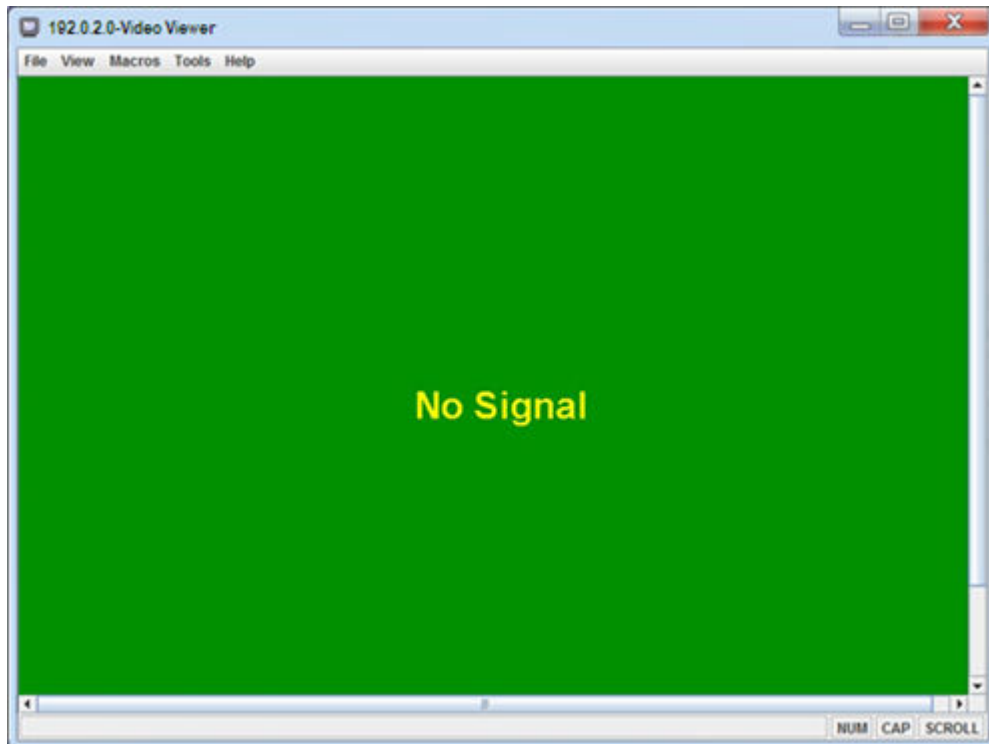
Step 6. Click **Launch remote control**.

Step 7. When you are prompted, choose whether to save a shortcut to the remote-control session on your local system. You can use this shortcut to launch a remote-control session without logging in to the XClarity Orchestrator web interface. The shortcut contains a link that opens an empty remote-control session to which you can manually add servers.

Note: Your local system must have access to XClarity Orchestrator to validate the user account with the XClarity Orchestrator authentication server.

After you finish

The remote-control session has a thumbnail (icon) for each server that is currently managed through the session.









If the remote-control session does not open successfully, see

You can perform the following actions from the remote-control session.

- Display multiple server consoles and move between server consoles by clicking a thumbnail. The server console is displayed in the video session area. If you are accessing more servers than fit in the icon area, click the **Scroll right** icon (») and **Scroll left** icon («) to scroll to additional server thumbnails. Click the **All sessions** icon (🖥️) to see a list of all open server sessions.
- Add a server console to the current remote-control session by clicking **Add server** icon (+).
- Hide or show the thumbnail area by clicking the **Toggle Thumbnails** icon (📄).
- Display the remote-control session as a window or full screen by clicking the **Screen** icon (🖥️) and then clicking **Toggle on full screen** or **Toggle off full screen**.

- Use the sticky key buttons Ctrl, Alt, and Shift to send keystrokes directly to the server. When click a sticky key, the key remains active until you press a keyboard key or click the button again. To send a Ctrl or Alt key combinations, click Ctrl or Alt in the toolbar, place the cursor in the video session area, and press a key on the keyboard.

Note: If mouse-capture mode is enabled, press the left Alt key to move the cursor outside of the video session area. Although mouse-capture mode is disabled by default, you can enable it from the Toolbar page (see [Setting remote-control preferences](#)).

- Define custom key sequences, known as softkeys, by clicking the **Keyboard** icon (). Softkey definitions are stored on the system from which you started the remote-control session. Therefore, if you launch the remote-control session from another system, you have to define the softkeys again. You can export user settings, including softkeys, by clicking the **Preference** icon () , clicking the **User Settings** tab, and then clicking **Import**.
- Take a screen capture of the currently selected server session and save that screen capture in a variety of formats by clicking the **Screen** icon () , and then clicking **Screenshot**.
- Mount remote media (such as CD, DVD, or USB device, disk image, or CD (ISO) image) to the selected server or move a mounted device to another server by clicking the **Remote Media** icon () .
- Upload images to a server from remote media by clicking the **Remote Media** icon () , clicking **Mount remote media** ., and then clicking **Upload the image to the IMM**.
- Power the server on or off from a remote console by clicking the **Power** icon () .
- Change remote-control preferences, including how often the server icon are refreshed (see [Setting remote-control preferences](#)).

Remote control considerations

Be aware of security, performance, and keyboard considerations that are related to accessing managed servers using a remote-control session.

Security considerations

The user account that is used to start the remote-control session must be a valid user account that has been defined in the Lenovo XClarity Orchestrator authentication server. The user account must also have sufficient user authority to access and manage a server.

By default, multiple remote-control sessions can be established to a server. However, when you start a remote-control session, you have the option to start the session in single-user mode, which establishes an exclusive session with the server. All other remote-control sessions to that server are blocked until you disconnect from the server.

Note: This option is available only if there are currently no other remote-control sessions established to the server.

To use Federal Information Processing Standard (FIPS) 140, you must enable it manually by completing the following steps on your local system:

1. Find the provider name of the FIPS 140 certified cryptographic provider that is installed on your local system.
2. Edit the file `$(java.home)/lib/security/java.security`.
3. Modify the line that includes `com.sun.net.ssl.internal.ssl.Provider` by appending the provider name of your FIPS 140 certified cryptographic provider. For example, change:

```
security.provider.4=com.sun.net.ssl.internal.ssl.Provider
```

to:

```
security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11 -NSS
```


Performance considerations

If a remote-control session becomes slow or unresponsive, close all video and remote media sessions that you have established with the selected server to reduce the number of open server connections. In addition, you might increase performance by changing the following preferences. For more information, see [Setting remote-control preferences](#).

- **KVM**

- Decrease the percentage of video bandwidth that is used by the application. The image quality of the remote-control session will be reduced.
- Decrease the percentage of frames that are refreshed by the application. The refresh rate of the remote-control session will be reduced.

- **Thumbnails**

- Increase the thumbnail refresh interval rate. The application will refresh thumbnails at a slower rate.
- Turn off the display of thumbnails completely.

The size of the remote-control session window and the number of active sessions might affect workstation resources, such as memory and network bandwidth, which can influence performance. The remote-control session uses a soft limit of 32 open sessions. If more than 32 sessions are open, performance might be severely degraded, and the remote-control session might become unresponsive. You might see performance degradation with fewer than 32 open sessions if resources, including network bandwidth and local memory, are not sufficient.

Keyboard considerations

The remote-control session supports the following keyboard types:

- Belgian 105-key
- Brazilian
- Chinese
- French 105-key
- German 105-key
- Italian 105-key
- Japanese 109-key
- Korean
- Portuguese
- Russian
- Spanish 105-key
- Swiss 105-key
- UK 105-key
- US 104-key

For information about keyboard preferences, see [Setting remote-control preferences](#).

Setting remote-control preferences

You can modify preference settings for the current remote-control session.

Procedure

Complete the following steps to modify remote-control preferences.

Step 1. To modify the remote-control preferences, click the **Preferences** icon (). All changes take effect immediately.

- **KVM**

- **Percentage of Video Bandwidth.** Increasing the bandwidth improves the quality in the appearance of the remote-control session but might affect the performance of the remote-control session.
- **Percentage of Frames Refreshed.** Increasing the frame-refresh percentage increases how often the remote-control session is updated but might affect the performance of the remote-control session.
- **Keyboard type.** Select the type of keyboard that you are using for the remote-control session. The keyboard type that you select must match the keyboard settings in the local system and match the keyboard settings on the remote host.

Note: If you select an international keyboard and you need to enter key combinations that require the Alternate Graphics key (AltGr), ensure that the operating system on the workstation that you use to invoke the remote-control session is the same type of operating system as the one on the server that you want to remotely access. For example, if the server is running Linux, ensure that you invoke the remote-control application from a workstation that is running Linux.

- **Scale image to window.** Select this option to scale the video image that is received from the server to the size of the video session area.

- **Security**

- **Prefer single-user mode connections.** Specify whether single-user mode connections is the default choice when connecting to a server. When a connection is made in single-user mode, only one user can be connected to a server at a time. If this box is not selected, the default function is to connect to the server in multi-user mode.
- **Require (secure) tunneling connections.** Select this option to access a server through the management node. You can use this option to access a server from a client that is not on the same network as the server.

Note: The remote-control application always attempts to connect directly to the server from the local system where remote control was launched. If you select this option, the remote-control application accesses the server through Lenovo XClarity Orchestrator if the client workstation cannot access the server directly.

- **Toolbar**

Note: Click **Restore defaults** to restore all settings on this page to the default settings

- **Pin the toolbar to the window.** By default, the toolbar is hidden above the remote-control session window and displays only when you move your mouse pointer over it. If you select this option, the toolbar is pinned to the window and is always displayed between the thumbnail panel and the remote-control session window.
- **Show keyboard buttons.** Specify whether to display the keyboard-button icons (CapsLock, NumLock, and ScrollLock) on the toolbar.
- **Show power control.** Specify whether to display the power-control options on the toolbar.
- **Show sticky key buttons.** Specify whether to display the sticky-key button icons (Ctrl, Alt, and Delete) on the toolbar.
- **Hide local mouse pointer.** Specify whether to display the local mouse pointer when you position the cursor in the server session that is currently displayed in the video session area.
- **Enable mouse-capture mode.** By default, mouse-capture mode is disabled. This means that you can freely move the cursor in and out of the video session area. If you enable mouse-capture mode, you must press the left Alt key before you can move the cursor out of the video session area. If mouse-capture mode is enabled, you can specify whether to use the Ctrl+Alt keys to exit mouse-capture mode. The default is to use the left Alt key.

- **Specify toolbar background opacity.** Lowering the opacity percentage displays more of the video session area through the toolbar background.
- Note:** This option is available only when the toolbar is not pinned to the window.
- **Thumbnails**
 - **Show thumbnails.** Select this option to show the thumbnail area in the remote-control session.
 - **Specify thumbnail refresh interval.** Decreasing the interval for refreshing thumbnails increases how often the server thumbnails are updated.
 - **General**
 - **Debug mode.** Specify whether to set debug mode for the remote-control application. The settings determine the granularity of events that are logged in the log files. By default, only severe events are logged.
 - **Inherit system appearance settings.** This setting changes the appearance to match color schemes that are configured for the local server (running Windows). You must restart the remote-control application for these settings to take effect.
 - **Create desktop icon.** This setting creates a desktop icon on your local system so that you can start the remote-control application directly from your system. You must still have access to the management software from your system.
 - **Synchronize with management server.** This setting ensures that the server data that is displayed in the remote-control application matches the server data that is displayed from management software.

Chapter 5. Provisioning resources

You can use Lenovo XClarity Orchestrator to provision your managed resources, such as deploying updates to Lenovo XClarity Administrator resource managers and managed servers and configuring managed servers.

Provisioning server configurations

Server-configuration patterns are used to quickly configure multiple servers from a single set of defined configuration settings. Each pattern defines the configuration characteristics for a specific type of server. You can create a server pattern by learning the settings from an existing server.

Before you begin

Ensure that the servers that you want to configure are up to date with the latest firmware.

About this task

Configuring servers using patterns is supported for only ThinkSystem servers (excluding SR635 and SR655).

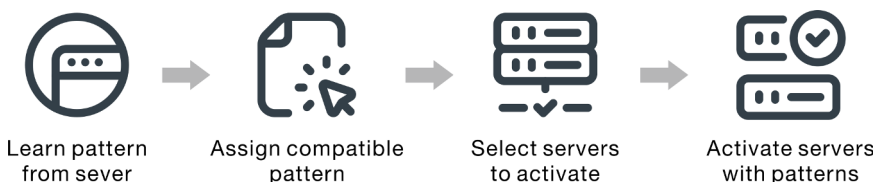
You can use server-configuration patterns to configure baseboard management controller and Unified Extensible Firmware Interface (UEFI) settings and definitions on managed servers. Patterns integrate support for virtualizing I/O addresses, so you can virtualize server fabric connections or repurpose servers without disruption to the fabric.

You cannot configure the following settings.

- Boot order
- Local storage and SAN zoning
- I/O adapters
- Local user accounts
- LDAP servers

Procedure

The following figure illustrates the workflow for configuring managed servers.



Step 1. Create a server pattern

You can create patterns to represent different configurations that are used in your data center by learning the configuration settings and definitions of existing servers.

Important: Consider creating a server pattern for each type of server in your data center. For example, create a server pattern for all ThinkSystem SR650 servers and another server pattern for all ThinkSystem SR850 servers. Do not deploy a server-configuration pattern that was created for one server type to another server type.

For more information about creating server patterns, see [Learning a server-configuration pattern from an existing server](#).

Step 2. **Assign the pattern to one or more managed servers**

You can assign a pattern to multiple servers; however, each server can have only one assigned pattern XClarity Orchestrator.

Consider creating a server pattern for each type of server in your data center. For example, create a server pattern for all ThinkSystem SR650 servers and another server pattern for all ThinkSystem SR850 servers.

Do not assign or deploy a server pattern that was created for one server type to another server type.

After you assign an applicable pattern to one or more target servers, XClarity Orchestrator runs a compliance check on the servers to determine whether the server configuration matches the pattern. Servers that are out of compliance with their assigned pattern are flagged.

For more information about creating server patterns, see [Applying and activating updates to resource managers](#).

Step 3. **Deploy the assigned pattern on target servers**

You can deploy patterns that are assigned to one or more specific servers or to groups of servers. When you deploy a pattern, the configuration settings and definitions from that pattern are written to shared memory and then activated. Some settings require a system reboot before they are activated.

Servers must be restated to activate certain configuration changes, such as baseboard management controller and Unified Extensible Firmware Interface (UEFI) configurations settings. You can choose when to activate the changes:

- **Deferred activation** activates all configuration changes after the next server restart. The target server must be restarted manually to continue the deployment process.

Important: Use **Restart Normally** to restart the server to continue the update process. *Do not* use **Restart Immediately**.

Note: The settings on a server can become out of compliance with its pattern if settings are changed directly on the server instead of in the assigned patterns or if an issue occurred when the assigned pattern was deployed, such a firmware issue or an invalid setting. You can determine the compliance status of each server from the **Assign and Deploy** tab.

Attention: XClarity Orchestrator does not assign IP and I/O addresses to individual servers when the server patterns are deployed.

For more information about creating update-compliance policies, see [Assigning and deploying a server-configuration pattern](#).

Step 4. **Modify and redeploy a pattern** You can make subsequent configuration changes to an existing pattern. When you save the pattern, XClarity Orchestrator runs a compliance check on the servers that are assigned that pattern to determine whether the server configuration matches the pattern. You can then redeploy the changed pattern to all or a subset of servers that are assigned that pattern.

Server-configuration considerations

Before you begin configuring servers using Lenovo XClarity Orchestrator, review the following important considerations.

Server considerations

- Configuring servers using patterns is supported for only ThinkSystem servers (excluding SR635 and SR655).
- Ensure that the servers that you want to configure are up to date with the latest firmware.

Configuration-pattern considerations

- You can assign a pattern to multiple servers; however, each server can have only one assigned pattern XClarity Orchestrator.

Note: XClarity Orchestrator does not prevent you from assigning or deploying a server-configuration pattern to a server that has an assigned pattern or server profile in Lenovo XClarity Administrator. Deploying a pattern using XClarity Orchestrator might affect pattern compliance in XClarity Administrator.

- You can use server-configuration patterns to configure baseboard management controller and Unified Extensible Firmware Interface (UEFI) settings and definitions on managed servers. Patterns integrate support for virtualizing I/O addresses, so you can virtualize server fabric connections or repurpose servers without disruption to the fabric.

You cannot configure the following settings.

- Boot order
 - Local storage and SAN zoning
 - I/O adapters
 - Local user accounts
 - LDAP servers
- Consider creating a server pattern for each type of server in your data center. For example, create a server pattern for all ThinkSystem SR650 servers and another server pattern for all ThinkSystem SR850 servers.
 - Do not assign or deploy a server pattern that was created for one server type to another server type.
 - The settings on a server can become out of compliance with its assigned pattern in the following instances. You can determine the compliance status of each server from the **Assign and Deploy** tab.
 - Configuration settings were changed directly on the server instead of in the assigned patterns.
 - An issue occurred during pattern deployment, such a firmware issue or an invalid setting.
 - Firmware was updated, which changed configuration settings and definitions.

Note: Deployment might fail if the assigned pattern is based on previous firmware levels. In this case, it is recommended that you choose to learn a new pattern based on the current installed firmware or modify the existing pattern to exclude the configuration of specific items before deploying the pattern.

Configuration-process considerations

- While the configuration is in progress, the target server is locked. You cannot initiate other management tasks on the target server until the configuration process is complete.
- After a configuration pattern is deployed to a server, one or more restarts might be required to fully activate the changes. You can choose to activate all changes by immediately restarting the server. If you choose to restart the server immediately, XClarity Orchestrator minimizes the number of restarts that are required. If you choose to deferred activation, all changes are activated the next time the server is restarted. If you choose partial activation, the changes that do not require a server restart are immediately activated, and all other changes are activated the next time the server is restarted.

- Ensure that no jobs are currently running on the target server. If jobs are running, the configuration job is queued until all other jobs have completed.
- Some advanced server functions are activated using Features on Demand keys. If features have configurable settings that are exposed during UEFI setup, you can configure the setting using configuration patterns; however, the resulting configuration is not activated until the corresponding Features on Demand key is installed.

Learning a server-configuration pattern from an existing server

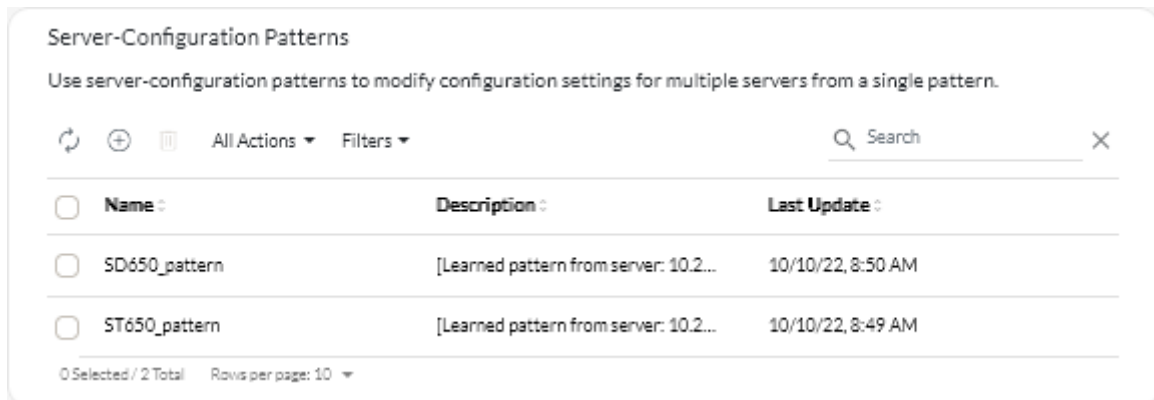
Server-configuration patterns define the configuration characteristics for a specific type of server. You can create a server pattern by learning the settings from an existing server

Before you begin

- Ensure that you read the server-configuration considerations before you create a server-configuration pattern (see [Update deployment considerations](#)).
- Ensure that the server that you want to use to create the pattern is online.
- Identify groups of servers that have the same hardware options and that you want to configure the same way. You can use a server pattern to deploy the same configuration settings to multiple servers, thereby controlling a common configuration from one place.

To create a pattern by learning the configuration of an existing server, complete the following steps.

Step 1. From the XClarity Orchestrator menu bar, click **Provisioning** (🔗) → **Server Configuration** and then click the **Patterns** tab to display the Server-Configuration Patterns card.



Step 2. Click the **Create** icon (+) to display the Create Server-Configuration Pattern dialog.

Create Server-Configuration Pattern x

Specify pattern name and description

Name

Description ///

Select server to pull from as a basic configuration ●

🔄 All Actions ▾ Filters ▾
🔍 Search x

	Devices :	IP Addresses :	Product Name :
<input type="radio"/>	Colossus-ST650V2-1	10.240.211.65, 2002:97bc:2bt	ThinkSystem ST650V2
<input type="radio"/>	Mehlow-ST250-1	10.240.211.39, 169.254.95.11	ThinkSystem ST250
<input type="radio"/>	OceanCat-SDV-6	10.240.211.221, 2002:97bc:2t	Lenovo ThinkSystem SD650

0 Selected / 3 Total Rows per page: 10 ▾

Learn

Step 3. Specify the name and optional description for the pattern.

Step 4. Select the server that you want to use as a basis for this pattern.

Note: Unsupported device models are displayed in grey text and cannot be selected.

Step 5. Click **Learn**.

A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📧) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

After you finish

You can perform the following actions from the Patterns card.

- View pattern details by clicking the row for the pattern.
- Copy a selected pattern by clicking the **Copy** icon (📄).
- Modify the configuration settings in a pattern by clicking the row for the pattern to display the pattern details, making necessary changes, and then clicking **Save**. By default, all learned settings are included in the pattern. You can exclude settings from the pattern by selecting **Exclude/Include settings in the pattern** and then clearing the settings that you do not want in the pattern. Settings that are cleared (marked for exclusion) are highlighted in yellow. When you click **Save**, only settings that are included in the pattern are listed. If you excluded settings, you could include them again by clicking **Exclude/Include settings in the pattern**, clicking **Display excluded settings**., and then selecting the settings you want to include. Settings that are selected (marked for inclusion) are highlighted in green.

Note: The compliance check is based on only included settings. Excluded settings are not checked.

When you save the modified pattern, XClarity Orchestrator runs a compliance check on the servers that are assigned that pattern to determine whether the server configuration matches the pattern. You can then deploy the changed pattern to the servers that are not compliant (see [Assigning and deploying a server-configuration pattern](#)).

Pattern Configuration

Extended BMC

Extended UEFI

Exclude/Include settings in this pattern

Display excluded settings

Color marker: Excluded Included

Pattern Configuration

Name*

SD650_pattern

Description

[Learned pattern from server: 10.240.211.221 on 2022-10-10]

Integrated Management Module

- > Login Profile
- > General Settings
- > Network Settings Interface

UEFI

- System Recovery**
 - POST Watchdog Timer
 - POST Watchdog Timer Value
 - Reboot System on NMI
 - Post Load Setup Default
 - <F1> Start Control
- > Devices and I/O Ports
- > Processors
- > Physical Presence Policy Configuration

- Copy a configuration pattern by clicking the row for the pattern to display the pattern details, and then clicking **Save As**.
- Delete a selected pattern by clicking the **Delete** icon (🗑️). If the pattern is assigned to one or more servers, a dialog is displayed with a list of applicable servers. When you confirm the delete request, the pattern is unassigned from those servers.

Note: You cannot delete a pattern that is actively being deployed to servers.

- Assign and deploy a pattern to one or more target servers (see [Assigning and deploying a server-configuration pattern](#)).

Assigning and deploying a server-configuration pattern

You can assign and deploy a server-configuration pattern to one or more managed servers.

Before you begin

- Ensure that you read the server-configuration considerations before you assign or deploy a pattern to a server (see [Update deployment considerations](#)).
- Ensure that the servers that you want to configure are up to date with the latest firmware.
- Do not assign or deploy a server pattern that was created for one server type to another server type.
- XClarity Orchestrator does not prevent you from assigning or deploying a server-configuration pattern to a server that has an assigned pattern or server profile in Lenovo XClarity Administrator. Deploying a pattern using XClarity Orchestrator might affect pattern compliance in XClarity Administrator.
- XClarity Orchestrator does not assign IP and I/O addresses to individual servers when the server patterns are deployed.

About this task

When a pattern is assigned to a server, XClarity Orchestrator runs a compliance check to compare the current configuration settings on the server with the settings in the configuration pattern and updates the **Compliance Status** column based on the results. The compliance status can be one of the following values.

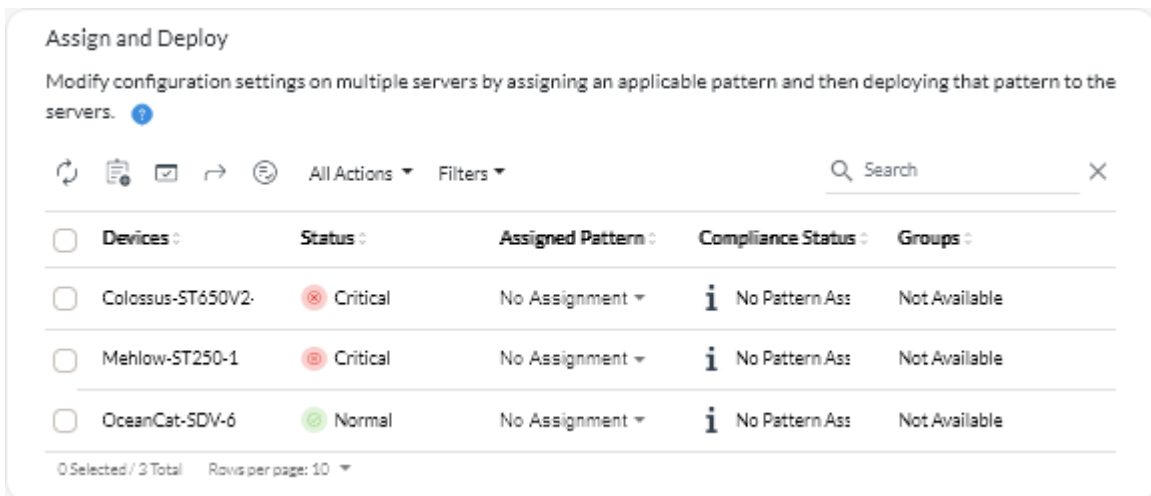
- **Compliant.** All configuration settings in the assigned pattern match the settings on the server.
- **Noncompliant.** One or more configuration setting in the assigned pattern *do not* match settings on the server. Hover the mouse over the table cell to display a pop-up that lists the mismatched settings and values.
- **Pending.** A pattern deployment or compliance check is in progress.
- **Pending Restart.** The server needs to be restarted to activate the configuration changes after pattern deployment.
- **Not Available.** A pattern is not assigned to the server.

When you deploy a pattern to a server, XClarity Orchestrator modifies the settings of the server to match its assigned server-configuration pattern. When the deployment is complete, XClarity Orchestrator runs the compliance check to verify that the settings in the assigned pattern match the setting on the server, and then updates the compliance status for the server.


Procedure

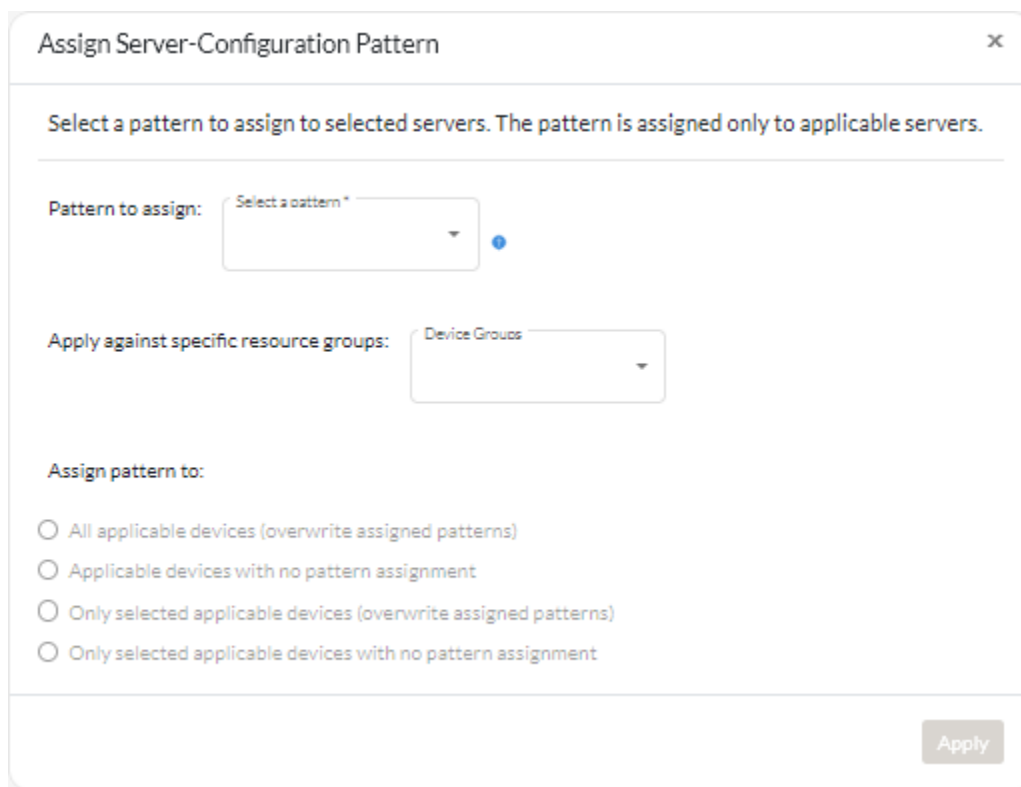
To assign and deploy a server-configuration pattern to one or more servers, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Provisioning** (🔗) → **Server Configuration** and then click the **Assign and Deploy** tab to display the Assign and Deploy Server-Configuration Patterns card.



Step 2. Assign a pattern to one or more servers.

1. Select one or more servers.
2. Click the **Assign** icon () to display the Assign Server Configuration Pattern dialog.



3. Select the pattern that you want to assign.

Notes:

- This list shows all applicable patterns for the specific servers. The list might be incomplete if the orchestrator server is still calculating the applicable patterns. In this case, close the dialog, wait some time, and then open the dialog again.
 - Select the **No Assignment** pattern to unassign a pattern from the selected list of devices.
4. Select the assignment rule. This can be one of the following values.

- **All applicable devices (overwrite assigned patterns)**
- **Applicable devices with no pattern assignment**
- **Only selected applicable devices (overwrite assigned patterns)**
- **Only selected applicable devices with no pattern assignment**

5. Click **Assign**.

Step 3. Deploy the assigned pattern on specific servers.

1. Select one or more servers.

Note: Unsupported device models are displayed in grey text and cannot be selected.

2. Click the **Deploy** icon (☑) to display the Deploy Server-Configuration Pattern dialog.

3. Choose when to activate the updates.

- **Deferred activation** activates all configuration changes after the next server restart. The target server must be restarted manually to continue the deployment process.

Important: Use **Restart Normally** to restart the server to continue the update process. *Do not* use **Restart Immediately**.

4. Click **Deploy**. A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

After you finish

You can perform the following actions from the Patterns card.

- Manually run a configuration-compliance check on selected servers by clicking **All Actions** → **Compliance Check**.
- Unassign a pattern from one or more target servers by assigning the **No Assignment** pattern.
- Troubleshoot issues when deploying a pattern (see .).
- Forward reports about configuration-compliance on a reoccurring basis to one or more email addresses by clicking the **Create Report Forwarder** icon (⊕). The report is sent using the data filters that are currently applied to the table. All shown and hidden table columns are included in the report. For more information, see [Forwarding reports](#).

- Add a configuration-compliance report to a specific report forwarder using the data filters that are currently applied to the table by clicking the **Add to Report Forwarder** icon (↗). If the report forwarder already includes a configuration-compliance report, the report is updated to use the current data filters.

Maintaining server-configuration compliance

The settings on a server can become out of compliance with the server settings were changed without using configuration patterns, if an issue occurred when applying a configuration pattern (for example, if the pattern was created from an earlier firmware level than what is on the server), or when applying a firmware update that changes the server configuration (for example, settings might be added or deleted, setting behaviors might change, new choices might be added, or value ranges might change).

About this task

You can determine the compliance status of each server from the **Compliance Status** column on the Server Configuration: Assign and Deploy page. If a server is non-compliant, hover the cursor over the status to determine the reason.

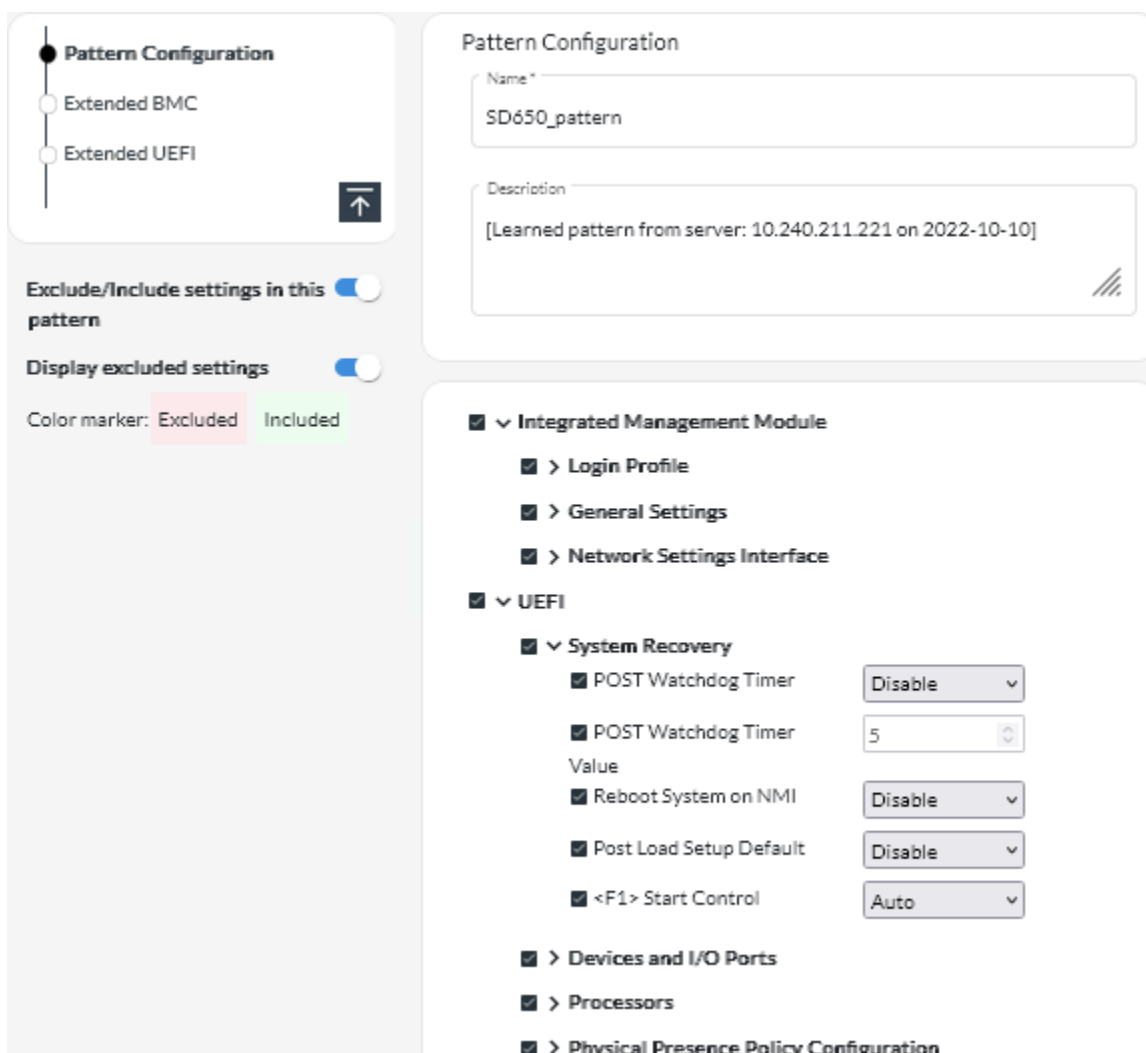
Procedure

To resolve configuration-compliance issues, perform one of the following steps.

- Learn a new configuration pattern based on the current firmware level (see [Learning a server-configuration pattern from an existing server](#)). Then, assign and apply that pattern to the server (see [Assigning and deploying a server-configuration pattern](#)).
- Modify the applicable configuration pattern to correct non-compliant settings by clicking the row for the pattern to display the pattern details, making necessary changes, and then clicking **Save**. By default, all learned settings are included in the pattern. You can exclude settings from the pattern by selecting **Exclude/Include settings in the pattern** and then clearing the settings that you do not want in the pattern. Settings that are cleared (marked for exclusion) are highlighted in yellow. When you click **Save**, only settings that are included in the pattern are listed. If you excluded settings, you could include them again by clicking **Exclude/Include settings in the pattern**, clicking **Display excluded settings**., and then selecting the settings you want to include. Settings that are selected (marked for inclusion) are highlighted in green.

Note: The compliance check is based on only included settings. Excluded settings are not checked.

When you save the modified pattern, XClarity Orchestrator runs a compliance check on the servers that are assigned that pattern to determine whether the server configuration matches the pattern. You can then deploy the changed pattern to the servers that are not compliant (see [Assigning and deploying a server-configuration pattern](#)).



- Create a modified copy of the configuration pattern by clicking the row for the pattern to display the pattern details, making necessary changes, and then clicking **Save As**. Then, assign and apply that pattern to the non-compliant server (see [Assigning and deploying a server-configuration pattern](#)).

Provisioning operating systems

You can use Lenovo XClarity Orchestrator to manage the OS-images repository and deploy operating-system images.

Before you begin

XClarity Orchestrator does not directly deploy operating systems to devices. Instead, it sends requests to the applicable resource manager to perform the deployment. Ensure that the resource manager has the necessary licenses to perform OS deployment functions.

Review the deployment considerations before you attempt to deploy operating systems to your managed devices (see [Operating-system deployment considerations](#)).

Ensure that all firmware on the managed server is at the latest levels (see [Provisioning updates to managed resources](#)).

Ensure that the configuration on the managed server is up to date (see [Provisioning server configurations](#)).

Attention: It is recommended that you *do not* use XClarity Orchestrator to perform a bare-metal operating-system deployment on Converged and ThinkAgile appliances.

Note: Ensure that servers are managed using XClarity Administrator v4.0 or later.

About this task

XClarity Orchestrator provides a simple way to deploy operating-systems images to *bare-metal* servers, which typically do not have an operating system installed. If you deploy an operating system to a server that has an operating system installed, XClarity Orchestrator performs a fresh installation that overwrites the partitions on the target disks.

Several factors determine the amount of time that is required to deploy an operating system to a server.

- The amount of RAM that is installed in the server, which affects how long the server takes to start up.
- The number of and types of I/O adapters that are installed on the server, which affects the amount of time that it takes to collect inventory data. It also affects the amount of time that it takes for the UEFI firmware to start when the server is started up. During an operating-system deployment, the server is restarted multiple times.
- The amount of network traffic. The operating-system image is downloaded to the server over the data network or the operating-system deployment network.
- The amount of RAM, processors, and hard drive storage that is available to the orchestrator server and resource managers.

Procedure

The following figure illustrates the workflow for deploying an OS image to a server.



Step 1. Import OS images.

Before you can deploy an operating system to a server, you must first import the operating system image into the OS-images repository in the XClarity Orchestrator resource manager. When you import an OS image:

- Ensures that there is sufficient space in the OS-images repository before importing the operating system. If you do not have sufficient space to import an image, delete an existing image from the OS-images repository and attempt to import the new image again.
- Creates one or more profiles of that image and stores the profile in the OS-images repository. Each *profile* includes the OS image and installation options. For more information about predefined OS image profiles, see [Operating-system image profiles](#).

A *base operating system* is the full OS image that was imported into the OS-images repository. The imported base image contains predefined profiles that describe the installation configurations for that image. You can create custom profiles based on predefined profiles in the base OS image that can be deployed for specific configurations.

For a list of supported base and custom operating systems, see [Supported operating systems](#).

Step 2. **Customize and assign the OS profile**

Operating system profiles are created automatically when you import an operating system. The profiles that are created are based on the operating system type and version. You can modify the profile, including OS credentials, hostname, networking and storage settings, license keys, and storage location.

Step 3. **Assign and deploy the OS profile**

You can assign an OS profile to one or more target servers, and then deploy the profile to those servers. . Remember that to deploy an operating system, the server must have a deployment status of **Ready**.

XClarity Orchestrator does not directly deploy operating systems to devices. Instead, it sends a request to the applicable resource manager to perform the deployment, and then tracks the progress of the request. XClarity Orchestrator transfers the applicable images to the resource manager and creates a request to start a job on the resource manager to perform the deployment.

Before you attempt to deploy an operating-system image, review the [Operating-system deployment considerations](#).

For more information about assign and deploying an OS profile, see the [Deploying an operating-system image](#).

Operating-system deployment considerations

Before you attempt to deploy an operating-system image, review the following considerations.

Resource-manager considerations

- For devices that are managed using Lenovo XClarity Administrator, ensure that the XClarity Administrator instance has the necessary licenses or trial period to perform OS deployment functions.
- OS deployment is not supported on devices that are managed by Lenovo XClarity Management Hub.

Managed-device considerations

- Ensure that the OS-deployment function is supported for the target devices. For information about operating-system deployment limitations for specific devices, see .
- Ensure that no jobs are currently running on the target server. To see a list of active jobs, click **Monitoring** → **Jobs**.
- Ensure that all firmware on the managed server is at the latest levels (see [Provisioning updates to managed resources](#)).
- Ensure that the configuration on the managed server is up to date (see [Provisioning server configurations](#)). Also, ensure that the target device does not have a deferred or partially activated server pattern. If a server pattern has been deferred or partially activated on the managed server, you must restart the server to apply all configuration settings. Do not attempt to deploy an operating system to a server with a partially activated server pattern.

To determine the configuration status of the server, see the **Configuration Status** field on the Summary page for the managed server (see [Viewing device details](#)).

- Ensure that a password for the root account that is to be used to deploy the operating system is defined. For more information about setting the password, see [Configuring operating-system profiles](#).
- Ensure there is no mounted media (such as ISOs) on the target server. Additionally, ensure there are no active Remote Media sessions open to the management controller.
- Ensure that the timestamp in BIOS is set to the current date and time.

- For ThinkSystem servers
 - Ensure that the Legacy BIOS option is disabled. From the BIOS/UEFI (F1) Setup utility, click **UEFI Setup → System Settings**, and verify that Legacy BIOS is set to Disabled.
 - The XClarity Controller Enterprise feature is required for operating-system deployment.
- For System x servers
 - Ensure that the Legacy BIOS option is disabled. From the BIOS/UEFI (F1) Setup utility, click **UEFI Setup → System Settings**, and verify that Legacy BIOS is set to Disabled.
 - Ensure that a Feature on Demand (FoD) key for remote presence is installed. You can determine whether remote presence is enable, disabled, or not installed on a server from the Servers page (see [Viewing device details](#)).
- For Flex System servers, ensure that the chassis is powered on.
- For NeXtScale servers, ensure that a Feature on Demand (FoD) key for remote presence is installed. You can determine whether remote presence is enable, disabled, or not installed on a server from the Servers page (see [Viewing device details](#)).
- For Converged and ThinkAgile appliances, it is recommended that you *do not* use XClarity Orchestrator to perform a bare-metal operating-system deployment.

Operating system considerations

- Ensure that you have all applicable operating-system licenses to activate the installed operating systems. You are responsible for obtaining licenses directly from the operating-system manufacturer.
- Ensure that the operating-system image that you intend to deploy is already loaded in the OS images repository. For information about importing images, see [Importing operating-system images](#).
- Operating-system images in the OS-images repository might not be supported only on certain hardware platforms. You can determine whether an operating system is compatible with a specific server from the [Lenovo OS Interoperability Guide website](#).
- Always install the latest operating system to ensure that you have the latest inbox I/O adapter device drivers that you need. For VMware, use the latest Lenovo Custom Image for ESXi, which includes support for the latest adapters. For information about obtaining that image, see the [VMware Support – Downloads webpage](#).

For more information about limitations for specific operating systems, see [Supported operating systems](#).

Network considerations

- Ensure that all required ports are open (see [Port availability for deployed operating systems](#)).
- Ensure that the resource manager is configured to use both management and data networks.
- Ensure that resource manager can communicate with the target server (both the baseboard management controller and the servers' data network) over both management and data network interfaces. To specify an interface to be used for operating-system deployment, see [Configuring network access](#) in the Lenovo XClarity Administrator online documentation.

For more information about the operating-system deployment network and interfaces, see [Network considerations](#) in the Lenovo XClarity Administrator online documentation.

- If the network is slow or unstable, you might see unpredictable results when deploying operating systems.
- You must use dynamically assigned IP addresses using DHCP. Static IP address are not supported.

For more information about the operating-system deployment network and interfaces, see [Configuring network access](#) and [Network considerations](#) in the Lenovo XClarity Administrator online documentation.

Storage and boot-option considerations

- You can install the operating system on only a local disk drive. Embedded hypervisor, M.2 drivers, and SAN storage are not supported.
- Each server must have a hardware RAID adapter or SAS/SATA HBA that is installed and configured. The software RAID that is typically present on the onboard Intel SATA storage adapter or storage that is set up as JBOD are not supported; however, if a hardware RAID adapter is not present, setting the SATA adapter to AHCI SATA mode enabled for operating-system deployment or setting unconfigured good disks to JBOD might work in some cases. For more information, see in the XClarity Orchestrator online documentation.
- Ensure that the UEFI boot option on the target server is set to “UEFI boot only” before you deploy an operating system. The “Legacy-only” and “UEFI first, then legacy” boot options are not supported for operating-system deployment.
- Each server must have a hardware RAID adapter that is installed and configured.

Attention:

- Only storage that is set up with hardware RAID is supported.
- The software RAID that is typically present on the onboard Intel SATA storage adapter or storage that is set up as JBOD are not supported; however, if a hardware RAID adapter is not present, setting the SATA adapter to **AHCI SATA mode** enabled for operating-system deployment or setting unconfigured good disks to JBOD might work in some cases.
- If a SATA adapter is enabled, the SATA mode *must not* be set to “IDE.”
- The NVMe storage that is connected to a server motherboard or HBA controller is not supported and must not be installed in the device; otherwise, OS deployment to non-NVMe storage will fail.
- Ensure that secure-boot mode is disabled for the server. If you are deploying a secure-boot mode enabled operating system (such as Windows), disable secure-boot mode, deploy the operating system, and then re-enable secure-boot mode.
- For ThinkServer servers, ensure that the following requirements are met.
 - The boot settings on the server must include a Storage OpROM Policy that is set to UEFI Only.
 - If you are deploying ESXi and there are network adapters that are PXE bootable, disable PXE support on the network adapters before deploying the operating system. The deployment is completed, you can re-enable PXE support, if desired.
 - If you are deploying ESXi and there are bootable devices in the boot-order list other than the drive on which the operating system is to be installed, remove the bootable devices from the boot-order list before deploying the operating system. After deployment is complete, you can add the bootable device back to the list. Ensure that the installed drive is at the top of the list.

For more information about storage-location settings, see [Configuring operating-system profiles](#).

Supported operating systems

Lenovo XClarity Orchestrator supports the deployment of several operating-systems. Only supported versions of the operating systems can be loaded into the XClarity Orchestrator OS-images repository.

Important:

- For information about operating-system deployment limitations for specific devices, see [Supported hardware and software](#) in the XClarity Orchestrator online documentation.
- The cryptographic management feature of XClarity Orchestrator allows limiting communication to certain minimum SSL/TLS modes. For example, if TLS 1.2 is selected, then only operating systems with an installation process that supports TLS 1.2 and strong cryptographic algorithms can be deployed through XClarity Orchestrator.

- Operating-system images in the OS-images repository might not be supported only on certain hardware platforms. You can determine whether an operating system is compatible with a specific server from the [Lenovo OS Interoperability Guide website](#).
- For OS and Hypervisor related compatibility and support information and resources for Lenovo servers and solutions, see the [Server OS Support Center webpage](#).

The following table lists the 64-bit operating systems that XClarity Orchestrator can deploy.

Operating system	Versions	Notes
Red Hat® Enterprise Linux (RHEL) Server	7.2 and later 8.x	Includes KVM Notes: <ul style="list-style-type: none"> • All existing and future minor versions are supported unless otherwise noted. • When importing the DVD version of the OS image, only DVD1 is supported. • When installing RHEL on ThinkSystem servers, RHEL v7.4 or later is recommended.
SUSE® Linux Enterprise Server (SLES)	12.3 and later 15.2 and later	Includes KVM and Xen hypervisors Notes: <ul style="list-style-type: none"> • All existing and future service packs are supported unless otherwise noted. • When importing the DVD version of the OS image, only DVD1 is supported.
VMware vSphere® Hypervisor (ESXi)	6.0.x 6.5.x 6.7.x 7.0.x	Base VMware vSphere Hypervisor (ESXi) images and Lenovo VMware ESXi Custom images are supported. Lenovo VMware ESXi Custom images are customized for select hardware to give you online platform management, including updating and configuring firmware, platform diagnostics, and enhanced hardware alerts. Lenovo management tools also support simplified management of the ESXi with select System x servers. This image is available for download from the VMware Support – Downloads webpage . The license that is provided with the image is a 60-day free trial. You are responsible for meeting all VMware licensing requirements. Important: <ul style="list-style-type: none"> • All existing and future update packs are supported unless otherwise noted. • Base ESXi images (without Lenovo customization) include only basic in-box device drivers for network and storage. The base image does not include the out-of-box device drivers (which are included in Lenovo VMware ESXi Custom images). • For some versions of Lenovo VMware ESXi Custom images, separate images might be available for ThinkSystem, System x, and ThinkServer. Only one image for a specific release can exist in the OS-images repository at a time. • ESXi deployment is not supported for certain older servers. For information about which servers are supported, see the Lenovo OS Interoperability Guide website.

Operating-system image profiles

Import an OS image generates predefined OS profiles. Each predefined profile includes the OS image and installation options for that image.

You can modify the profiles to configure credentials, network, and storage settings. You can also create new profiles based on the predefined OS policies. For more information, see [Configuring operating-system profiles](#).

The following table lists the predefined OS image profiles that are created when you import an operating-system image. This table also lists the packages that are included in each profile.

Operating system	Profile	Packages included in the profile
Red Hat Enterprise Linux (RHEL) Note: Includes KVM	Basic	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686
	Minimal	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686
	Virtualization	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages
SUSE Linux Enterprise Server (SLES) 12.3 and later	Basic	<pattern>32bit</pattern> <pattern>Basis-Devel</pattern> <pattern>Minimal</pattern> <pattern>WBEM</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>gateway_server</pattern> <pattern>lamp_server</pattern> <pattern>mail_server</pattern> <pattern>ofed</pattern> <pattern>printing</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>

Operating system	Profile	Packages included in the profile
	Minimal	<pattern>Minimal</pattern> <pattern>file_server</pattern> <pattern>sap_server</pattern>
	Virtualization-KVM	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>kvm_server</pattern> <pattern>kvm_tools</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>
	Virtualization-Xen	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern>
SUSE Linux Enterprise Server (SLES) 15.2 and later	Basic	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Minimal	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>

Operating system	Profile	Packages included in the profile
	Virtualization-KVM	<pre> <pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package> </pre>
	Virtualization-Xen	<pre> <pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package> </pre>
VMware vSphere® Hypervisor (ESXi)	Virtualization	Base VMware vSphere Hypervisor (ESXi) images and Lenovo VMware ESXi Custom images are supported.

Port availability for deployed operating systems

Some ports are blocked by certain operating-system profiles. The following tables list the ports that are open (not blocked).

Ensure that the hypervisor that is running the Lenovo XClarity Orchestrator appliance allows network traffic (TCP/UDP) on ports 139, 445, 3001, 3900, 8443. These are required for operating-system deployment.

RHEL Virtualization profile

By default, the Red Hat Enterprise Linux (RHEL) Virtualization profile blocks all ports except for those that are listed in the following table.

Table 1. Port availability for RHEL Virtualization profiles

Port	TCP or UDP	Direction	Communication description
22	TCP	Inbound	SSH communication
53	TCP, UDP	Outbound/Inbound	Communication with RHEL KVM networking devices
67	TCP, UDP	Outbound/Inbound	Communication with RHEL KVM networking devices

Table 1. Port availability for RHEL Virtualization profiles (continued)

Port	TCP or UDP	Direction	Communication description
161	UDP	Outbound	Communication with SNMP agents
162	UDP	Inbound	Communication with SNMP agents
427	TCP, UDP	Outbound/Inbound	Communication with SLP service agent, SLP directory agent
3001	TCP	Outbound/Inbound	Communication with management software image-deployment service
15988	TCP	Outbound	CIM-XML over HTTP communication
15989	TCP	Outbound	CIM-XML over HTTP communication
49152 - 49215	TCP	Outbound/Inbound	KVM Virtual Server communication

RHEL Basic and Minimal profiles

By default, the RHEL Basic and Minimal profiles block all ports except for those that are listed in the following table.

Table 2. Port availability for RHEL Basic and Minimal profiles

Port	TCP or UDP	Direction	Communication description
22	TCP	Inbound	SSH communication
3001	TCP	Outbound/Inbound	Management software image-deployment service communication

SLES Virtualization, Basic, and Minimal profiles

For SUSE Linux Enterprise Server (SLES), some open ports are dynamically assigned based on the operating system version and profiles. For a complete list of open ports, see your SUSE Linux Enterprise Server documentation.

VMware ESXi Virtualization profile

For a complete list of open ports for VMware vSphere Hypervisor (ESXi) with Lenovo customization, see the VMware documentation for ESXi on the [VMware Knowledge Base website](#).

Importing operating-system images

Before you can deploy a licensed operating system to managed servers, you must import the image into the OS images repository.

About this task

For information about operating system images that you can import and deploy, including supported base and custom operating systems, see [Supported operating systems](#).

For ESXi only, you can import multiple ESXi images with same major/minor version to the OS images repository.

For ESXi only, you can import multiple customized ESXi images with same major/minor version and build number to the OS images repository.

When you import an operating system image, XClarity Orchestrator:

- Ensures that there is sufficient space in the OS-images repository before importing the operating system. If you do not have sufficient space to import an image, delete an existing image from the repository and attempt to import the new image again.
- Creates one or more profiles of that image and stores the profile in the OS-images repository. Each *profile* includes the OS image and installation options. For more information about predefined OS image profiles, see [Operating-system image profiles](#).

Note: 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).

Procedure

To import an operating-system image into the OS-images repository, complete the following steps.

Step 1. Obtain a licensed ISO image of the operating system.

Note: You are responsible for obtaining applicable licenses for the operating system.

Step 2. From the XClarity Orchestrator menu bar, click **Provisioning** (🔗) → **OS Deployment**, and click the **OS Management** tab to display the OS Management page.

Step 3. Click **OS Images** in the left navigation to display the OS Images card.

OS Management

Here is the list of OS images managed by and stored in this management server. You can import a new OS image from your local workstation, or delete an OS image from this repository.

OS Storage Usage: 394.2 MB of 185.8 GB.

OS Images

🔄 📁 🗑️ 📄 All Actions ▾ Filters ▾ 🔍 Search ✕

<input type="checkbox"/>	OS Name ^	Version	Status
<input type="checkbox"/>	esxi7.0_3-20036589.1	7.0	Ready

0 Selected / 1 Total Rows per page: 10 ▾

Step 4. Click the **Import Files** icon (📁) to display the Import OS Images dialog.

Step 5. Drag and drop the .iso image that you want to import, or click **Browse** to find the ISO image that you want to import

Step 6. Optional: **Optional:** Select a checksum type, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded OS image. The value must come from a secure source from an organization that you trust. If the uploaded image matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the image again or check the checksum value.

The following checksum types are supported: MD5, SHA1, and SHA256.






Step 7. Click **Import**.

XClarity Orchestrator uploads the OS image in the OS images repository and add the predefined OS profiles to the **OS Profiles** tab.

Tip: The ISO image is uploaded over a secure network connection. Therefore, network reliability and performance affect how long it takes to import the image.

After you finish

From this page, you can perform the following actions.

- Delete a selected OS image by clicking the **Delete** icon (.
- View and edit OS profiles by clicking click XClarity Orchestrator menu bar, click **Provisioning** () → **OS Deployment**, and click the **OS Profiles** tab, select the profile, and click the **Edit** icon () (see Configuring operating-system profiles).
- Delete OS profiles by clicking click XClarity Orchestrator menu bar, click **Provisioning** () → **OS Deployment**, and click the **OS Profiles** tab, select the profiles, and click the **Delete** icon (.

Note: If you delete the last remaining predefined profile for an operating system, the operating system is also deleted.

Configuring operating-system profiles



Operating system profiles are created automatically when you import an operating system. The profiles that are created are based on the operating system type and version. You can modify the profile, including OS credentials, hostname, networking and storage settings, license keys, and storage location.

Before you begin

Review the considerations before deploying an operating system to a managed server device. For information, see [Operating-system deployment considerations](#).

Procedure

To configure an OS profile for deployment, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click **Provisioning** () → **OS Deployment**, and click the **OS Profiles** tab to display the OS Profiles page.
- Step 2. Select the OS profile.
- Step 3. Click the **Edit** icon () to display the OS Profile Details card.

OS Profile
Based on esxi7.0_3-20036589.1 and Virtualization profile.

Name*
esxi7.0_3-20036589.1-x86_64-install-Virtualization

Description
Generated by default

OS Credentials
ESXi/Linux

Username
root

New Password*

Confirm Password*

Hostname

Use default hostname ⓘ

Network Setting

Use DHCP

MAC Address Setting

Use AUTO ⓘ

Storage

Use Disk Drive

Step 4. Configure the profile attributes.

- **Name.** Modifying the profile name creates a new OS profile.
- **Description.** Modify the description for this OS profile.
- **OS Credentials.** Enter the OS credentials for the administrator account to be used to log in to the operating system.
- **Hostname.** Select what to use for the hostname. You can choose one of the following values.
 - **Use default hostname.** (default) The hostname is “node” followed by the first 11 characters of the device ID (for example, nodeABC31213310).
- **Network Setting.** Select the IP settings for this profile. You can choose one of the following values.
 - **DHCP.** (default) Use your existing DHCP infrastructure to assign IPv4 addresses to servers.
- **MAC Address Setting.** Select the MAC address of the port on the host where the operating system is to be installed. You can choose one of the following values.

Note: Virtual network ports are not supported. Do not use one physical network port to simulate multiple virtual network ports.

- **Use AUTO.** (default) Automatically detect the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the server is automatically restarted to use the newly detected MAC address for deployment. XClarity Administrator resource manager can automatically detect network ports in slots 1 – 16. At least one port in slots 1 – 16 must have a connection to the applicable resource manager.

If you want to use a network port in slot 17 or greater for the MAC address, you cannot use AUTO.

- **Storage.** Select the storage location where you want to deploy the operating-system image.
 - **Use Disk Drive.** Install the operating-system image on the first enumerated local RAID disk drive in the managed server. Only disk drives attached to a RAID-controller or SAS/SATA HBA are supported.

If the RAID configuration on the server is not configured correctly, or if it is inactive, the local disk might not be visible to the orchestrator server. To resolve the issue, enable the RAID configuration through configuration patterns (see [Learning a server-configuration pattern from an existing server](#)) or through the RAID management software on the server.

Notes:

- If an M.2 drive is also present, the disk drive must be configured for hardware RAID.
- If an SATA adapter is enabled, the SATA mode *must not* be set to **IDE**.
- For ThinkServer servers, configuration is available only through the RAID management software on the server.

Step 5. Click **Save**.

After you finish

You can perform the following actions.

- Assign an OS profile to one or more servers from the **Assign and Deploy** tab by clicking selecting servers and then **Assign** icon (↔) or by clicking the **Assign** icon (↔) and then selecting a group of servers. After you select the OS profile, you can choose to assign the OS profile to.
 - **All applicable devices (overwrite assigned profiles)**
 - **Applicable devices with no profile assignment**
 - **Only selected applicable devices (overwrite assigned profiles)**
 - **Only selected applicable devices with no profile assignment**
- Delete selected OS profiles by clicking the **Delete** icon (☒).

Note: If you delete the last remaining predefined profile for an operating system, the operating system is also deleted.

Deploying an operating-system image

You can use Lenovo XClarity Orchestrator to deploy an operating-system to your managed servers.

Before you begin

Read the operating-system deployment considerations before you attempt to deploy operating systems on your managed servers (see [Operating-system deployment considerations](#)).

Attention: If the server currently has an operating system installed, deploying an OS-image profile will overwrite the current operating system.

Procedure

To deploy an operating-system image to one or more managed servers, complete one of the following procedures.

- **To specific devices**
 1. From the XClarity Orchestrator menu bar, click **Provisioning** (🔧) → **OS Deployment**, and click the **Assign and Deploy** tab to display the Assign and Deploy card.

Assign and Deploy

Assign an OS profile on managed servers or group, then perform OS deployment.

All Actions ▾ Filters ▾

 Search X

<input type="checkbox"/>	Devices ▾	IP Addresses :	Deploy Status :	Assigned Profile	Groups :
<input type="checkbox"/>	Draco-19-11	10.241.19.11, 169.:	Ready	No Assignm... ▾	Not Available

0 Selected / 1 Total Rows per page: 10 ▾

2. Select one or more servers on which you want to deploy an operating system.
3. For each target server, select the OS profile to be deployed from the drop-down list in the **OS Profiles** column. Ensure that you select an OS profile that is compatible with the target server.
4. Verify that the deployment status in the **Status** column is Ready for all selected servers.
5. Click the **Deploy** icon () to display the Deploy Profile dialog.
6. Click the **Deploy** to initiate the operating-system deployment. A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** () → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

- **To all devices in specific a group**

1. From the XClarity Orchestrator menu bar, click **Provisioning** () → **OS Deployment**, and click the **Assign and Deploy** tab to display the Assign and Deploy card.
2. Assign an OS profile to the group of servers.
 - a. Click the **Assign** icon () to display the Assign Profile dialog.

Assign Profile X

Select a profile to assign to multiple resources. The profile will be assigned only to applicable resources.

Profile to assign

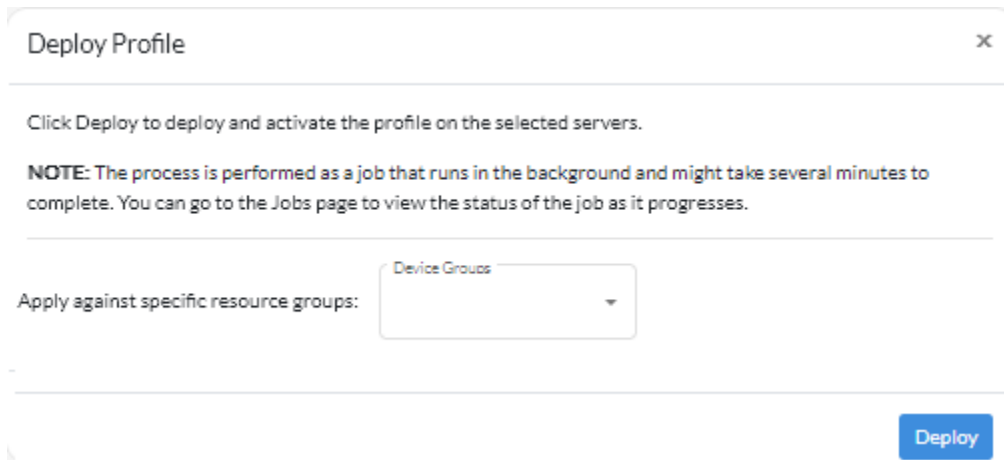
Apply against specific resource groups:

Assign profile to:

- All applicable devices (overwrite assigned profiles)
- Applicable devices with no profile assignment
- Only selected applicable devices (overwrite assigned profiles)
- Only selected applicable devices with no profile assignment

- b. Select the profile to be assigned.

- c. Select the group of devices to be assigned.
 - d. Choose which devices in the group to assign.
 - **All applicable devices (overwrite assigned profiles)**
 - **Applicable devices with no profile assignment**
 - **Only selected applicable devices (overwrite assigned profiles)**
 - **Only selected applicable devices with no profile assignment**
 - e. Click **Deploy**.
3. Click the **Deploy** icon (🗲) to display the Deploy Profile dialog.



4. Select the group of devices on which you want to deploy the assigned OS profile.
5. Click the **Deploy** to initiate the operating-system deployment. A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

Provisioning updates to managed resources

You can use Lenovo XClarity Orchestrator to maintain current software levels on Lenovo XClarity Administrator resource managers and managed servers. You can use the updates catalog to know what software levels are available, use update-compliance policies to identify which resources need to be updated based on custom criteria, and then deploy the desired updates to those resources.

Procedure

The following figure illustrates the workflow for updating managed resources.



Step 1. Update the catalog

The *updates repository* contains a catalog and the update packages that can be applied to managed resources.

The *catalog* contains information about updates that are currently available. The catalog organizes the updates by resource types (platforms) and components. When you update the catalog, XClarity Orchestrator retrieves information about the latest available updates from the Lenovo Support website and stores the information in the updates repository.

Important: XClarity Orchestrator must be connected to the Internet to update the catalog.

When new update packages become available, you must import the applicable update packages before you can apply an update. Updating the catalog does not automatically import the update packages.

When XClarity Orchestrator is initially installed, the updates repository is empty.

Step 2. **Download or import update packages into the repository**

If XClarity Orchestrator is connected to the Internet, you can download update packages that are listed in the updates catalog directly from the Lenovo Support website. If XClarity Orchestrator is not connected to the Internet, you can manually import update packages that you previously downloaded from the [Lenovo Data Center Support website](#) to a workstation that has network access to the XClarity Orchestrator host.

If you choose to download a minor release, the prerequisite update packages are also downloaded.

When you manually import repository packs, you must import the payload (.tgz), metadata (.xml), change log (.chg) and readme (.txt).

When you manually import updates, you must import the required files base on the resource type.

- For ThinkSystem V3 servers, import the single update package (*.zip). This zip file contains the payload, metadata files (several *.json files), change log file (*.chg) and readme file (*.txt).
- For ThinkEdge Client devices, import the payload (Windows .exe). The readme (.txt) is optional. Note that only the **BIOS flash utility package for Windows** update is currently supported.
- For Management Hub, import the single update-package file (.tgz). This file contains the payload, metadata, change history, and readme files.
- For all other resources (including XClarity Administrator, ThinkEdge servers, ThinkSystem V1 and V2, and legacy devices), import the payload (.zip, .uxz, .tar.gz, .tar, .bin), metadata (.xml), change log (.chg) and readme (.txt).

For more information about importing updates, see [Downloading and importing updates](#).

Step 3. **Create and assign update-compliance policies**

Update-compliance policies ensure that the software or firmware on certain managed resources are at the current or specific level by flagging the resources that need attention. Each update-compliance policy identifies which resources are monitored and which software or firmware level must be installed to keep the resources in compliance. XClarity Orchestrator then uses these policies to check the status of managed resources and to identify resources that are out of compliance.

When you create an update-compliance policy, you can choose to have XClarity Orchestrator flag a resource when the software or firmware on the resource is down level.

After an update-compliance policy is assigned to a resource, XClarity Orchestrator checks the compliance status of the resource when the updates repository changes. If the software or firmware on the resource is not compliant with the assigned policy, XClarity Orchestrator flags that

resource as not compliant on the Apply / Activate page, based on the rules that you specified in the update-compliance policy.

For example, you can create an update-compliance policy that defines the baseline software level for XClarity Administrator, and then assign that policy to all XClarity Administrator resource managers. When the updates catalog is refreshed and when a new update is downloaded or imported, the XClarity Administrator instances might become out of compliance. When that happens, XClarity Orchestrator updates the Apply / Activate page to show which XClarity Administrator instances are not compliant and generates an alert.

For more information about creating update-compliance policies, see [Creating and assigning update-compliance policies](#).

Step 4. **Apply and activate updates**

XClarity Orchestrator does not automatically apply updates. To update software resources, you must manually apply and activate the update on selected resources that are not compliant with the assigned update-compliance policy.

XClarity Orchestrator does not directly update resources. Instead, it sends a request to the applicable resource manager to perform the update, and then tracks the progress of the request. XClarity Orchestrator identifies the dependencies that are required to perform the update, ensures that the target resources are updated in the correct order, transfers the applicable update packages to the resource manager, and creates a request to start a job on the resource manager to perform the update.

For more information about applying updates, see [Applying and activating updates to resource managers](#) and [Applying and activating updates to managed servers](#).

Update deployment considerations

Before deploying updates using Lenovo XClarity Orchestrator, review the following important considerations.

- For the best performance, ensure that Lenovo XClarity Administrator resource managers are running v3.2.1 or later
- Ensure that the updates repository contains the update packages that you intend to apply. If not, refresh the product catalog, and download the appropriate updates (see [Downloading and importing updates](#)).
- Ensure that no jobs are currently running on the target resource. If jobs are running, the update job is queued until all other jobs have completed.
- If the resource has an assigned update-compliance policy that results in compliance violations, you must correct the violations either by adjusting the compliance policy or assigning an alternate policy.
- If you choose to install an update package that contains updates for multiple components, all components to which the update package applies are updated.

Resource considerations

- The updates function supports updating only servers and XClarity Administrator resource managers. For ThinkSystem SR635 and SR655, only BMC and UEFI firmware-updates are supported.

For ThinkSystem and ThinkAgile devices, firmware updates are not supported for baseboard managed controller and UEFI backup banks. Instead, update the primary bank and then enable auto promotion.

- Before updating managed devices, ensure that you read important update considerations (see [Firmware-update considerations](#) in the Lenovo XClarity Administrator online documentation).

- Before updating XClarity Administrator resource managers, ensure that you read the update considerations for XClarity Administrator (see [Updating the XClarity Administrator management server](#) in the Lenovo XClarity Administrator online documentation).
- Before updating XClarity Administrator resource managers, back up the virtual appliance by creating a clone (see [Backing up XClarity Administrator](#) in the Lenovo XClarity Administrator online documentation).
- Ensure that the resources that you want to update have an assigned update-compliance policy.
- XClarity Orchestrator transfers the applicable updates to the resource manager during the update process. Ensure that there is enough disk space in the management server to contain the updates.
- For ThinkEdge Client devices, only BIOS updates on servers running Windows 10 version 1809 or later 64-bit operating system is supported. Special editions (such as 10 S or 10x) are not currently supported.
- You cannot download firmware updates for the following servers from the web interface. Instead, manually download updates from [ibm.com](#) and then import the updates.
 - IBM System x iDataPlex dx360 M4
 - IBM System series M4
 - IBM System x3100 M5 and x3250 M
 - IBM System x3850 X5 and x3950 X5
 - IBM System x3850 X6 and x3950 X6
 - IBM Flex System

Repository considerations

- Ensure that the updates repository contains the update packages that you intend to apply. If not, refresh the product catalog, and download the appropriate updates (see [Downloading and importing updates](#)). You can choose to install prerequisite updates in addition to the target update. All prerequisite updates must be downloaded to the repository before they can be applied.

In some cases, multiple versions might be needed to apply an update, and all versions need to be downloaded to the repository.

Update-process considerations

- If you choose to install an update package that contains updates for multiple components, all components to which the update package applies are updated.
- When a request is made to apply updates to an XClarity Administrator resource manager and one or more devices that are managed by that resource manager, updates are applied to the resource manager first.
- While an update is in progress, the target resource is locked. You cannot initiate other management tasks on the target resource until the update process is complete.
- After an update is applied to a resource, one or more restarts might be required to fully activate the update. You can choose whether to restart the resource immediately or delay the activation, or prioritize activation. If you choose to restart immediately, XClarity Orchestrator minimizes the number of restarts that are required. If you choose to delay activation, the updates are activated the next time the resource is restarted. If you choose prioritized activation, the updates are immediately activated on the baseboard management controller, and all other updates are activated the next time the device is restarted.
- If you choose to restart the resource during the update process (*immediate activation*), ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different resource.
- Some firmware updates require a monitor to be connected to the target device. The update process might fail if a monitor is not connected.

Downloading and importing updates

Updates packages must be available in the updates repository before you can apply updates to managed resources.

Before you begin

To retrieve the latest information about update packages, select the resource type, and click **Check for Updates** → **Update Selected** to get information about all available update packages or click **Check for Updates** → **Update Selected – Latest only** to get information about only the latest update package for that resource. Then, sort the table using the **Name** column to order the updates by version.

XClarity Orchestrator uses a separate drive for the updates repository. The minimum size requirement for this drive is 100 GB.

About this task

You can download or import a single XClarity Administrator repository pack or one or more update packages at a time.








- **XClarity Administrator repository packs** Lenovo XClarity Administrator repository packs contain the latest firmware updates that are available at a specific point in time for most supported devices and a refreshed default firmware-compliance policy. When you download a repository pack from the [XClarity Administrator download webpage](#), each update package in the repository pack is extracted and imported into the updates repository, and then the repository payload file is deleted. The refreshed default firmware-compliance policy is also imported as a predefined policy. You cannot modify this predefined policy.

The following repository packs are available.

- **Invgy_sw_lxca_cmmswitchrepo** $x-x.x.x_anyos_noarch$. Contains firmware updates for all CMMs and Flex System switches.
- **Invgy_sw_lxca_storagerackswitchrepo** $x-x.x.x_anyos_noarch$. Contains firmware updates for all RackSwitch switches and Lenovo Storage devices.
- **Invgy_sw_lxca_systemxrepo** $x-x.x.x_anyos_noarch$. Contains firmware updates for all Converged HX Series, Flex System, and System x servers.
- **Invgy_sw_thinksystemrepo** $x-x.x.x_anyos_noarch$. Contains firmware updates for all ThinkSystem servers.
- **Invgy_sw_lxca_thinksystemv2repo** $x-x.x.x_anyos_noarch$. Contains firmware updates for all ThinkSystem V2 servers.
- **Invgy_sw_lxca_thinksystemv3repo** $x-x.x.x_anyos_noarc$. Contains firmware updates for all ThinkAgile and ThinkSystem V3 servers.

When you manually import repository packs, you must import the payload (.tgz), metadata (.xml), change log (.chg) and readme (.txt).

You can determine the status of a repository pack from the **Status** column on the Repository Management page. This column contains the following values.

-  **Not Downloaded**. The repository pack is available from the web but not downloaded and extracted to the updates repository.
-  **Pending Download**. The repository pack is in queue for downloading from the Internet.
-  **Downloading**. The repository pack is being downloaded from the Internet.
-  **Pending Apply**. The repository pack is in queue for extracting update packages in the repository pack to the updates repository.
-  **Applying**. The update packages in the repository pack are being extracted to the updates repository.
-  **x of y Downloaded**. Some but not all repository packs are downloaded and extracted to the updates repository. The numbers in parentheses indicate the number of downloaded updates and the number of available updates.
-  **Downloaded**. All update packages in the repository pack are stored in the updates repository, and the repository-pack payload file is deleted.

- **Update packages** If XClarity Orchestrator is connected to the Internet, you can download update packages that are listed in the updates catalog directly from the Lenovo Support website. If XClarity Orchestrator is not connected to the Internet, you can manually import update packages that you previously downloaded from the [Lenovo Data Center Support website](#) to a workstation that has network access to the XClarity Orchestrator host.






If you choose to download a minor release, the prerequisite update packages are also downloaded.

When you manually import updates, you must import the required files base on the resource type.

- For ThinkSystem V3 servers, import the single update package (*.zip). This zip file contains the payload, metadata files (several *.json files), change log file (*.chg) and readme file (*.txt).
- For ThinkEdge Client devices, import the payload (Windows .exe). The readme (.txt) is optional. Note that only the **BIOS flash utility package for Windows** update is currently supported.
- For Management Hub, import the single update-package file (.tgz). This file contains the payload, metadata, change history, and readme files.
- For all other resources (including XClarity Administrator, ThinkEdge servers, ThinkSystem V1 and V2, and legacy devices), import the payload (.zip, .uxz, .tar.gz, .tar, .bin), metadata (.xml), change log (.chg) and readme (.txt).

Important: The maximum size of all files to be imported at one time is 8 GB.


You can determine whether specific updates files are stored in the updates repository from the **Status** column on the Repository Management page. This column contains the following values.

-  **Not Downloaded.** The entire update package or the individual update is available from the web but not currently stored in the repository.
-  **Pending Download.** The update package is in queue for downloading from the Internet.
-  **Downloading.** The update package is being downloaded from the Internet.
-  **x of y Downloaded.** Some but not all updates in the update package are stored in the repository. The numbers in parentheses indicate the number of stored updates and the number of available updates.
-  **Downloaded.** The entire update package or the individual update is stored in the repository.

Note: Some update packages are used by multiple platforms. If you select an update package in the table, it is selected under every platform that uses it.

Procedure

To download or manually import update packages and repository packs, complete one of the following steps.

- If XClarity Orchestrator is connected to the Internet, download update packages that are listed in the catalog.
 1. From the XClarity Orchestrator menu bar, click **Provisioning**  → **Updates** and then click **Repository Management** to display the Repository Management card. The Repository Management card lists information about update packages in a tree structure, organized by resource types, components, and update packages. By default, resources types for only *managed* resources are listed in the table. Click **Show Available Resource Types** to list *all supported* resource types that are available in catalog.

Repository Management

Manage the updates repository, including importing update packages from the local system, and downloading catalog information and update packages from the Internet. Update the catalog to retrieve the latest information before downloading update packages.

Repository Usage: 18.2 GB of 93.2 GB.

If the selected package is a minor release then the prerequisite update packages will also be downloaded.

Show managed resource types only

Update Catalog All Actions

<input type="checkbox"/>	Name	Resour	Versior	Releas	Status	Packag	Releas
<input type="checkbox"/>	> IBM Flex System x220 Compute Node	79...				77...	
<input type="checkbox"/>	> IBM Flex System x222 Compute Node	79...				65...	
<input type="checkbox"/>	> IBM Flex System x240 Compute Node	87...				1...	
<input type="checkbox"/>	> IBM Flex System x280/x480/x880 X6 Compute Node	79...				1...	
<input type="checkbox"/>	> IBM Flex System x440 Compute Node	79...				85...	
<input type="checkbox"/>	> Lenovo Converged HX5510/HX5510-C/HX3510-G/HX7	86...				5...	
<input type="checkbox"/>	> Lenovo Devices Repository Pack	Re...				27...	
<input type="checkbox"/>	> Lenovo Flex System x240 Compute Node	71...				6...	
<input type="checkbox"/>	> Lenovo Flex System x240 M5 Compute Node	95...				6...	
<input type="checkbox"/>	> Lenovo Flex System x280/x480/x880 X6 Compute Node	71...				6...	

0 Selected / 14 Total Rows per page: 10

- (Optional) Download information about the latest available updates for specific resource types by selecting one or more resources types in the table, clicking **Check for Updates**, and then clicking one of the following options.
 - Update Selected.** Retrieves information about all update versions that are available for the selected resource.
 - Updated Selected – Latest Only.** Retrieves information about the most current update version that is available for the selected resource. For ThinkEdge Client devices, only **Updated Selected – Latest Only** is supported.

A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (🔍) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)
- Select one or more repository packs, resources, components, and update versions that you want that you want to download. You can expand the resource types and components to display the list of update versions that are available in the catalog for each resource type and component.
- Click the **Download Updates** icon (⬇️) to download the selected updates. A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (🔍) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

When the download is complete, the **Download Status** for the selected updates changes to “Downloaded.”

- If XClarity Orchestrator is not connected to the Internet, manually import update packages and repository packs.
 1. Download the files for each repository pack and update package to a workstation that has network access to the XClarity Orchestrator host using a web browser. Use these links to download the applicable updates.
 - For Lenovo XClarity Administrator updates, go to the [XClarity Administrator download webpage](#). You can also download XClarity Administrator updates using Lenovo XClarity Essentials OneCLI commands. The following example downloads the latest update (including the payload) to the /lxca-updates directory and stores the log files in the /logs/lxca-updates directory. For more information about OneCLI, see [acquire command](#) in the Lenovo XClarity Essentials OneCLI online documentation.

```
Onecli.exe update acquire --lxca --ostype none --mt lxca --scope latest --superseded --xml --dir ./lxca-updates --output ./logs/lxca-updates
```
 - For firmware-update repository packs, go to the [XClarity Administrator download webpage](#).
 - For firmware-updates, go to the [Lenovo Data Center Support website](#).
 2. From the XClarity Orchestrator menu bar, click **Provisioning** (🔌) → **Updates** and then click **Repository Management** to display the Repository Management card.
 3. Click the **Import** icon (📁) to display the Import Updates dialog.
 4. Drag and drop the downloaded files to the Import dialog, or click **Browse** to locate the files.

Attention:

- For ThinkEdge Client devices, you must import the payload file for each update package. The readme file is optional.
 - For all other devices, you must import the metadata file as well as the image or payload file, change history file, and readme file for each repository pack and update package. Any files that are selected but are not specified in the metadata file are discarded. If you do not include the metadata file, the update is not imported.
 - Do not import other files that might be found on the Lenovo download websites.
 - If you do not include the metadata file (.xml or .json) for the repository pack or update package, the repository pack or update package is not imported.
5. Click **Import**. A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📧) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

When the files are imported and stored in the repository, the **Download Status** column changes to “Downloaded.”

After you finish

You can perform the following actions from the Repository Management card.

- Review the readme file, change history file, and list of fixed common vulnerabilities and exposures (CVEs) for a specific update by clicking the information (ℹ️) icon in the **Release Notes** column. You can also find a list of fixed CVEs by hovering the cursor over the **Fixed CVEs** column. Click on the CVE ID to view detailed information about the CVE from the National Vulnerability Data website.

The **Release Notes** and **Fixed CVEs** columns are hidden by default. To show these columns in the table, click **All Actions** → **Toggle Columns**.

- Delete only the image (payload) file for each selected update by clicking the **Delete only payload files** icon (🗑️). Information about the update (the XML metadata file) remains in the repository, and the download status changes to “Not downloaded.”

Important:

- The payload for repository packs is deleted automatically after the update packages are extracted during the download or import process.
- You cannot delete payloads from update packages that are used in update-compliance policies. You must first remove the update package from the policies (see [Creating and assigning update-compliance policies](#)).
- Some update packages are common for multiple platforms and components. Deleting a common update package affects all platforms and components that use it.

Creating and assigning update-compliance policies

You can create an update-compliance policy based on the acquired updates in the updates repository. You can then assign the policy to one or more XClarity Administrator resource managers or managed servers.

Before you begin

When you create an update-compliance policy, you select the target update version to be applied to the resources that will be assigned to the policy. Ensure that update files for the target version are in the updates repository before you create the policy.

When you download or import a firmware-update repository pack, the predefined firmware-compliance policies in the repository pack are added to the updates repository. This is considered a *predefined policy*, which cannot be modified or deleted.

About this task

Update-compliance policies ensure that the software or firmware on certain managed resources are at the current or specific level by flagging the resources that need attention. Each update-compliance policy identifies which resources are monitored and which software or firmware level must be installed to keep the resources in compliance. XClarity Orchestrator then uses these policies to check the status of managed resources and to identify resources that are out of compliance.

When you create an update-compliance policy, you can choose to have XClarity Orchestrator flag a resource when the software or firmware on the resource is down level.

After an update-compliance policy is assigned to a resource, XClarity Orchestrator checks the compliance status of the resource when the updates repository changes. If the software or firmware on the resource is not compliant with the assigned policy, XClarity Orchestrator flags that resource as not compliant on the Apply / Activate page, based on the rules that you specified in the update-compliance policy.

For example, you can create an update-compliance policy that defines the baseline software level for XClarity Administrator, and then assign that policy to all XClarity Administrator resource managers. When the updates catalog is refreshed and when a new update is downloaded or imported, the XClarity Administrator instances might become out of compliance. When that happens, XClarity Orchestrator updates the Apply / Activate page to show which XClarity Administrator instances are not compliant and generates an alert.

Procedure

To create and assign an update-compliance policy, complete the following steps.

Step 1. Create an update-compliance policy.

1. From the XClarity Orchestrator menu bar, click **Provisioning** (🔗) → **Updates** and then click **Policy Management** to display the Policy Management card.

Policy Management

Policy Management allows you to create or modify a policy based on the acquired updates in the Firmware Repository.

ⓘ You cannot edit or delete a compliance policy that is assigned. ✕

🔄 ⊕ 🗑️ ✍️ 📄 🔗 All Actions ▾ Filters ▾ 🔍 Search ✕

<input type="checkbox"/>	Compliance Policy N	Usage Status :	Compliance Policy O	Last Modified :	Description :
<input type="checkbox"/>	ThinkAgile_VX_0...	← Not Assigned	👤 User Defined	10/4/22, 6:08 PM	ThinkAgile VX.M...
<input type="checkbox"/>	v2.6.0-2020-01-...	← Not Assigned	👤 User Defined	10/4/22, 6:23 PM	Production firmw...
<input type="checkbox"/>	v3.2.0-2021-07-...	← Not Assigned	👤 User Defined	10/4/22, 6:34 PM	Production firmw...
<input type="checkbox"/>	v3.6.0-2022-06-...	← Not Assigned	👤 User Defined	10/4/22, 6:42 PM	Production firmw...
<input type="checkbox"/>	ThinkAgile-VX-5e...	← Not Assigned	👤 User Defined	10/4/22, 6:54 PM	System and Com...
<input type="checkbox"/>	ThinkAgile-VX-5e...	← Not Assigned	👤 User Defined	10/4/22, 7:07 PM	System and Com...
<input type="checkbox"/>	v3.6.0-2022-06-...	← Not Assigned	👤 User Defined	10/4/22, 7:25 PM	Production firmw...
<input type="checkbox"/>	v3.6.0-2022-06-...	← Not Assigned	👤 User Defined	10/4/22, 7:33 PM	Production firmw...
<input type="checkbox"/>	v2.6.0-2019-12-...	← Not Assigned	👤 User Defined	10/4/22, 7:41 PM	Production firmw...

0 Selected / 9 Total Rows per page: 10 ▾

2. Click the **Create** icon (⊕) to display the Create compliance policy dialog.
3. Specify the name and optional description for the policy.
4. Specify the trigger for the policy. This can be one of the following values.
 - **Flag if not exact match.** If the software or firmware version that is installed on resource is *earlier or later* than the target firmware version in the update-compliance policy, the resource is flagged as not compliant. For example, if you replace a network adapter in a server, and the firmware on that network adapter is different than the target firmware version in the assigned update-compliance policy, the sever is flagged as Not Compliant.
 - **Do not flag.** Resources that are out of compliance are not flagged.
5. Click the **Rules** tab to add compliance rules for this policy.
 - a. Select the type of resource for this policy.
 - b. Specify the compliance target for the applicable resource and components. For resources with components, you can choose one of the following values.
 - **Custom.** The compliance target for each resource component defaults to the current latest version in the repository for that component.
 - **Do not update.** The compliance target for each resource component defaults to **Do not update**. Note that if you change the default value for any component, the compliance target for the overall resource changes to **Custom**. For resources without components and for each component, you can choose one of the following values.

- *{firmware_level}*. Specifies that the firmware on the component must be at the selected baseline firmware version.
- **Do not update**. Specifies that the firmware on the component is not to be updated. Note that firmware on the backup (secondary) management controller is not updated by default.

c. Click the **Add** icon (⊕) to add additional rules, and click the **Delete** icon (⏏) to delete rules.

6. Click **Create**.

Step 2. From the XClarity Orchestrator menu bar, click **Provisioning** (⚙️) → **Updates** and then click **Apply and Activate** to display the Apply and Activate card.

Step 3. Assign the update-compliance policy to resources.

- **To a single resource** For each resource, select a policy from the **Assigned Compliance Policy** column drop-down list.

You can select from a list of compliance policies that are applicable to the resource. If a policy is not currently assigned to the resource, the assigned policy is set to **No Assignment**. If no policies are applicable to the resource, the assigned policy is set to **No applicable policies**.

- **To multiple resources**

1. Select one or more resources to which you want to assign the policy.

2. Click the **Assign** icon (⚙️) to display the Assign Policy dialog.

3. Select the policy that you want assign. You can select from a list of compliance policies that are applicable to all selected resources. If a policy is not currently assigned to the resource, the assigned policy is set to **No Assignment**. If no policies are applicable to the resource, the assigned policy is set to **No applicable policies**. If resources were not selected before opening the dialog, all policies are listed.

Note: Select **No Assignment** to remove the policy assignment from the selected resource.

4. Select one of the following scopes for the policy assignment.

- **All applicable devices that are...**
- **Only selected applicable devices that are ...**

5. Select one or more policy criteria.

- **Without an assigned policy**
- **Non-compliant (overwrite current assigned policy)**
- **Compliant (overwrite current assigned policy)**

6. Click **Apply**. The policy that is listed in the Assigned Policy column on the Firmware Updates: Repository page changes to the name of the selected firmware-compliance policy.

- **To groups of resources**

1. Click the **Assign** icon (⚙️) to display the Assign Policy dialog.

2. Select the policy that you want assign. You can select from a list of compliance policies that are applicable to all resources in the group. If a policy is not currently assigned to the resource, the assigned policy is set to **No Assignment**. If no policies are applicable to the resource, the assigned policy is set to **No applicable policies**.

Note: Select **No Assignment** to remove the policy assignment from the resources in the group.

3. Select one or more groups of resources to which you want to assign the policy.

4. Select one of the following scopes for the policy assignment.

- **All applicable devices that are...**

- **Only selected applicable devices that are ...**
5. Select one or more policy criteria.
 - **Without an assigned policy**
 - **Non-compliant (overwrite current assigned policy)**
 - **Compliant (overwrite current assigned policy)**
 6. Click **Apply**. The policy that is listed in the Assigned Policy column on the Firmware Updates: Repository page changes to the name of the selected firmware-compliance policy.

After you finish

You can perform the following actions from the Policy Management card.

- View policy details by clicking on the row in the table.
- Modify a selected policy by clicking the **Edit** icon (✎).

Note: You cannot modify a policy that is assigned to one or more resources. You must first unassign the policy.

- Copy and modify a selected policy by clicking the **Copy** icon (📄).
- Delete a selected *user-defined* policy by clicking the **Delete** icon (🗑).

Note: You cannot delete a policy that is assigned to one or more resources. You must first unassign the policy.

From the Apply and Activate card, you can unassign a policy for a selected resource by clicking the **Assign** icon (📌), selecting **No Assignment** policy, and then selecting whether to apply the change to all resources with a policy assignment or to only the selected resources.

Applying and activating updates to resource managers

XClarity Orchestrator does not automatically apply updates. To update software, you must manually apply and activate the update on selected Lenovo XClarity Administrator resource managers that are not compliant with the assigned update-compliance policy.

Before you begin

Before you attempt to apply and activate updates on any resources, ensure that you read the update considerations (see [Update deployment considerations](#)).

Ensure that a update-compliance policy is assigned to the target resource (see [Creating and assigning update-compliance policies](#)).

You cannot apply an update of the same or earlier software level as the one that is currently installed.

About this task

You can apply firmware updates to XClarity Administrator resource managers that have an assigned update-compliance policy and are not compliant with that policy. You can update software in the following ways.

- To specific non-compliant managers
- To all non-compliant managers in specific groups
- To all non-compliant managers that are assigned a specific update-compliance policy
- To all non-compliant managers in specific groups that are assigned a specific update-compliance policy
- To all non-compliant managers that are assigned to any policy and are not compliant with that policy

XClarity Orchestrator does not directly update resources. Instead, it sends a request to the applicable resource manager to perform the update, and then tracks the progress of the request. XClarity Orchestrator identifies the dependencies that are required to perform the update, ensures that the target resources are updated in the correct order, transfers the applicable update packages to the resource manager, and creates a request to start a job on the resource manager to perform the update.

During the update process, the target resource might be restarted automatically several times until the entire update process is complete. Ensure that you quiesce all applications on the target resource before you proceed.

If an error occurs while updating any of the components in a target resource, the update process does not update that component; however, the update process continues to update the other components in the resource and continues to update all other target resources in the current update job.

Prerequisite updates are not applied automatically.

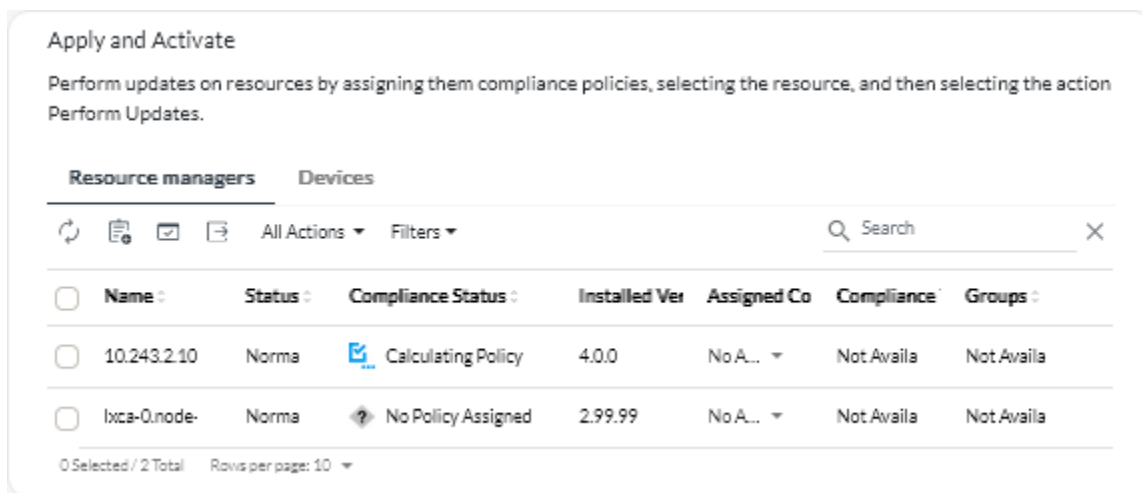
Tip:

- The table lists only resource managers that can be updated.
- The **Build Number** and **Compliance Target Build Number** columns are hidden from view by default. You can show these columns by clicking **All Actions** → **Toggle Columns**.

Procedure

To apply updates to XClarity Orchestrator resource managers, complete one of the following procedures.

- **To specific non-compliant resource managers**
 1. From the XClarity Orchestrator menu bar, click **Provisioning** (🔑) → **Updates** and then click **Apply and Activate** to display the Apply and Activate card.



2. Click the **Resource Managers** tab.
3. Select one or more resource managers to which you want to apply updates.
4. Click the **Apply Update** icon (📄) to display the Update Summary dialog.
5. Click **Perform Updates** to apply the updates. A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

- **To all non-compliant resource managers in specific groups or that are assigned a specific update-compliance policy**
 1. From the XClarity Orchestrator menu bar, click **Provisioning** (🔧) → **Updates** and then click **Apply and Activate** to display the Apply and Activate card.
 2. Click the **Resource Managers** tab.
 3. Click the **Apply Update** icon (📄) to display the Update Summary dialog.
 4. Select the groups and update-compliance policy.
 - If you do not select a policy or group, all managers that have an assigned policy and that are not compliant with that policy are updated.
 - If you select a policy but not a group, all managers that are assigned that policy and that are not compliant with that policy are updated.
 - If you select one or more groups and not a policy, all managers in the group that are not compliant with the assigned policy are updated.
 - If you select a policy and one or more groups, all managers in the group that are assigned that policy and that are not compliant with that policy are updated.
 5. Click **Perform Updates** to apply the updates. A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

Applying and activating updates to managed servers

Lenovo XClarity Orchestrator does not automatically apply updates. To update firmware, you must manually apply and activate the update on selected devices that are not compliant with the assigned update-compliance policy.

Before you begin

Before you attempt to apply and activate updates on any device, ensure that you read the update considerations (see [Update deployment considerations](#)).

Ensure that a update-compliance policy is assigned to the target device (see [Creating and assigning update-compliance policies](#)).

You can apply firmware updates to only managed servers.

When updating firmware on many devices at one time, use XClarity Orchestrator v1.3.1 or later and Lenovo XClarity Administrator v3.2.1 or later for better performance.

About this task

You can apply firmware updates to devices that have an assigned update-compliance policy and are not compliant with that policy. You can update firmware in the following ways.

- To specific non-compliant devices
- To all non-compliant devices in specific groups
- To all non-compliant devices that are assigned a specific update-compliance policy
- To all non-compliant devices in specific groups that are assigned a specific update-compliance policy
- To all non-compliant devices that are assigned to any policy and are not compliant with that policy

A server is flagged as Not Compliant when the installed firmware version of one or more components is *earlier or later* than the target firmware version in the update-compliance policy. If the installed firmware version is *later* than the target firmware version, you must select the **Force update** option when applying the

update to downgrade the firmware on the components. If the **Force update** option is not selected, only target firmware versions that are later than the installed versions are applied.

Note: Only certain device options, adapters, and drives support downgrading. See your hardware documentation to determine if downgrading is supported.

XClarity Orchestrator does not directly update resources. Instead, it sends a request to the applicable resource manager to perform the update, and then tracks the progress of the request. XClarity Orchestrator identifies the dependencies that are required to perform the update, ensures that the target resources are updated in the correct order, transfers the applicable update packages to the resource manager, and creates a request to start a job on the resource manager to perform the update.

During the update process, the target device might be restarted automatically several times until the entire update process is complete. Ensure that you quiesce all applications on the target device before you proceed.

If an error occurs while updating any of the components in a target device, the update process does not update that component; however, the update process continues to update the other components in the device and continues to update all other target device in the current update job.

Prerequisite updates are not applied automatically.

Tips:

- The table lists only devices that can be updated.
- The **Build Number**, **Compliance Target Build Number**, and **Product Name** columns are hidden from view by default. You can show these columns by clicking **All Actions** → **Toggle Columns**.
- For ThinkSystem SR635, SR645, SR655, and SR665 servers, to apply both in-band and out-of-band firmware, first apply updates to the baseboard management controllers, and then apply firmware updates to the remaining options.

Procedure

To apply updates to managed devices, complete one of the following procedures.

• To specific non-compliant devices

1. From the XClarity Orchestrator menu bar, click **Provisioning** (🔑) → **Updates** and then click **Apply and Activate** to display the Apply and Activate card.
2. Click the **Devices** tab.
3. Select one or more devices to which you want to apply updates.
4. Click the **Apply Update** icon (📄) to display the Update Summary dialog.
5. Select when to activate the updates.
 - **Prioritized activation.** Firmware updates on the baseboard management controller are activated immediately; all other firmware updates are activated the next time the device is restarted. Additional restarts are then performed until the update operation completes. An event is raised when the status changes to Pending Firmware Maintenance Mode to notify you when the server needs to be restarted.
 - **Delayed activation.** Some but not all update operations are performed. Target devices must be restarted manually to continue the update process. Additional restarts are then performed until the update operation completes. An event is raised when the status changes to Pending Firmware Maintenance Mode to notify you when the server needs to be restarted.

If the target device restarts for any reason, the delayed update process completes.

Important:

- Use **Restart Normally** to restart the server to continue the update process. *Do not* use **Restart Immediately**.
- Do not choose Delayed Activation for more than 50 devices at one time. XClarity Orchestrator actively monitors devices with delayed activation so that the delayed activation is serviced when a device is restarted. If you want to apply updates with delayed activation for more than 50 devices, break the update selection into batches of 50 devices at one time.
- **Immediate activation.** During the update process, the target device might be restarted automatically several times until the entire update process is complete. Ensure that you quiesce all applications on the target device before you proceed.

Notes:

- For ThinkEdge Client devices, only Immediate activation is supported.
 - When enabled, the Wake-on-LAN boot option can interfere with Lenovo XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.
6. **Optional:** Select **Force** update to update firmware on the selected components even if the firmware level is up to date or to apply a firmware update that is earlier than the one currently installed on the selected components.
 7. Click **Perform Updates** to apply the updates. A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)
- **To all non-compliant devices in specific groups that are assigned a specific update-compliance policy**
 1. From the XClarity Orchestrator menu bar, click **Provisioning** (🔧) → **Updates** and then click **Apply and Activate** to display the Apply and Activate card.
 2. Click the **Devices** tab.
 3. Select one or more device groups to which you want to apply updates.
 4. Click the **Apply Update** icon (📧) to display the Update Summary dialog.
 5. Select the groups and update-compliance policy.
 - If you do not select a policy or group, all devices that have an assigned policy and that are not compliant with that policy are updated.
 - If you select a policy but not a group, all devices that are assigned that policy and that are not compliant with that policy are updated.
 - If you select one or more groups and not a policy, all devices in the group that are not compliant with the assigned policy are updated.
 - If you select a policy and one or more groups, all devices in the group that are assigned that policy and that are not compliant with that policy are updated.
 6. Select when to activate the updates.
 - **Prioritized activation.** Firmware updates on the baseboard management controller are activated immediately; all other firmware updates are activated the next time the device is restarted. Additional restarts are then performed until the update operation completes. An event is raised when the status changes to Pending Firmware Maintenance Mode to notify you when the server needs to be restarted.
 - **Delayed activation.** Some but not all update operations are performed. Target devices must be restarted manually to continue the update process. Additional restarts are then performed until the update operation completes. An event is raised when the status changes to Pending Firmware Maintenance Mode to notify you when the server needs to be restarted.

If the target device restarts for any reason, the delayed update process completes.

Important:

- Use **Restart Normally** to restart the server to continue the update process. *Do not* use **Restart Immediately**.
- Do not choose Delayed Activation for more than 50 devices at one time. XClarity Orchestrator actively monitors devices with delayed activation so that the delayed activation is serviced when a device is restarted. If you want to apply updates with delayed activation for more than 50 devices, break the update selection into batches of 50 devices at one time.
- **Immediate activation**. During the update process, the target device might be restarted automatically several times until the entire update process is complete. Ensure that you quiesce all applications on the target device before you proceed.

Notes:

- For ThinkEdge Client devices, only Immediate activation is supported.
 - When enabled, the Wake-on-LAN boot option can interfere with Lenovo XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.
7. **Optional:** Select **Force** update to update firmware on the selected components even if the firmware level is up to date or to apply a firmware update that is earlier than the one currently installed on the selected components.
 8. Click **Perform Updates** to apply the updates. A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📧) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

After you finish

You can perform the following actions from the Patterns card.

- Forward reports about firmware compliance on a reoccurring basis to one or more email addresses by clicking the **Create Report Forwarder** icon (⊕). The report is sent using the data filters that are currently applied to the table. All shown and hidden table columns are included in the report. For more information, see [Forwarding reports](#).
- Add a firmware compliance report to a specific report forwarder using the data filters that are currently applied to the table by clicking the **Add to Report Forwarder** icon (↗). If the report forwarder already includes a firmware compliance report, the report is updated to use the current data filters.

Chapter 6. Analyzing trends and predicting problems

Lenovo XClarity Orchestrator generates analytics alerts based on known hardware and firmware issues, monitors trends to detect anomalies that occur in your managed resources, and builds heuristics that can calculate the likelihood of impending problems or failures. The trends are visualized as queries, graphs, and charts that show the compliance status, problem history, and breakdown of resources that have the most problems. You can then analyze these trends to get insights into the cause of problems and resolve them quickly.

Important:

- The analytics functions are supported for ThinkAgile, ThinkSystem, and ThinkEdge servers running XCC firmware v1.4 or later.
- To use the analytics functions, a Lenovo XClarity Orchestrator Analytics license is needed for each device that supports the analytics functions. A license *is not* tied to specific devices. For more information, see [Applying XClarity Orchestrator licenses](#) in the XClarity Orchestrator online documentation.

Creating custom analytics reports

Analytics reports run continuously in the background to give insight into how well your data center is operating in real time.

About this task

Lenovo XClarity Orchestrator provides several predefined analytics reports that are based on event, inventory, or metrics data that is collected from the managed resources. These are then displayed as statistics (in tabular form) or graphically as bar charts or pie charts. You can see examples of these reports on the **Analytics (🔍) → Predefined Analytics** pages.

You can also create your own custom reports to represent data that interests you the most.

Procedure

To create a custom analytics reports, complete the following steps.

Step 1. Create custom alerts.

XClarity Orchestrator generates analytics alerts based on known hardware and firmware issues. You can also create custom alerts to use in your custom reports.

Step 2. Create custom reports (queries).

You can add custom graphical reports to XClarity Orchestrator by defining queries based on data that interests you the most.

Creating rules for custom analytics alerts

Lenovo XClarity Orchestrator raises alerts based on known hardware and firmware issues. You can define custom *alert rules* to raise analytics alerts when a specific event occurs or when a specific metric is breached. Then, you can use those alerts to generate custom analytics reports (queries).

About this task

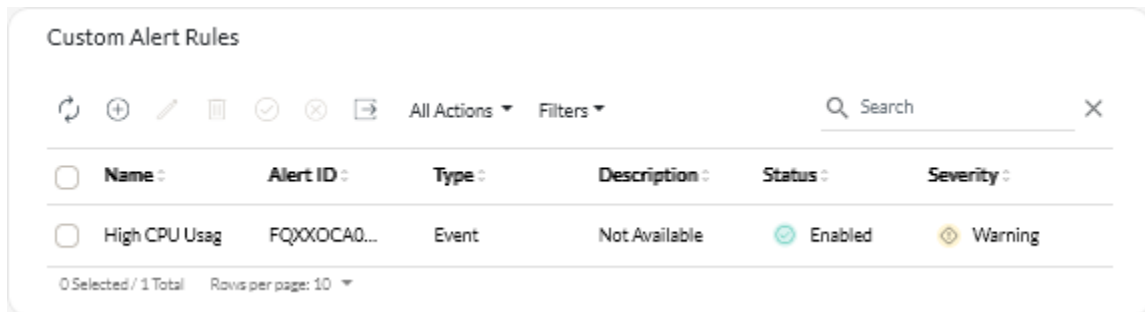
Events are raised for all alerts, including custom analytics alerts. The same event code is used for both the active alert and the event using the format FQXX0CAxxxxc, where xxxx is the unique identifier and c is the severity (see).

Custom alerts are included in the list of active alerts for health status. All active alerts, including custom alerts, and are displayed in a single, unified view (see [Monitoring active alerts](#)).

Procedure

To create a custom alert rule, complete the following steps.

Step 1. From the XClarity Orchestrator menu bar, click **Analytics** (📊) → **Custom Alerts**, to display the Custom Alert Rules card.



Step 2. Click the **Create** icon (⊕) to display the Create Custom Alert Rule dialog.

Step 3. Specify a unique name and an optional description for the custom alert.

Step 4. Select the source type for this rule.

- **Event.** Raises an alert when a specific event occurs, based on the rule criteria.
- **Metric.** Raises an alert when a specific metric is breached, based on the rule criteria.

Step 5. Click **Rule Trigger Details**, and specify the criteria for this rule. The criteria varies depending on the source type.

- **Event-based alerts rules**

- Specify the target type for this alert.
 - **Device.** Raises an alert when the event occurs on any device. The device name is included in this alert.
 - **Device group.** Raises an alert when the event occurs on a device in any device group. The group name is included in the alert.
- Specify the ID of the event that triggers an alert. For a list of event IDs, see [Event and alert messages](#) in the XClarity Orchestrator online documentation.
- Specify the number of times (count) that the event must occur in the specified interval before an alert is raised.
- Select the period of time (interval), in minutes, in which the event occurs before an alert is raised.

- **Metric-based alerts rules**

- Select the criteria mode.
 - **average.** Raises an alert when the average value of the metric breaches the threshold (based on the comparator) during a specific interval.

For example, you can create a rule to raise an alert when the average CPU Temperature (**metric**) during a 24-hour period (**interval**) is greater than (**operator**) 40 degrees C (**threshold**).

- **count.** Raises an alert when the metric breaches the threshold (based on the comparator) a certain number of times during a specific interval.

For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**) for 5 times (**count**) in a 24-hour period (**interval**).

- **simple.** Raises an alert when the metric breaches the threshold (based on the comparator).

For example, you can create a rule to raise an alert when the CPU Temperature (**metric**) is greater than (**operator**) 40 degrees C (**threshold**).

- Select the measurement (metric) for this alert from a list of measurements that are supported for the managed resources.
- If the criteria mode is “count,” specify the number of times that the value is breached in the specified interval before an alert is raised.
- Select the comparison function.
 - **>=.** Greater than or equal to
 - **<=.** Less than or equal to
 - **>.** Greater than
 - **<.** Less than
 - **=.** Equal to
 - **!=.** Not equal to
- Specify the threshold value to compare to the metric value.
- If the criteria mode is “average” or “count,” select the period of time (interval), in minutes, in which the metric is evaluated.


Step 6. Click **Alert and Event Details**, and specify the information to display for the alert and event.

1. Specify the message, description, and user action to display for the associated alert and event. You can include variables by enclosing the field (variable) name in double brackets, for example, `[[DeviceName]]`. A list of available fields (based on the selected measurement) is displayed in the table to the right of the input fields.
2. Select the severity for this alert rule.
 - **Warning.** User can decide if action is needed.
 - **Critical.** Action is needed immediately, and the scope is broad (perhaps an imminent outage to a critical resource will result).
3. Specify a unique 4-digit number to use as the event code for this alert. You can specify a number from 0001 – 9999 that is not already used.





Step 7. Optionally change the status to **Enabled** to enable XClarity Orchestrator to raise an analytics alert when the criteria for the custom alert is met.

Step 8. Click **Create**.

After you finish

You can view the list of analytics alerts that were raised based on the enabled custom alert rules by clicking **Monitoring**  → **Alerts**.

You can perform the following actions from the Custom Alert Rules card.

- Modify the properties of a selected custom alert rule by clicking the **Edit** icon .
- Delete a selected custom alert rule by clicking the **Delete** icon .
- Enabled or disable one or more selected custom alert rule, click the **Enable** icon  or **Disable** icon .

Creating custom reports (queries)

You can add custom tabular and graphical reports to Lenovo XClarity Orchestrator by defining queries based on collected data, such as alerts, events, inventory, device metrics, or your custom metrics (aggregations).

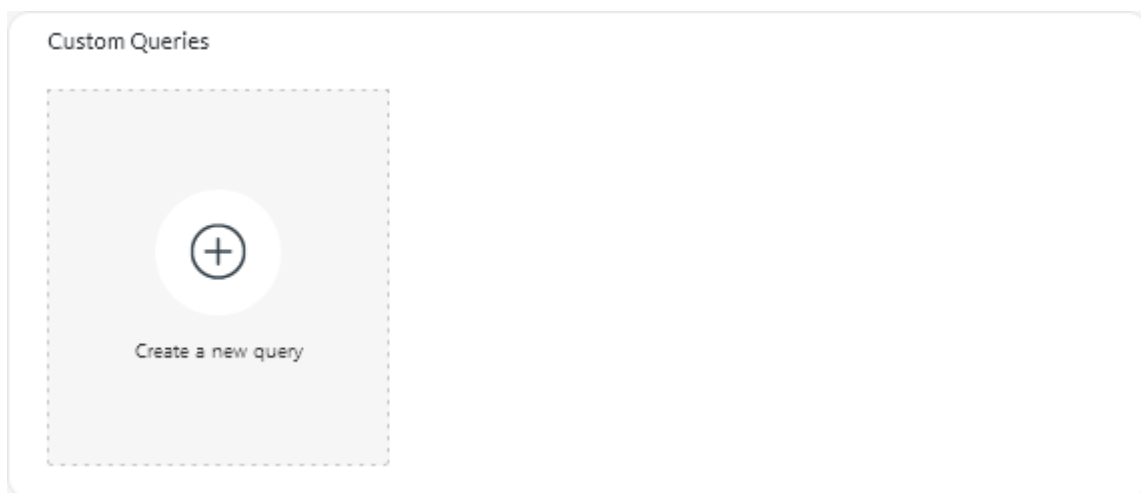
Before you begin

Important: Creating custom analytics reports in XClarity Orchestrator requires a basic understanding databases and database queries.

About this task

To create a custom report, complete the following steps.

Step 1. From the XClarity Orchestrator menu bar, click **Analytics** (🔍) → **Customized Queries**, to display the Custom Queries card.



Step 2. Click the **Create** icon (⊕) to display the Create Custom Query dialog.

Step 3. Specify a unique name for the custom query.

Step 4. Select the type of data that you want to use as the source for this query.

You can choose one of the following data-source types.

- **Alerts.** Hardware or management conditions that require investigation and user action
- **Events.** Resource and audit events
- **Events-Resource.** Hardware or orchestrator condition that occurred on a managed device, resource manager, or XClarity Orchestrator
- **Events-Audit.** User activities that were performed from a resource manager or XClarity Orchestrator
- **Inventories-Manager.** Inventory data for resource managers
- **Inventories-Device.** Inventory data for managed devices of all types
- **Inventories-Device-Server.** Inventory data for managed servers
- **Inventories-Device-Switch.** Inventory data for managed switches
- **Inventories-Device-Storage.** Inventory data for managed storage devices
- **Inventories-Device-Chassis.** Inventory data for managed chassis
- **CPU Temp.** Metrics data for the temperature, in Celsius, of each processor in a managed device. The metric is captured every minute.
- **CPU Utilization Stats.** Metrics data for the processor usage, as a percentage, for a managed device. The metric is captured every minute.
- **Inlet Air Temp.** Metrics data for the inlet-air temperature, in Celsius, of a managed device. The temperature is captured every minute.

- **MemoryUtilizationStats.** Metrics data for the memory used, as a percentage, by a managed device. The metric is captured every minute.
- **PowerMetrics.** Metrics data for power consumption, in Watts, by all processors, memory modules or the entire system for a managed device. These metrics are captured every 30 seconds.
- **PowerSupplyStats.** Metrics data for power supply input and output, in Watts, for a managed device. These metrics are captured every 30 seconds.

The types of data sources (alerts, events, inventories, and metrics) that are listed vary based on the data is available in XClarity Orchestrator. For example, if alerts data is available, the **Alerts** type is listed. If events data is available, all **Events-*** types are listed.

The selected data source affects the data that is available on the **Query Conditions** tab. If you select a generic type, such as **Inventories-Devices**, only attributes that are common to all devices are listed. If you select **Inventories-Device-Server**, attributes that are common to all servers are listed.

Step 5. Click **Query Conditions** to define the query conditions for the report.

1. Narrow down the data that you want to use for this query.
 - a. Selecting one or more fields from the **Filtered Fields** drop-down list. The fields that are listed as based on the data-source type that you selected in [step 4](#).
 - b. If you selected multiple filter fields, choose the operator to use to construct the query. This can be one of the following values.
 - **AND.** All values must match.
 - **OR.** One or more value must match.
 - **AND (Negated).** All values must be not match.
 - **OR (Negated).** One or more values must not match.
 - c. For each filtered field that you selected, select the comparison operator from the **Comparison** drop-down list and the value of field. The comparison operators that are available differ based on the data type for the attribute.
 - **>=.** Matches values that are *greater than or equal* to a specified value
 - **<=.** Matches values that are *less than or equal* to a specified value
 - **>.** Matches values that are *greater than* a specified value
 - **<.** Matches values that are *less than* a specified value
 - **=.** Matches values that are *equal to* a specified value
 - **!=.** Matches all values that are *not equal to* a specified value
 - **Contains.** (Inventory and event queries only) Matches any partial values specified in an array
 - **In.** (Inventory and event queries only) Matches any values specified in an array
 - **NotIn.** (Inventory and event queries only) Matches none of the values specified in an array

Tip: To find the current values for any field, create a new query with the same data-source type, select the field name from the **Grouped Fields** drop-down list, specify 0 for the **Limit**, and click **Save**. The **Chart Options** tab is display with a list of all current values.

2. Optionally choose an aggregation function in the **Results Aggregation** section to create a new field based on the filtered data, and specify a name (alias) for the new field. For some aggregation functions like average and maximum, you must also specify the field on which you want to apply the function.

For event and inventory queries, you can choose one of the following functions.

- **Average.** Statistical mean of all values
- **Sum.** Sum of all values
- **Count.** Number of values

- **Maximum.** Highest value
- **Minimum.** Lowest value
- **First.** Value with the oldest timestamp
- **Last.** Value with the newest timestamp

For metrics queries, you can choose one of the following functions.

- **Count.** Number of non-null values
- **Distinct.** List of unique values
- **Integral.** Average field value
- **Mean.** Arithmetic mean (average) of values
- **Median.** Middle value
- **Mode.** Most frequent value
- **Spread.** Difference between the minimum and maximum values
- **Stddev.** Standard deviation
- **Sum.** Sum of all values

3. Optionally choose the fields that you want to use to group the query results from the **Grouped Fields** drop-down list. When you choose a grouped field, XClarity Orchestrator unwinds (deconstructs) the data so that there is a data point for each value of selected fields.
4. Optionally choose how to sort the query results by selecting a field from the **Sort by Field** drop-down list and the sort order from the **Sort Order** drop-down list. For metrics queries, you can sort only by time.
5. Optionally specify the number of data points to return in the query results in the **Limit** field. The default limit is 10. If you specify 0 or leave it empty, all data points are returned.

You can also optionally specify the number of data points that you want to skip in the query results in the **Offset** field.

6. (Metrics queries only) If you choose grouped fields, optionally specify the number of data sets to return in the query results in the **Series Limit** field. The default limit is empty (0). If you specify 0 or leave it empty, all data sets are returned.

You can also optionally specify the number of data sets that you want to skip in the query results in the **Series Offset** field.

7. Click **Save** to save the query and generate the report.

Step 6. Click **Chart Options** to choose the look and feel for the report. The following charts types are available.

- **Table.** Displays data in tabular form.
- **Bar.** Displays data as a graphical bar chart. Choose the fields that you want to use for the x and y axis.
- **Pie.** Display data as a graphical pie chart. Choose the fields that you want to use for the x and y axis. You can choose to use a pie chart only when data is not grouped.


Step 7. Click **Create** to add a new card that contains a report with current query results.

After you finish

You can perform the following actions from the Customized Queries card.

- Enlarge a custom report by clicking the **Enlarge** icon () on the custom report card. For tabular reports, the report icon on the Customized Queries card shows only the first four columns of the table. You can enlarge the report to see all columns in the table.


The **See Details** link in a table column indicates that column contains multiple data fields. Click on the **See Details** link to display a popup table that lists the additional data.

- Modify the properties a custom report by clicking the **Edit** icon () on the card.

- Delete a custom report by clicking the **Delete** icon () on the card.

Analyzing device boot times

The Analytics panel contains report cards that summarize the boot times for managed devices. The *boot time* is the amount of time, in seconds, that it took for the system boot to complete, prior to handing over to the operating system.

To display the boot-time reports, click **Analytics** () → **Predefined Analytics**, and then click **Boot Times** to display the related analytics cards.

Note: Boot statistics are available only for ThinkSystem and ThinkAgile devices running XCC firmware v1.40 or later.

Boot times


This report card includes a bar graph that shows the amount of time that it took boots to complete, for devices with the longest of the latest boot times.

Analyzing connectivity issues

The Analytics panel contains report cards that show statistics about connectivity issues.


Lost connectivity is reported using the following event.

- **FQXHMDM0163J**. The connection between the resource manager and the baseboard management controller in the device is offline.

To display the lost-connectivity reports, click **Analytics** () → **Predefined Analytics**, and then click **Connectivity Issues** to display the related analytics cards

Connectivity issues by time

This report card includes a bar graph that shows the number of connectivity issues that occurred during the current day or month for each resource.

You can choose to display data for a specific range of time by selecting the **Settings** icon () in the upper-right corner of the card.

Top 10 devices by number of connectivity issues

This report card includes a bar graph that shows the top 10 devices that are reporting the most connectivity issues overall. You can click an item in the legend to get more information about a specific resource.

Analyzing security fixes

The Analytics panel contains report cards that shows analytics about security fixes for known common vulnerabilities and exposures (CVEs).

To display the CVE reports, click **Analytics** () → **Predefined Analytics**, and then click **Security Fixes** to display the related analytics cards.

Security Fixes

This report card includes the following statistics and graphs.

- A circular graph that shows the number of managed devices that have common vulnerabilities and exposures (CVEs) for which a security fix is available, by the highest CVE severity

- **Critical.** Number of devices that have at least one critical CVE
- **Non-critical.** Number of devices that have at least one high, medium, or low CVE but no critical CVEs
- **Protected.** Number of devices that have no known CVEs and are protected
- A circular graph that shows the number of unique CVEs for which security fixes are available, by severity (critical, high, medium, or low)

You can hover over each colored bar in the circular graphs to get more information about the state. You can also click the number next to each state to view a list of all devices that fit the criteria.

Devices

The Devices card lists the total number of CVEs for which a security fix is available and the highest severity of CVEs for each device. You can expand the device to view a list of components in that device that have security fixes and the number of security fixes that are available from firmware updates that are downloaded in the updates repository.

You can click the number of security fixes to open a dialog with a filtered list of applicable CVEs for that component. From that dialog, you can click the CVE link to get detailed information about that CVE on the web.

You can show or hide the Devices card by clicking the **Show/Hide Devices** toggle. The toggle changes to **Show Devices** automatically when you click a number in the graphs.

Analyzing drive health

The Analytics panel contains report cards that shows analytics about the health and predictive failure of hard disk drives and solid-state drives in managed ThinkAgile and ThinkSystem servers.

To display the firmware reports, click **Analytics** (🔍) → **Predefined Analytics**, and then click **Drive Predictive Analytics** to display the related analytics cards.

Analytics are supported for the following drives model types.

Hard drives

- ST2000NX0253
- ST8000NM0055
- ST10000NM0086
- ST12000NM0008

Solid state drives

- Intel SSDSC2BB800G4

Important: Drives with older firmware are not eligible for analysis. Update the drives to the latest firmware level to enable predictive analysis.

Drives At Risk

This report card contains a pie graph that shows the number of drives in each health state (normal or risky).

Drives At Risk History

This report card contains a bar graph that shows the number of failed drives, during the last week or last year. Hover the cursor over each bar in the graph to display a filtered list of failed drives, by device, on that day.

Drives with Predictive Failure

The report card contains a table that lists the devices with failed drives. You can click on a device to list the details of each at-risk drive in that device.

Analyzing firmware

The Analytics panel contains report cards that shows analytics about firmware.

To display the firmware reports, click **Analytics** (🔍) → **Predefined Analytics**, and then click **Firmware Analytics** to display the related analytics cards.

Firmware Analytics

This report card includes a bar graph that shows the number of firmware that is installed on managed devices based on the firmware category and age.

Firmware is grouped into the following categories.

- Management controller
- System tools
- UEFI

Firmware ages are grouped into the following intervals

- **Under 6 months**
- **6 – 12 months**
- **1 – 2 years**
- **Over 2 years**

You can filter the devices that are included in the report by using the **Filters** input fields. You can also save filtered queries that you want to use regularly.

You can show or hide the Devices card by clicking the **Show/Hide Devices** toggle. The Devices card lists the firmware types and ages for all devices that are included in the graph.

Analyzing lost events

The Analytics panel contains report cards that show statistics about lost events. Lost events are determined by a gap in sequence numbers

Events have a sequence number that indicates the order in which each event occurred on a specific device. The event sequence numbers should be consecutive for a specific device. If there are sequence numbers that are not consecutive, the gap might indicate that one or more events were lost.

To display the lost-events reports, click **Analytics** (🔍) → **Predefined Analytics**, and then click **Lost Events** to display the related analytics cards.

Lost events by time

This report card includes a bar graph that shows the number of events that were lost during the current day or month for each resource.

You can choose to display data for a specific range of time by selecting the **Settings** icon (⚙️) in the upper-right corner of the card.

Top 10 devices by number of lost events

This report card includes a bar graph that shows the top 10 devices that are reporting the most lost events overall.

Analyzing and predicting resource-manager capacity

The Analytics panel contains report cards that predict when resource managers will exceed the maximum number of managed devices. For Lenovo XClarity Administrator resource managers, up to 1,000 managed devices are supported.

To display the resource-manager capacity reports, click **Advanced Analytics** (🔍) → **Predefined Analytics**, and then click **Manager Capacity Prediction** to display the related analytics cards.

Manager Capacity

This report lists the device capacity for each resource manager, including the number of managed devices and capacity status, which indicates whether the capacity is overloaded. The following capacity states are used.

- (✅) **Normal**. The number of managed devices less than the maximum number of supported devices.
- (⚠️) **Warning**. The number of managed devices close to the maximum number of supported devices.
- (❌) **Critical**. The number of managed devices greater than the maximum number of supported devices.

Manage Capacity Trend

This report card includes a line graph that shows the number of devices that were managed, over time, for a specific resource manager and the forecasted trend when the number of managed devices will be reached the maximum supported capacity for that resource manager.

Click a row in the Manager Capacity table to display capacity trends for that resource manager.

You can change the time period that is displayed by clicking the drop-down menu. You can choose to display data by year, quarter, month, or day. You can also change the number of periods that are shown in the graph using the zoom box under the graph.

Analyzing and predicting utilization trends

The Analytics panel contains report cards that show historical and forecasted processor, storage, and memory usage in devices and virtual resources (such as hosts, clusters, and virtual machines).

Important: This function requires a connection to VMware vRealize Operations Manager resource manager (see [Connecting resource managers](#)).

To display the utilization trend reports, click **Advanced Analytics** (🔍) → **Predefined Analytics**, and then click **Workload Utilization Trend** to display the related analytics cards.

Resource Selection

This report lists the devices and virtual resources that are managed by the orchestrator server.

Click a row in the table to display the utilization trends for that resource.

CPU Utilization Trend

This report card includes a line graph that shows the processor usage, over time, for a specific virtual resource, and the forecasted trend when the processor usage will be reached the maximum supported capacity for that virtual resource.

You can change the time period that is displayed for historical and forecasted data from the **History** and **Projection** drop-down menus, respectively. You can also change the number of periods that are shown in the graph using the zoom box under the graph.

Memory Utilization Trend

This report card includes a line graph that shows the memory usage, over time, for a specific virtual resource, and the forecasted trend when the memory usage will be reached the maximum supported capacity for that virtual resource.

You can change the time period that is displayed for historical and forecasted data from the **History** and **Projection** drop-down menus, respectively. You can also change the number of periods that are shown in the graph using the zoom box under the graph.

Storage Utilization Trend

This report card includes a line graph that shows the storage usage, over time, for a specific virtual resource, and the forecasted trend when the storage usage will be reached the maximum supported capacity for that virtual resource.

You can change the time period that is displayed for historical and forecasted data from the **History** and **Projection** drop-down menus, respectively. You can also change the number of periods that are shown in the graph using the zoom box under the graph.

Analyzing performance and usage metrics

The Analytics panel contains report cards that shows heatmaps based on specific metrics and resources over a specific time period.

To display the performance heatmap, click **Advanced Analytics** (🔍) → **Predefined Analytics**, and then click **Performance Heatmap** to display the related analytics cards.

Performance Heatmap

This report card includes a heatmap that illustrates number of devices that have metric values within a specific number of ranges over a certain time period.

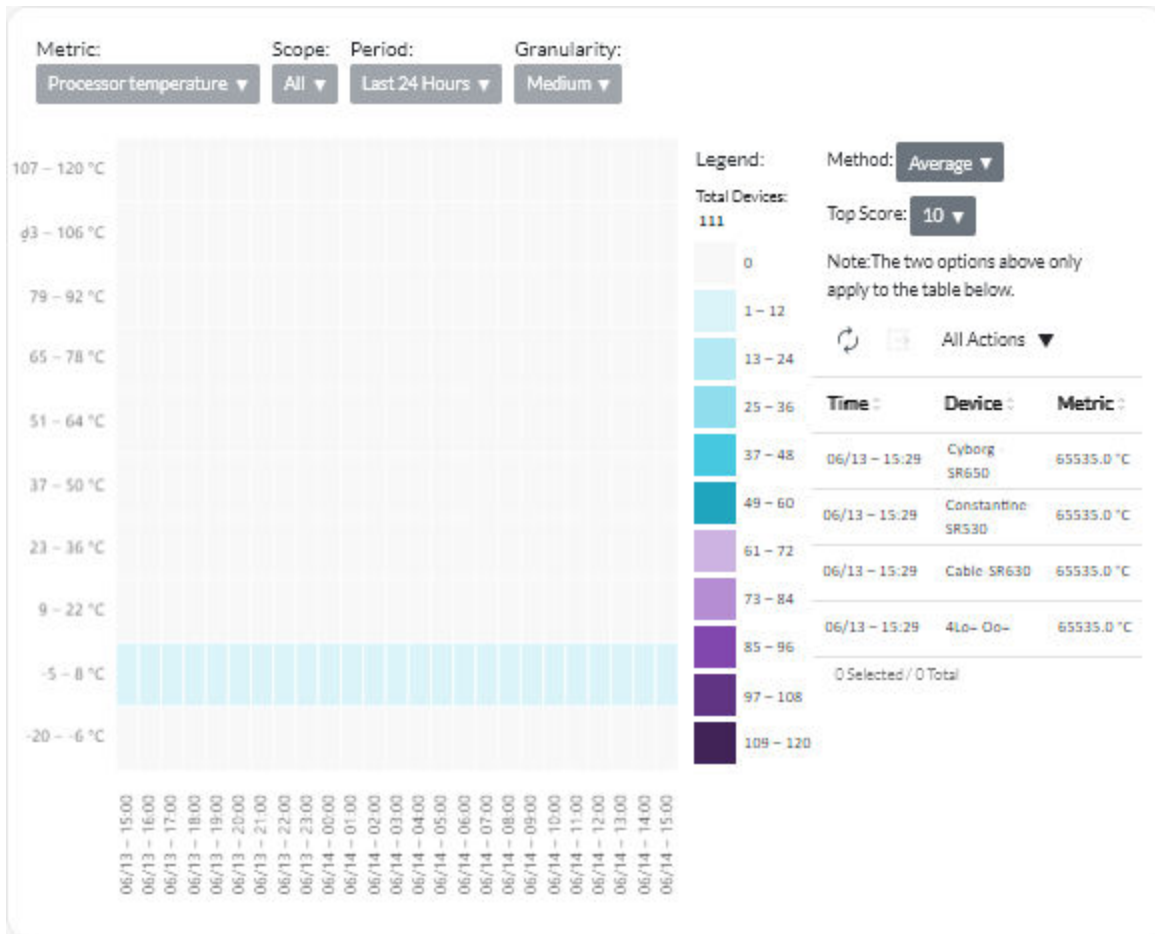
You can click any cell in the heatmap to display a popup list of devices that are represented by that cell, with information the actual metric value for each device and timestamp when the metric was collected.

You can configure the heatmap to show only the information that you are interested in.

- You can choose to display data for one of the following metrics.
 - Processor temperature
 - Processor utilization
 - Memory utilization
- You can choose to aggregate the metrics data based on the average or the peak (highest) value.
- You can filter the heatmap to include only metrics data for devices in a specific device group.

Note: If you scope the user interface to a specific resource manager, only data for devices in the selected groups that are also managed by the resource manager is included in the heatmap.

- You can display data over the last 24 hours, last 14 days, or the last 30 days.
- You can also choose the number value ranges to display on the x-axis of the heatmap. The number of values between the maximum and minimum are divided into equal parts based on the number you choose. You can choose 10, 15 or 20.
- You can also choose to list the top 10, 15, or 20 devices with the highest values and the timestamp when the metric was collected.



Analyzing repeated events

The Analytics panel contains report cards that summarize the repeated events for each device.

Repeated events are generated when the following conditions occur:

- **FQXXOIS0002J.** A critical or warning event with the same ID was generated one or more times for the same device in at least three consecutive 5-minute periods.
- **FQXXOIS0003J.** More than five critical or warning events were generated for the same device each hour for two or more consecutive hours.

To display the repeated-event reports, click **Advanced Analytics** (🔍) → **Predefined Analytics**, and then click **Repeated Events** to display the related analytics cards.

Repeated Events

This report card includes a bar graph that shows the number of repeated events overall for each device.

Repeated Events per Time

This report card includes a bar graph that shows the number of repeated events that were generated on the current day, for each device.

Analyzing unauthorized-access attempts

The Analytics panel contains report cards that summarize unauthorized-access (failed login) attempts.

To display the unauthorized-access reports, click **Analytics** (📊) → **Predefined Analytics**, and then click **Unauthorized Access Attempts** to display the unauthorized-access analytics cards.

Number of Failed Login Attempts per User

This report card includes a graph that shows the number of unauthorized-access attempts overall for each user (by user name). You can display data as a bar graph (📊) or pie graph (🥞) by clicking the appropriate icon in the upper left corner of the card.

You can hover over each bar or piece in the graph to get more information, such as the last occurrence.

Number of Failed Login Attempts per User, in Each Period

This report card includes a bar graph that shows the number of unauthorized-access attempts that occurred on the current day for each user (by user name).

Number of Failed Login Attempts per User IP address

This report card includes a bar graph that shows the total number of all unauthorized-access attempts overall for each user (by IP address). You can display data as a bar graph (📊) or pie graph (🥞) by clicking the appropriate icon in the upper left corner of the card.

You can hover over each bar or piece in the graph to get more information, such as the last occurrence.

Number of Failed Login Attempts per User IP Address, in Each Period

This report card includes a bar graph that shows the number of unauthorized-access attempts that occurred on the current day for each user (by IP address).

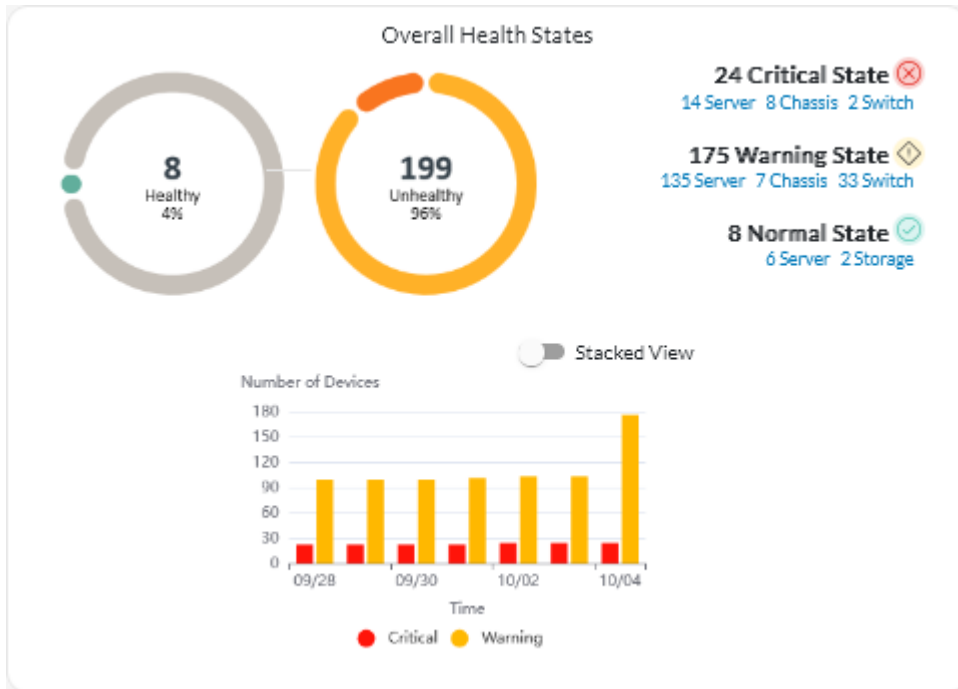
Analyzing device health

The Overall Health States card on the dashboard and the Device Analytics card on each devices page summarize the overall health of managed devices.

Status summary of all devices

From the XClarity Orchestrator menu bar, click **Dashboard** (📊) to display the dashboard cards with an overview and status of all managed devices and other resources (see [Viewing a summary of your environment](#)).

You can change the scope of the summary to only those devices that are managed by a specific resource manager or in a specific resource group by using the **Select manager** drop-down menu.



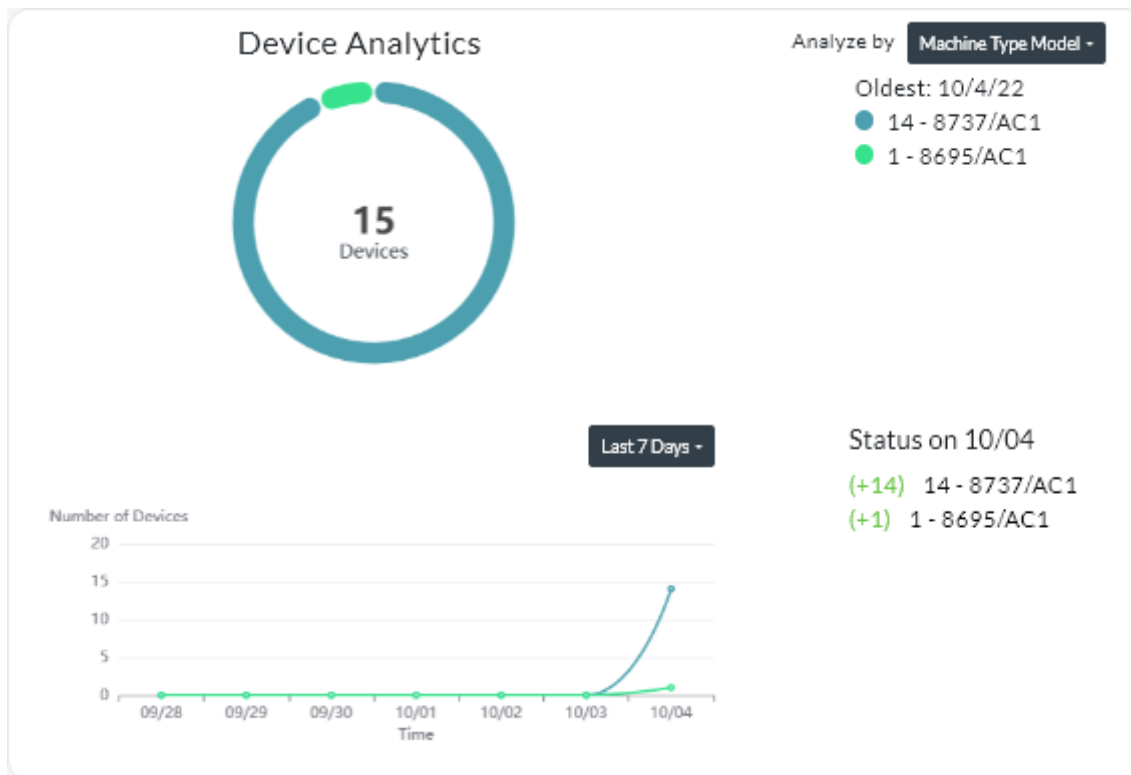
Each colored bar in the circular and bar graphs indicates the number of devices in a specific state. You can hover over each colored bar to get more information about the state. You can also click the number of devices in each state to view a list of all devices that fit the criteria.

Status summary of all devices of a specific type

To view the overall active alert summaries, click **Resources** (🔍) from the XClarity Orchestrator menu bar, and then click the device type to display a card with a tabular view of all devices of that type. For example, if you select **Severs**, a list of all rack, tower, and dense servers and all Flex System and ThinkSystem servers in a chassis is displayed.

You can change the scope of the summary based on device property from the **Analyze by** drop-down list.

- **Machine Type Model.** (default) This report summarizes device health by machine type model (MTM).
- **Machine Type.** This report summarizes device health by machine type.
- **Product Name.** This report summarizes device health by product.



XClarity Orchestrator summarizes device health based on specific criteria. Each summary includes the following information.

- A circular chart that shows the total number of devices that are unhealthy and percentage of devices in each unhealthy state (critical, warning, and unknown).
Each colored bar in the circular graph indicates the number of devices in a specific state. You can hover over each colored bar to get more information about the state.
- A line graph that shows number of devices in each health state per day over the specified number of days.
Each colored bar in the line graph indicates the number of devices in a specific state. You can hover over each colored bar to get more information about the state.
- The number of devices of each type that are unhealthy on a specific day. The current day is shown by default. You can change the day by hovering over each day in the line graph.

Analyzing infrastructure-resource health


You can determine the overall health and sensor trends of infrastructure resources.

Health status of infrastructure resources

From the Lenovo XClarity Orchestrator menu bar, click **Resources** (⚙️) → **Infrastructure** to display the Infrastructure card. You can determine the health status of each resource from the **Status** column.

Sensor Trends

From the XClarity Orchestrator menu bar, click **Resources** (⚙️) → **Infrastructure** to display the Infrastructure card, and then click an infrastructure resource from the table to view a list of sensors for that resource and the latest measurement of each.

Select one or more sensors, and then click the **Graph** icon () to view line graphs that shows the measurements, over time for each selected sensor. By default, sensors with the same unit (such as watts or amps) are plotted on the same graph.

Note: Schneider Electric EcoStruxure IT Expert collects sensor data every 5 minutes, and XClarity Orchestrator synchronizes this data every hour. Currently, XClarity Orchestrator saves only the last 60 minutes of data.

Analyzing active alerts


The Alerts Analytics card summarize the active alerts.

Lenovo XClarity Orchestrator summarizes active alerts based on specific criteria. Each summary includes the following information.

- A circular chart that shows the total number of active alerts and percentage of alerts that are associated with each summary type
- The number of active alerts for each summary type
- Age of the older active alert
- A line graph that shows number of active alerts for each summary type per day over the specified number of days
- The number of alerts that were active for each summary type on a specific day. The current day is shown by default. You can change the day by hovering over each day in the line graph.


Overall active alerts

To view the overall active alert summaries, complete the following steps.

1. From the XClarity Orchestrator menu bar, click **Monitoring** () → **Alerts** to display the Alerts Analytics card.
2. Select the time period from the drop-down list above the line graph. The default is the last seven days.
3. Select the summary type from the **Analyze by** drop-down list.
 - **Severity.** (default) This report summarizes active alerts by severity: critical, warning, and informational.
 - **Source type.** This report summarizes active alerts that were generated by each source type, such as device, management, and analytics.
 - **Resource type.** This report summarizes active alerts for each resource type, such as devices, resource managers and XClarity Orchestrator.
 - **Serviceability.** This report summarizes active alerts that are associated with each serviceability type: **none** (service is not required), **user** (service is performed by the user), **serviceable** (service is performed by Lenovo).

Active alerts for a specific device

To view the active alert for a specific device, complete the following steps.

1. From the XClarity Orchestrator menu bar, click **Resources** () and then click the device type to display a card with a tabular view of all managed devices of that type.
2. Click the row for the device to display the device summary cards for that device.
3. Click **Alerts Log** to display the list of active alerts for the device and the Alerts Analytics card.
4. From the Alerts Analytics card, select the time period from the drop-down list above the line graph. The default is the last seven days.
5. Select the summary type from the **Analyze by** drop-down list.

- **Source type.** This report summarizes active alerts that were generated by each source type, such as device, management, and analytics.
- **Serviceability type.** This report summarizes active alerts that are associated with each serviceability type: none (service is not required), user (service is performed by the user), serviceable (service is performed by Lenovo).
- **Severity.** This report summarizes active alerts for by severity: critical, warning, and informational.

Chapter 7. Working with service and support

Lenovo XClarity Orchestrator provides a set of tools that you can use to 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.

Sending periodic data to Lenovo

You can optionally allow Lenovo XClarity Orchestrator to collect information about your hardware 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

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

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

About this task

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.

- **Daily hardware data.** Only changes to inventory data and drive-analytics data (if data collection is enabled) for each managed device
- **Weekly hardware data.** All inventory data for managed devices, and information about connected resource managers

Attention: This data *is not anonymous*.

- The collected data *includes* UUIDs, WWNs, device IDs, and serial numbers. XClarity Orchestrator modifies the inventory by hashing the UUIDs, WWNs, and device IDs using SHA512.
- The collected data *does not include* networking information (IP addresses, domain names, or hostnames) or user information.

When data is sent to Lenovo, it is transmitted from the XClarity Orchestrator 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 Orchestrator is used for authentication. If an XClarity Orchestrator instance does not have direct access to the Internet, and there is a proxy configured in XClarity Orchestrator, the data is transmitted through that proxy.

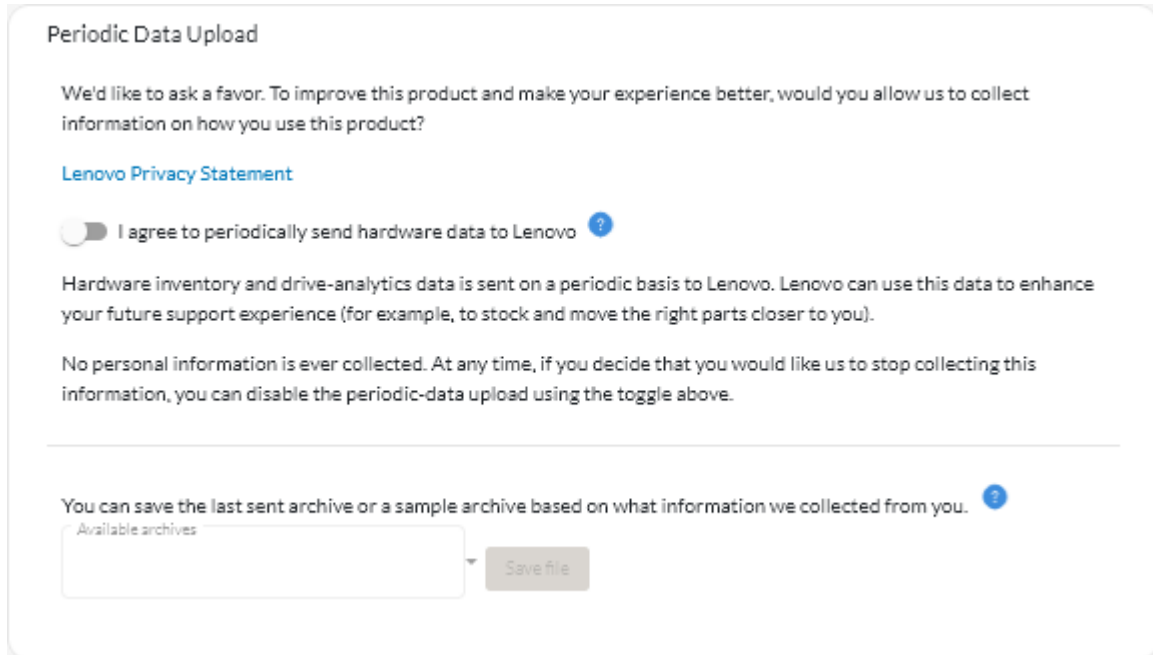
The data is then moved to the Lenovo Customer Care repository, where it is stored for up to 5 years. This repository is a secure location that is also used when debug data is sent to Lenovo to troubleshoot problems. It is used by most Lenovo server, storage, and switch products.

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

Procedure

To allow XClarity Orchestrator to collect and send customer data to Lenovo, complete the following steps.

Step 1. From the XClarity Orchestrator menu bar, click the **Administration** (⚙️) → **Service and Support**, and then click **Periodic Data Upload** in the left navigation to display the Periodic Data Upload card.



Periodic Data Upload

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

[Lenovo Privacy Statement](#)

I agree to periodically send hardware data to Lenovo ?

Hardware inventory and drive-analytics data is sent on a periodic basis to Lenovo. Lenovo can use this data to enhance your future support experience (for example, to stock and move the right parts closer to you).

No personal information is ever collected. At any time, if you decide that you would like us to stop collecting this information, you can disable the periodic-data upload using the toggle above.

You can save the last sent archive or a sample archive based on what information we collected from you. ?

Available archives

Step 2. Optionally agree to send hardware data to Lenovo.

Step 3. Accept the [Lenovo Privacy Statement](#).

After you finish

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

- You can save the last daily and weekly data archives that were sent to Lenovo to the local system by selecting the archive that you want to download and then clicking **Save file**.

Collecting service data for XClarity Orchestrator

You can manually collect service data for Lenovo XClarity Orchestrator and then save the information as an archive in tar.gz format to the local system. You can then send the service files to your preferred service provider to get assistance in resolving issues as they arise.

Learn more:  [How to collect service data](#)

Before you begin

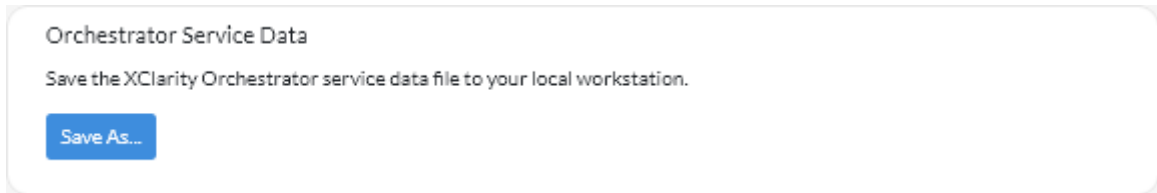
You must be a member of a user group to which the predefined **Supervisor** role is assigned.

Ensure that web browser does not block pop-ups for the XClarity Orchestrator website when downloading service data

Procedure

To collect service data for XClarity Orchestrator, complete the following steps.

Step 1. From the XClarity Orchestrator menu bar, click the **Administration** (⚙️) → **Service and Support**, and then click **Service Data** in the left navigation to display the Management Service Data card.



Step 2. Click **Save As** to collect service data and save the archive to the local system.

A job is created to collect service data. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

After you finish

You can also perform these related actions.

- Manually open a service ticket for a specific device from the Service Tickets card on the device-specific Service page by clicking the **Open service ticket** icon (📄) (see [Manually opening a service ticket in the Lenovo Support Center](#)).
- Attach a service-data archive to a selected active service ticket from the Service Tickets card on the device-specific Service page by clicking the **Attach service file** icon (📎). You can attach a file from XClarity Orchestrator or the local system.

Notes:

- You can attach a single archive file that is no more than 2 GB. The file name can be no longer than 200 characters. For information about creating service-data archives, see (see [Collecting service data for devices](#)).
- The service ticket must be in the Open, In Progress, or On Hold state. You cannot attach an archive to a service ticket that is in the Closed or Other state.
- You cannot attach an archive to a *software* service ticket that was opened for Lenovo XClarity Administrator.
- Save one or more selected service-data archives to the local system from the Management Service Data card by clicking the **Save** icon (↓). If multiple files are selected, the files are compressed into a single .tar.gz file before downloading.
- Delete one or more selected service-data archives that are no longer needed from the Management Service Data card by clicking the **Delete** icon (🗑️), or delete all archives by clicking the **Delete All** icon (⊖).

Collecting service data for devices

When there is a problem with a device that requires the assistance of a service provider such as Lenovo Support to resolve, you can manually collect service data (including service information, inventory, and logs) for that device as an archive file in tar.gz format to help identify the cause of the issue. You can save the archive file to your local system, and then send the archive to your preferred service provider.

Before you begin

You must accept the [Lenovo Privacy Statement](#) before you can collect service data. You can accept the privacy statement by clicking **Administration** (🔧) → **Service and Support**, and clicking **Call Home Configuration** in the left navigation, and then selecting **I Agree with the Lenovo Privacy Statement**.

About this task

When you collect service data through Lenovo XClarity Orchestrator, the orchestrator server sends the request to the resource manager (such as Lenovo XClarity Administrator). The resource manager collects and saves the data as an archive file in its local repository, and then transfers the archive file to XClarity Orchestrator.

For information about saving service data for XClarity Orchestrator to your local system, see [“Collecting service data for XClarity Orchestrator” on page 188](#).

For information about manually opening a service ticket and sending service data to the Lenovo Support Center, see [“Manually opening a service ticket in the Lenovo Support Center” on page 196](#).

For information about setting up Call Home to automatically open a service ticket in the Lenovo Support Center and send the service-data archive when a serviceable event occurs on a device, see [“Automatically opening service tickets using Call Home” on page 193](#).

Procedure

To collect service data for a specific device, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click the **Administration** (🔧) → **Service and Support**, and then click **Device Actions** in the left navigation to display the Device Actions card.

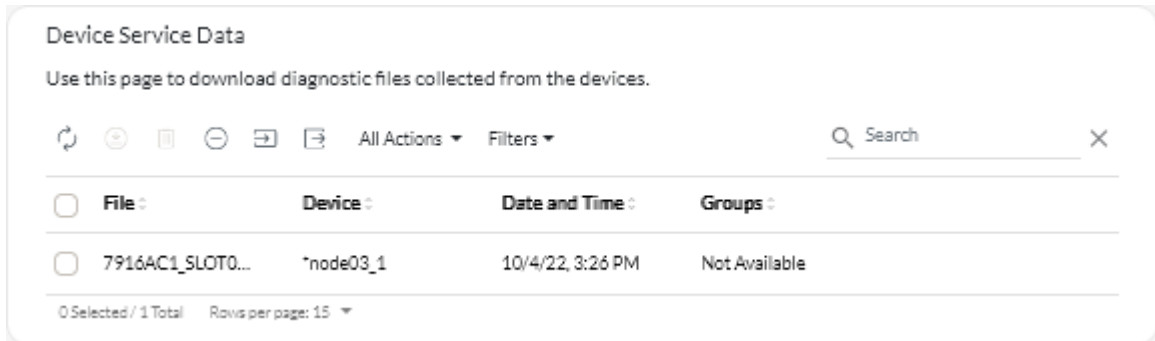
<input type="checkbox"/>	Device	Status	Type	Connectivity	Power	IP Address	Groups	Product Name	Device Type
<input type="checkbox"/>	Newp...	🟡...	Server	🟢...	🟢...	10.243.1	Not Ava	Lenov...	Server
<input type="checkbox"/>	IO Ma...	🟡...	Switch	🟢...	🟢...	10.243.1	Not Ava	IBM F...	Switch
<input type="checkbox"/>	IO Ma...	🟡...	Switch	🟢...	🟢...	10.243.1	Not Ava	IBM F...	Switch
<input type="checkbox"/>	IO Ma...	🟡...	Switch	🟢...	🟢...	10.243.1	Not Ava	IBM F...	Switch
<input type="checkbox"/>	IO Ma...	🟡...	Switch	🟢...	🟢...	10.243.1	Not Ava	IBM F...	Switch
<input type="checkbox"/>	IO Ma...	🟡...	Switch	🟢...	🟢...	192.168	Not Ava	IBM F...	Switch
<input type="checkbox"/>	ite-bt...	🟡...	Server	🟢...	🟢...	10.243.1	Not Ava	Lenov...	Server
<input type="checkbox"/>	IO Ma...	🟡...	Switch	🟢...	🟢...	10.243.1	Not Ava	IBM F...	Switch
<input type="checkbox"/>	IO Ma...	🟡...	Switch	🟢...	🟢...	10.243.1	Not Ava	IBM F...	Switch
<input type="checkbox"/>	IO Ma...	🟡...	Switch	🟢...	🟢...	0.0.0.0,1	Not Ava	IBM F...	Switch

0 Selected / 84 Total Rows per page: 10

Step 2. Select the device for which you want to collect service data, and click the **Collect service data** icon (📄↓).

A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📧) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

Step 3. Click **Device Service Data** in the left navigation to display the Service Data card. The service-data archive is listed in the table.



Device Service Data

Use this page to download diagnostic files collected from the devices.

🔄 📄 🗑️ 📄 📄 All Actions ▾ Filters ▾ 🔍 Search ✕

<input type="checkbox"/>	File :	Device :	Date and Time :	Groups :
<input type="checkbox"/>	7916AC1_SLOT0...	*node03_1	10/4/22, 3:26 PM	Not Available

0 Selected / 1 Total Rows per page: 15 ▾

Step 4. Optionally save the service file to the local system by selecting the file clicking the **Save** icon (📄↓).

After you finish

You can also perform these related actions.

- Manually open a service ticket for a specific device from the Service Tickets card on the device-specific Service page by clicking the **Open service ticket** icon (📄📄) (see [Manually opening a service ticket in the Lenovo Support Center](#)).
- Attach a service-data archive to a selected active service ticket from the Service Tickets card on the device-specific Service page by clicking the **Attach service file** icon (📄⊕). You can attach a file from XClarity Orchestrator or the local system.

Notes:

- You can attach a single archive file that is no more than 2 GB. The file name can be no longer than 200 characters. For information about creating service-data archives, see (see [Collecting service data for devices](#)).
- The service ticket must be in the Open, In Progress, or On Hold state. You cannot attach an archive to a service ticket that is in the Closed or Other state.
- You cannot attach an archive to a *software* service ticket that was opened for Lenovo XClarity Administrator.
- Save one or more selected service-data archives to the local system from the Service Data card by clicking the **Save** icon (📄↓). If multiple files are selected, the files are saved as a single .tar.gz file.
- Delete one or more selected service-data archives that are no longer needed from the Service Data card by clicking the **Delete** icon (🗑️), or delete all archives by clicking the **Delete All** icon (🗑️).

Note: You must be a member of the **SupervisorGroup** group to delete all archives.

Importing service data for devices

You can import a service-data archive for a specific device. The archive can be retrieved from a Lenovo XClarity Administrator resource manager or directly from the baseboard management controller.

About this task

You can import up to 10 files at a time with combined total of 2GB or less.

If you import service data for the same device multiple times, the inventory data is overwritten by the service data that was imported last.

Procedure

To import a service-data archive, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click the **Administration** (⚙️) → **Service and Support**, and then click **Service Data** in the left navigation to display the Device Service Data card.
- Step 2. Click the **Import** icon (📁) to import service-data archives.
- Step 3. Drag and drop one or more service-data archives (in .tar.gz, tzz, or tgz format) to the Import dialog, or click **Browse** to locate the archive.
- Step 4. Optional: Select **Add the server in the service data to the inventory for review only** if the archive is for a device that is not currently managed by XClarity Orchestrator (see [Managing devices offline](#)).
- Step 5. Click **Import** to import and parse the archive and optionally manage the offline device.

A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring** (📊) → **Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see .)

Creating and assigning contacts for service and support

When resources require assistance from Lenovo Support, Lenovo needs to know who to contact. You can define contact information in one place and then assign those contacts as default primary and secondary contacts for specific resources.

Before you begin

Ensure that the [Lenovo Privacy Statement](#) is accepted. You can review and accept the privacy statement from the **Administration** → **Service and Support** → **Call Home Configuration** page.

About this task

You can assign primary and secondary contacts to resource groups. When you assign contacts to a resource group, the contacts are assigned to all resources in that group.

Assigning primary and secondary contacts is optional; however, if you want to assign a secondary contact, you must also assign a primary contact.

If a device is a member of multiple groups, it is possible that each group is assigned a different primary contact. You can choose to use the primary contact assignment for the first group or the last group that the device was assigned to (see [Manually opening a service ticket in the Lenovo Support Center](#)).

If a device is not a member of a group with an assigned primary contact, the Call Home contact is assigned by default. The Call Home contact is used when service tickets are opened automatically using Call Home (see [Automatically opening service tickets using Call Home](#)). Contacts assigned to resources and groups take precedence over the default Call Home contact.

When manually open a service ticket, you can choose to use the contacts that are assigned to the problem resource, or you can choose another contact (see [Manually opening a service ticket in the Lenovo Support Center](#)).

Procedure

- **Define a contact**

1. From the Lenovo XClarity Orchestrator menu bar, click **Administration** (⚙️) → **Service and Support**, and then click **Contact Information** in the left navigation to display the Contact Information card.
2. Click the **Create** icon (+) to display the Add Contact dialog.
3. Fill in the contact name, email, phone number, and location.
4. Select the preferred method of contact.
5. Click **Save** to create the contact.

- **Assign contacts to resource groups**

1. From the Lenovo XClarity Orchestrator menu bar, click **Resources** (📁) → **Groups** to display the Groups card.
2. Select the group, and click the **Edit** icon (✎) to display the Edit group dialog.
3. Select the resource group.
4. Click the **Contact Information** tab.
5. Select the primary support contact and one or more secondary support contact to assign to all devices in the group.
6. Click **Save**.

After you finish

You can perform the following actions from the Contact Information card.

- Modify a selected contact by clicking the **Edit** icon (✎).
- Delete a selected contact by clicking **Remove** icon (🗑️).

Automatically opening service tickets using Call Home

You can set up Lenovo XClarity Orchestrator to automatically open a service ticket and send collected service data to Lenovo Support using the Call Home function when a device generates certain serviceable events, such as an unrecoverable memory, so that the issue can be addressed.

Before you begin

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

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

If XClarity Orchestrator 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 settings](#) in the XClarity Orchestrator online documentation.

Important: If Call Home is enabled on both XClarity Orchestrator and Lenovo XClarity Administrator, ensure that Lenovo XClarity Administrator v2.7 or later is used to avoid duplicate service tickets. If Call Home is enabled on XClarity Orchestrator and disabled on Lenovo XClarity Administrator, then Lenovo XClarity Administrator v2.6 or later is supported.

When contacts are in the following countries, Call Home requires a Lenovo Premier Support contract. For more information, contact your Lenovo representative or authorized business partner.

- Qatar
- Saudi Arabia
- United Arab Emirates

About this task

If Call Home is configured and enabled and a serviceable event occurs on a specific device, XClarity Orchestrator *automatically* opens a service ticket and transfers service data for that device to the Lenovo Support Center.

Important: 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.

When Call Home is not enabled, you can manually open a service ticket and send service files to the Lenovo Support Center by following the instructions on the [How to open a support ticket webpage](#). For information about collecting service files, see .

For information about viewing service tickets that were opened automatically by Call Home, see .

Procedure

To setup Call Home for automatic problem notification, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click the **Administration** (⚙️) → **Service and Support**, and then click **Call Home Configuration** in the left navigation to display the Call Home Configuration card.

Call Home Configuration

From this page, you can configure a Call Home that automatically sends service data for any managed endpoint to Lenovo Support when certain serviceable events occur on a managed endpoint.

[Lenovo Privacy Statement](#)

I agree with the Lenovo Privacy Statement

Customer Details

Customer Number

Primary contact to use from multiple group assignments ?

First group assignment
 Last group assignment

Default Contact

Call Home State: Enabled Disabled

<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

System Location ?

Step 2. Review the [Lenovo Privacy Statement](#), and then click **I Agree with the Lenovo Privacy Statement**

Step 3. Optional: Specify the default Lenovo customer number to use when reporting problems.

You can find your customer number in the proof-of-entitlement email that you received when you purchased your XClarity Orchestrator license.

Step 4. Change the Call Home status to **Enable**.

Step 5. Select the primary contact to use from multiple group assignments.

You can assign a primary support contact to a group of devices. If a device is a member of multiple groups, it is possible that each group is assigned a different primary contact. You can choose to use the primary contact assignment for the first group or the last group that the device was assigned to.

Step 6. Fill in the contact information and preferred method of contact by Lenovo Support.

If a device is not a member of a group with an assigned primary contact, the default contact is used for Call Home.



Step 7. Optional: Fill in the system location information.

Step 8. Click **Call Home Connection Test** to verify that XClarity Orchestrator can communicate with the Lenovo Support Center.


Step 9. Click **Apply**.

After you finish

You can perform the following actions that are related to service data.

- Reset Call Home settings to the default values by clicking **Reset Configuration**.
- View information about *all* service tickets that were submitted to the Lenovo Support Center either automatically or manually using Call Home by clicking **Service Tickets** in the left navigation. For more information, see [Viewing service tickets and status](#).
- Collect service data for a selected device from the Device Actions card by clicking the **Collect Service Data** icon () . For more information, see [Collecting service data for devices](#).
- Attach a service-data archive to a selected active service ticket from the Service Tickets card on the device-specific Service page by clicking the **Attach service file** icon () . You can attach a file from XClarity Orchestrator or the local system.

Notes:

- You can attach a single archive file that is no more than 2 GB. The file name can be no longer than 200 characters. For information about creating service-data archives, see (see [Collecting service data for devices](#)).
- The service ticket must be in the Open, In Progress, or On Hold state. You cannot attach an archive to a service ticket that is in the Closed or Other state.
- You cannot attach an archive to a *software* service ticket that was opened for Lenovo XClarity Administrator.
- 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 from the Device Actions card, selecting the device and then clicking the **Open service ticket** icon () . For more information, see [Manually opening a service ticket in the Lenovo Support Center](#). 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.

Manually opening a service ticket in the Lenovo Support Center

If Call Home is enabled using a service forwarder and a serviceable event occurs on a managed device, Lenovo XClarity Orchestrator 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 service files for a managed device as an archive, save the archive to the local system, and send the files to the Lenovo Support Center at any time. 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.

Before you begin

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.

- Ensure that the Call Home contact information is configured and enabled ([Automatically opening service tickets using Call Home](#)).
- Ensure that XClarity Orchestrator can communicate with the Lenovo Support Center by clicking **Administration** (⚙️) → **Service and Support** from the XClarity Orchestrator menu bar, and clicking **Call Home Configuration** in the left navigation to display the Call Home Configuration page. Then, click **Call Home Configuration Test** to generate a test event and verify that XClarity Orchestrator can communicate with the Lenovo Support Center.
- Ensure that all ports that XClarity Orchestrator 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 Orchestrator 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 Orchestrator online documentation.
- If XClarity Orchestrator 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 settings](#).

Important: 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.

About this task

When manually open a service ticket, you can choose to use the contacts that are assigned to the problem resource, or you can choose another contact.

When primary and secondary contacts are assigned to a group, those contacts become assigned to each device in that group. Each device can be assigned one primary contact and one or more secondary contacts. If a device is a member of multiple groups, all secondary contacts that are assigned to all groups of which the device is a member are assigned to the device. If a device is a member of multiple groups, it is possible that each group is assigned a different primary contact. You can choose to use the primary contact assignment for the first group or the last group that the device was assigned to (see [Automatically opening service tickets using Call Home](#)).

If a device is not a member of a group with an assigned primary contact, the Call Home contact is assigned by default. The Call Home contact is used when service tickets are opened automatically using Call Home (see [Automatically opening service tickets using Call Home](#)). Contacts assigned to resources and groups take precedence over the default Call Home contact.

Procedure

To manually open a service ticket, complete the following steps.

- If Call Home is configured and enabled, perform the following steps to open a service ticket, collect service data, and send the files to the Lenovo Support Center.
 1. From the XClarity Orchestrator menu bar, click **Resources** (🔍), and then click the device type to display a card with a tabular view of all managed devices of that type.
 2. Click the row for the device to display the device summary cards for that device.
 3. Click **Service** in the left navigation to display the Service Tickets card.
 4. Click the **Open service ticket** icon (📄➕) to display the Add New Ticket dialog.
 5. Provide a description of the problem that is being reported, including relevant event codes.
 6. Optionally choose the severity of the problem. This can be one of the following values.
 - **Urgent**
 - **High**
 - **Medium** (default)
 - **Low**
 7. Click **Send**.
- If Call Home is configured and enabled and a serviceable event occurs on a specific device, XClarity Orchestrator *automatically* opens a service ticket and transfers service data for that device to the Lenovo Support Center.

After you finish

You can perform the following actions from the device-specific Service page.

- View information about *all* open service tickets by clicking **Service and Support** → **Service Tickets** from the XClarity Orchestrator menu bar.
- Add a note to a selected service ticket by clicking the **Add service ticket note** icon (📄).

Notes:

- The service ticket must be in the Open, In Progress, or On Hold state. You cannot add a note to a service ticket that is in the Closed or Other state.
- You can add a note to only Lenovo service tickets. You cannot add a note to IBM, Service Now, or Cherwill service tickets.
- You cannot add a note to a *software* service ticket that was opened for Lenovo XClarity Administrator.
- Attach a service-data archive to a selected active service ticket from the Service Tickets card on the device-specific Service page by clicking the **Attach service file** icon (📄➕). You can attach a file from XClarity Orchestrator or the local system.

Notes:

- You can attach a single archive file that is no more than 2 GB. The file name can be no longer than 200 characters. For information about creating service-data archives, see (see [Collecting service data for devices](#)).
- The service ticket must be in the Open, In Progress, or On Hold state. You cannot attach an archive to a service ticket that is in the Closed or Other state.
- You cannot attach an archive to a *software* service ticket that was opened for Lenovo XClarity Administrator.






Viewing service tickets and status

You can view information about service tickets that were manually created or automatically submitted to the Lenovo Support Center using Call Home, and service tickets that were generated by support services other than Call Home.

About this task

Service ticket status is synchronized with Lenovo Support Center every 24 hours.

The **State** column identifies the service ticket status. A service ticket can be in one of the following states:

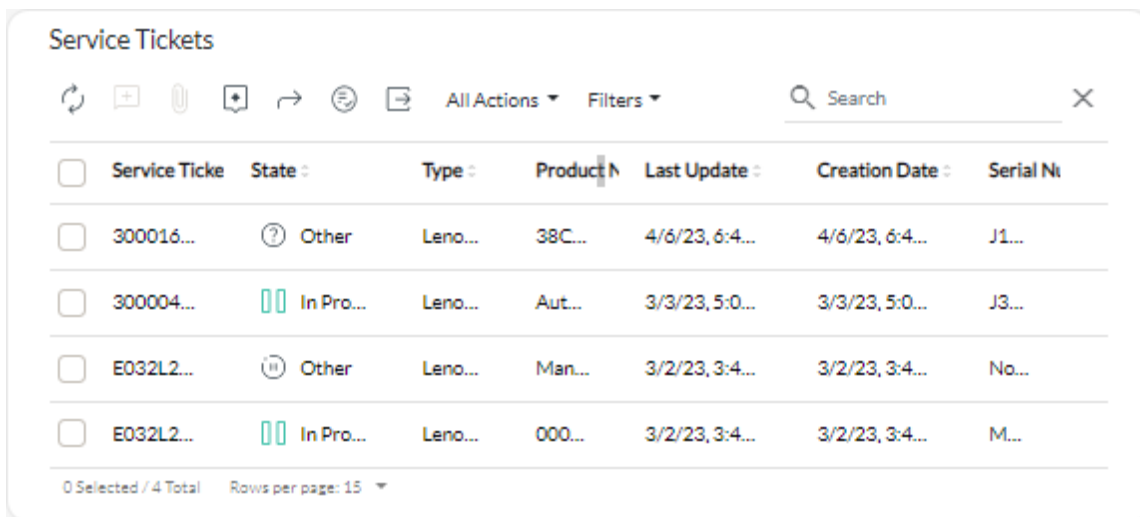
-  **Open**. Lenovo Support received the service ticket but is not actively working on the issue.
-  **In progress**. Lenovo Support is actively working on the issues.
-  **On hold**. Lenovo Support is waiting for feedback and has temporarily paused work on the issue.
-  **Closed**. The service ticket was resolved and is no longer active.
-  **Other**. The status of the service ticket is unknown.





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.


- **Cherwill Ticket**
- **IBM Call Home Ticket**
- **Lenovo Call Home Ticket**
- **Lenovo Call Home Pass Through Ticket**
- **Lenovo Software Call Home Ticket**
- **ServiceNow**

Procedure

- **View the status of all service tickets** Click **Administration**  → **Service and Support**, and then click **Service Tickets** in the left navigation to display the Service Tickets card.



<input type="checkbox"/>	Service Ticket	State	Type	Product	Last Update	Creation Date	Serial Number
<input type="checkbox"/>	300016...	 Other	Leno...	38C...	4/6/23, 6:4...	4/6/23, 6:4...	J1...
<input type="checkbox"/>	300004...	 In Pro...	Leno...	Aut...	3/3/23, 5:0...	3/3/23, 5:0...	J3...
<input type="checkbox"/>	E032L2...	 Other	Leno...	Man...	3/2/23, 3:4...	3/2/23, 3:4...	No...
<input type="checkbox"/>	E032L2...	 In Pro...	Leno...	000...	3/2/23, 3:4...	3/2/23, 3:4...	M...

- **View the status of service tickets for a specific device**
 1. From the XClarity Orchestrator menu bar, click **Resources** , and then click the device type to display a card with a tabular view of all managed devices of that type.
 2. Click the row for the device to display the device summary cards for that device.

- Click **Service** in the left navigation to display the Service Tickets card with a list of service tickets for the device.

Service Data

You can download service-data archives that were collected for a device.

🔄
📄
🗑️
⊖
⬇️
📄

All Actions ▾
Filters ▾

✕

	File :	Device :	Date and Time :	Groups :
<input type="checkbox"/>	7X05RCZ000_SR65...	XCC-7X05-SR650R...	5/4/23, 9:59 AM	Not Available
<input type="checkbox"/>	7X05RCZ000_SR65...	XCC-7X05-SR650R...	5/4/23, 10:11 AM	Not Available
<input type="checkbox"/>	7X05RCZ000_SR65...	XCC-7X05-SR650R...	5/5/23, 8:09 AM	Not Available

0 Selected / 3 Total Rows per page: 15 ▾

After you finish

You can perform the following actions that are related to service tickets.

- Configure XClarity Orchestrator to automatically open a service ticket when a serviceable event occurs (see [Automatically opening service tickets using Call Home](#)).
- Synchronize data with the Lenovo Support Center, and update the status of all active service tickets by clicking the **Update service ticket status** icon (📄+).
- Manually open a service ticket for a specific device from the Service Tickets card on the device-specific Service page by clicking the **Open service ticket** icon (📄+).
- Add a note to a selected service ticket by clicking the **Add service ticket note** icon (📄+).

Notes:

- The service ticket must be in the Open, In Progress, or On Hold state. You cannot add a note to a service ticket that is in the Closed or Other state.
- You can add a note to only Lenovo service tickets. You cannot add a note to IBM, Service Now, or Cherwill service tickets.
- You cannot add a note to a *software* service ticket that was opened for Lenovo XClarity Administrator.
- Attach a service-data archive to a selected active service ticket from the Service Tickets card on the device-specific Service page by clicking the **Attach service file** icon (📄+). You can attach a file from XClarity Orchestrator or the local system.

Notes:

- You can attach a single archive file that is no more than 2 GB. The file name can be no longer than 200 characters. For information about creating service-data archives, see (see [Collecting service data for devices](#)).
- The service ticket must be in the Open, In Progress, or On Hold state. You cannot attach an archive to a service ticket that is in the Closed or Other state.
- You cannot attach an archive to a *software* service ticket that was opened for Lenovo XClarity Administrator.

- Forward reports about active service tickets on a reoccurring basis to one or more email addresses by clicking the **Create Report Forwarder** icon (⊕). The report is sent using the data filters that are currently applied to the table. All shown and hidden table columns are included in the report. For more information, see [Forwarding reports](#).
- Add an active service tickets report to a specific report forwarder using the data filters that are currently applied to the table by clicking the **Add to Report Forwarder** icon (↗). If the report forwarder already includes an active service-tickets report, the report is updated to use the current data filters.

Viewing warranty information

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

Before you begin

Lenovo XClarity Orchestrator 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 Orchestrator online documentation.

- Lenovo Warranty Database (world-wide) – <https://ibase.lenovo.com/POIRequest.aspx>
- Lenovo Warranty Web Service – <http://supportapi.lenovo.com/warranty/> or <https://supportapi.lenovo.com/warranty/>

Notes:

- Warranty support for users in China currently is not supported.
- Warranties are listed for chassis but not the corresponding Chassis Management Modules (CMMs).





About this task



Warranty information is retrieved weekly for devices that have warranties and daily for devices that do not have warranties.

Procedure









To view warranty information, click the **Administration** (⚙️) → **Service and Support**, and then click **Warranty** in the left navigation to display the Warranty card.

Warranty





 All Actions ▾ Filters ▾



 Search 

Device	Status	Product Na	Type-Mode	Warranty N	Serial Num	Start Date	Expiration	Groups
*node02	Not Av...	IBM Flex	7916/...	Not Avail	SLOT002	Not Avail	Not Avail	Not Avail
*node02	Not Av...	IBM Flex	7916/...	Not Avail	SLOT002	Not Avail	Not Avail	Not Avail
*node03	Not Av...	IBM Flex	7916/...	Not Avail	SLOT003	Not Avail	Not Avail	Not Avail
*node03	Not Av...	IBM Flex	7916/...	Not Avail	SLOT003	Not Avail	Not Avail	Not Avail
*node06	Not Av...	IBM Flex	7916/...	Not Avail	SLOT006	Not Avail	Not Avail	Not Avail
*node06	Not Av...	IBM Flex	7916/...	Not Avail	SLOT006	Not Avail	Not Avail	Not Avail
*node09	Not Av...	IBM Flex	7916/...	Not Avail	SLOT009	Not Avail	Not Avail	Not Avail
*node09	Not Av...	IBM Flex	7916/...	Not Avail	SLOT009	Not Avail	Not Avail	Not Avail
*node11	Not Av...	IBM Flex	7916/...	Not Avail	SLOT011	Not Avail	Not Avail	Not Avail
*node11	Not Av...	IBM Flex	7916/...	Not Avail	SLOT011	Not Avail	Not Avail	Not Avail
10.243.1	Expired	Lenovo F	9532/...	3XL	06DGCV	2/24/15,	3/5/18, 7	Not Avail
10.243.1	Expired	IBM Flex	8731/...	IBM	23LAR6E	10/9/11,	10/9/11,	Not Avail
10.243.1	Not Av...	IBM Flex	7916/...	Not Avail	CAR206:	Not Avail	Not Avail	Not Avail
10.243.1	Expired	IBM Flex	7917/...	3XL	06EKZB:	9/12/12,	9/21/15,	Not Avail
10.243.2	Expired	IBM Flex	8737/...	3XL	06PGVA:	4/15/13,	4/24/16,	Not Avail

211 Total Rows per page: 15 ▾


1







After you finish

You can perform the following actions from the Warranty card.

- Look up warranty information (if available) for a specific device on the Lenovo Support website by clicking the link in the **Status** column..
- Forward reports about warranties on a reoccurring basis to one or more email addresses by clicking **All Actions** →  **Add Report Forwarder**. The report is sent using the data filters that are currently applied to the table. All shown and hidden table columns are included in the report. For more information, see [Forwarding reports](#).
- Add a warranties report to a specific report forwarder using the data filters that are currently applied to the table by clicking the **Add to Report Forwarder** icon (). If the report forwarder already includes a warranties report, the report is updated to use the current data filters.

Lenovo