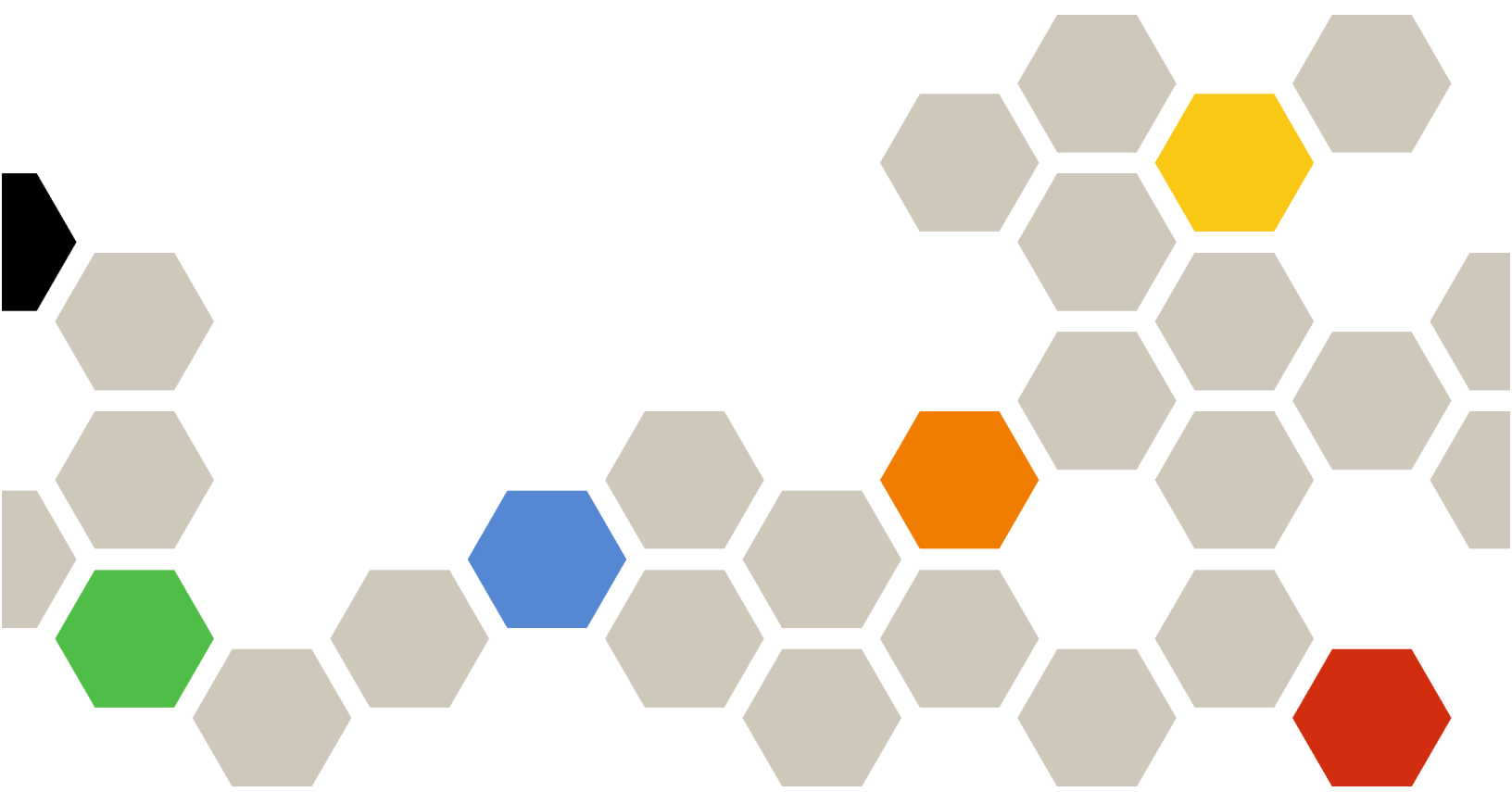




Lenovo XClarity One User's Guide



August 2025 / v1.0

Note

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

Fifth Edition (July 2025)

© Copyright Lenovo 2025, 2025.

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 changes	.iii
Chapter 1. Lenovo XClarity One.	1
Chapter 2. Signing in to the XClarity One portal	3
Signing in to the XClarity One cloud portal	3
Signing in to the XClarity One local portal	4
Chapter 3. Exploring the portal	7
Web interface elements	7
View, pages, and panels	7
Accessibility	11
Chapter 4. Things to do	13
Chapter 5. Security	15
Data security	15
Security emergency	16
Chapter 6. Portal configuration and management	19
Portal network	19
Portal date and time	20
Security certificates	21
Regenerating the self-signed XClarity One server certificate	22
Installing a trusted, externally-signed XClarity One server certificate	23
Importing the XClarity One server certificate into a web browser	25
XClarity One service data	25
Portal backup and restore	27
Backing up and restoring data on a VMware ESXi host	27
Portal restart	28
Portal updates	28
Chapter 7. Authentication and authorization	31
Users	32
Authentication	34
External identity provider	35
Chapter 8. Licenses	37
Importing and activating licenses	39

Chapter 9. Organizations	41
Organizations for managed service providers	42
Chapter 10. Management hubs	45
Management hub connection and management	45
Signing in to the management-hub web interface	47
Management-hub health summary and details	48
Management-hub metrics and trends	49
Function enablement	49
Management-hub power actions	50
Management-hub security certificates	51
Regenerating the self-signed management hub server certificate	52
Installing a trusted, externally-signed management hub server certificate	53
Importing the management hub server certificate into a web browser	55
Management-hub service data	56
Management-hub updates	57
Uninstalling a management hub	58
Chapter 11. Devices	61
Device discovery and management	61
Device health summaries	64
Management functions	64
Usage metrics and trends	66
Device details	67
Collections	69
Remote sever access	70
Power operations	71
Device configuration	71
Firmware	72
Device settings	75
Device templates	77
Vulnerabilities	80
Warranties	81
Call Home contacts	81
Service data	82
Service tickets	83
Chapter 12. Alerts and events	85
Custom alerts	86
Data forwarders	87
Chapter 13. Jobs	91
Chapter 14. Service and support	93

Automatic problem notification (Call Home)	93
Service tickets	94
Technical assistance	95

Chapter 15. Troubleshooting and resolving problems 97

Troubleshooting Organization issues	97
Cannot access an organization	97
Troubleshooting management-hub issues	97
Cannot connect to a management hub	97

Sudden connectivity loss to a management hub	98
Troubleshooting device issues	98
Cannot manage a device	98
Sudden connectivity loss to a device.	98
Troubleshooting firmware-update issues	98
Cannot deploy firmware	98
Troubleshooting template issues	99
Cannot create or edit a template	99

Summary of changes

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

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

This version supports the following enhancements to the management software.

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

Lenovo XClarity One

Function	Description
General	You can use XClarity One for free to manage a maximum of 50 devices for up to 30 days using the free-trial license; however, after the free trial expires, you must purchase and install appropriate licenses to continue using applicable XClarity One functions (see Licenses).
Accessibility	You can navigate through interactive elements in the web interface by using standard keyboard keys (see Accessibility).
Authentication	If you forget your password, your user administrator can reset your password for you (Signing in to the XClarity One portal).
Devices	<p>You can manually import firmware when Lenovo creates a limited-availability fix specifically for you (see Firmware updates).</p> <p>You can choose to deploy a template using prioritized active to limit workload disruption (see Firmware updates).</p> <p>XClarity One can quickly configure and maintain device settings on your managed devices by learning the device-settings configuration from an existing device and then applying that configuration to your other servers (see Device settings).</p> <p>You can disable the device-settings deployment functions globally in all management hubs in your organization from the XClarity One web interface (see Management functions).</p> <p>You can deploy a template to specific devices to update firmware and device settings (see Device templates).</p>
Alert and events	You can create custom alert rules to raise alerts for multiple events, based on metric thresholds (see Custom alerts).

XClarity Management Hub 2.0

Function	Description
Management hubs	<p>You can manage servers using non-standard certificate configurations by importing custom certificate authorities (CAs) and intermediate CAs within the management hub (see Management-hub security certificates).</p> <p>You can configure device settings on target devices through the XClarity One portal (see Device settings).</p> <p>You can view processor, memory, and storage usage statistics for the last hour (see Management-hub metrics and trends).</p>

Chapter 1. Lenovo XClarity One

Designed for unified systems management across supported Lenovo devices, Lenovo XClarity One improves operational efficiency and secures your infrastructure. Building on this foundation, XClarity One is developing AI-powered Smarter Support, with future capabilities set to include advanced predictive maintenance and intelligent analytics. This will empower your infrastructure with enhanced performance, reliability, and efficiency by anticipating needs before they arise.

Attention: XClarity One is a *for-free* offering. To purchase XClarity One or to request a free trial, contact your local Lenovo sales representative (see [Licenses](#)).

XClarity One leverages management hubs that can be installed across multiple sites where your devices are located. The management hubs are light-weight virtual machines that act as a bridge between your devices and the XClarity One portal to collect inventory, incidents, and service data, and to configure firmware and settings on those devices.

XClarity One provides a modern, intuitive interface to manage and monitor your management hubs and managed devices.

- Dashboards that highlight items in your organization that require your attention.
- Summary views of the health of your organizations, hubs, and managed devices.
- Summary and detailed views of component health, asset inventory, and warranty status for your devices across multiple sites
- Aggregation of critical alerts and events, and event forwarding external applications
- Life-cycle control for managed devices using templates (including firmware updates and device settings configuration).
- Remote server and remote console access for management hubs and managed devices
- Usage data and trends, such as processor and memory usage, power consumption, processor temperature
- Automatically problem notification to Lenovo Support using Call Home

XClarity One can be installed flexibly. Today this allows XClarity One to be hosted in the Lenovo cloud with on premise management hubs or as a fully on-premises solution.

- **Cloud**

Using XClarity One in the cloud is recommended for small to medium businesses that desire enterprise-grade capabilities without the heavy upfront investments and IT overhead and for management service providers (MSPs).

The advantages of using XClarity One in the cloud are:

- Lenovo hosts, manages and maintains the XClarity One environment for you.
- Software updates are installed as soon as it is released.
- Security fixes and software updates are installed as soon as possible.
- Customer fixes are installed as soon as possible, depending on the severity.
- Latest Lenovo firmware updates are uploaded as soon as they are released.
- High service level objectives (SLOs).

To get started using XClarity One in the cloud, you need to set up an organization in the XClarity One cloud portal. Your view of XClarity One is based on the organizations that you are part of. An *organization* can be created for your entire company or one or more departments in your company. Only the organization owners and users that are assigned to the organization can access management hubs, devices, and data within the realm of that organization. You can request a new organization from the Sign-in page at xclarityone.lenovo.com. After the organization request is approved by Lenovo, you will receive an email from XClarity One that lets you know that the organization was created and gives a link to get

started. For more information, see [Setting up XClarity One in the cloud](#) in the XClarity One online documentation.

- **Local virtual machine**

XClarity One can be deployed in your local datacenter. This currently requires an internet link for some functions. Note that some functions are not available as local virtual machine.

- Automatic problem notification through Call Home
- Service ticket status and history
- Device warranty
- Lenovo firmware CVE analysis
- Premium Support Plus
- Predictive failure analysis

To get started using XClarity One locally in your data center, you need to download and install XClarity One as a virtual machine. A setup wizard guides you through the initial configuration. For more information, see [Setting up XClarity One as a local VM](#) in the XClarity One online documentation.



[XClarity One: Managing your data center assets](#)

Chapter 2. Signing in to the XClarity One portal

You can sign in to the Lenovo XClarity One portal from any system that has access to the Internet.

Signing in to the XClarity One cloud portal

You can sign in to the [Lenovo XClarity One portal \(xclarityone.lenovo.com\)](https://xclarityone.lenovo.com) from any system that has access to the Internet.

Note: If five consecutive sign-in attempts fail within a 15-minute period or if consecutive sign-in attempts occur too quickly (within 1 second), your user account is locked for 60 minutes.

User sessions

Each user can have up to three user sessions.

A user session expires after 2 hours of active use or after 30 minutes of idle time. When a user session expires, you are signed out automatically and must sign in again to continue your work.

You can view a list of active user sessions and sign out of any unfamiliar sessions. Click **User settings** from the user-account drop-down menu in the upper-right corner, and then click **Account security** → **Active user sessions**.

Notes:

- If your web browser is set up to use a popup blocker, configure the popup blocker to allow the xclarityone.lenovo.com website.
- Ensure that you are using one of the following supported web browsers.
 - Chrome 120 or later
 - Firefox ESR 115.6 or later
 - Microsoft Edge 123 or later
 - Safari 17.2 or later

Signing in to the portal

XClarity One requires two-factor authentication using user credentials and a one-time passcode from an authenticator application.

Local users

When using XClarity One in the cloud, after your user administrator adds you as a new user in the portal, you will receive an email from XClarity One that lets you know that you have access to an organization in the XClarity One portal. Click the **Get started** link in the email to configure your user account and sign in to XClarity One.

Notes:

- The **Get started** link in the email expires after 72 hours. If you do not click the link within that time, contact your user administrator to resend the invitation.
- When you are on the sign-in page, you have 1 hour to complete the sign-in process before you must start over.

During the setup, you are prompted to:

1. Read and accept the [End User License Agreement](#).

2. Configure your password. It is recommended that you use strong passwords of 16 or more characters. By default, passwords for local user accounts must have **8 – 256** characters, including one or more uppercase and lowercase alphabetic characters, numbers, and special characters. Consider the following recommendations when creating passwords.
 - Do not use known passwords obtained from earlier breaches, leaks, or hacks.
 - Do not use dictionary words.
 - Do not use context-specific words, such as the name of a service, an email address, or derivatives thereof.
 - Do not use more than two repetitive or sequential characters (for example, aaa or 123abc).
 - Do not reuse any of the last five passwords.
3. Configure your account settings, including your first and last name.
4. Set up an authenticator application on a mobile device and connect it to XClarity One to obtain the one-time passcode (OTP) that is needed each time you sign in. The following authenticator applications are supported.
 - FreeOTP
 - Google Authenticator
 - Microsoft Authenticator
5. Sign in using your new user credentials and one-time passcode.

Corporate users

After logging in to your company's identity provider, you can access XClarity One portal without providing additional credentials.

Note: Multi factor authentication (MFA) using a one-time passcode is imposed by XClarity One for every user if your external IDP is not set up with MFA (does not have the "amr" claim with value "mfa" set in the JWT tokens).

After your user settings are configured, you can sign in to the XClarity One portal by pointing your browser to xclarityone.lenovo.com.

You can update your personal information, change your password, and manage your authentication applications by clicking **User settings** from the user-account drop-down menu in the upper-right corner.

Resetting your password

If you forget your password, your user administrator can reset your password for you from the **Users** page and provide you with a temporary password. You must change this password the next time you sign in.

Terms, conditions, and Call Home agreements

When you sign in for the first time, you are asked to agree to the [End User License Agreement](#) and the [Call Home agreement](#) (privacy statement). Ensure that you read these agreements in their entirety before clicking **Accept**. You must accept the statements to sign in to XClarity One.

If you already agreed and want to withdraw your agreement, contact XClarity One support using the [Contact Us webpage](#).

Signing in to the XClarity One local portal

When XClarity One is running as a virtual machine, you can sign in to the portal from any system that has network connectivity to XClarity One virtual appliance.

Note: If five consecutive sign-in attempts fail within a 15-minute period or if consecutive sign-in attempts occur too quickly (within 1 second), your user account is locked for 60 minutes.

User sessions

Each user can have up to three user sessions.

A user session expires after 2 hours of active use or after 30 minutes of idle time. When a user session expires, you are signed out automatically and must sign in again to continue your work.

You can view a list of active user sessions and sign out of any unfamiliar sessions. Click **User settings** from the user-account drop-down menu in the upper-right corner, and then click **Account security** → **Active user sessions**.

Notes:

- If your web browser is set up to use a popup blocker, configure the popup blocker to allow the xclarityone.lenovo.com website.
- Ensure that you are using one of the following supported web browsers.
 - Chrome 120 or later
 - Firefox ESR 115.6 or later
 - Microsoft Edge 123 or later
 - Safari 17.2 or later

Signing in to the portal

XClarity One requires two-factor authentication using user credentials and a one-time passcode from an authenticator application.

To sign in to the XClarity One portal, point your browser to the IP address of the XClarity One virtual appliance. If you specified an IPv4 address during installation, use that IPv4 address. If a DHCP server is set up in the same broadcast domain as XClarity One, use the IPv4 address that is displayed in the XClarity One virtual-appliance console.

`https://{IPv4_address}/`

For example, `https://192.0.2.10`

Local users

When you sign in for the first time, you are prompted to set up your user account.

1. Sign in using your username and the temporary password that was set when your user account was created. If you do not know the temporary password, ask your user administrator.
2. Read and accept the [End User License Agreement](#).
3. Configure your password. It is recommended that you use strong passwords of 16 or more characters. By default, passwords for local user accounts must have **8 – 256** characters, including one or more uppercase and lowercase alphabetic characters, numbers, and special characters. Consider the following recommendations when creating passwords.
 - Do not use known passwords obtained from earlier breaches, leaks, or hacks.
 - Do not use dictionary words.
 - Do not use context-specific words, such as the name of a service, an email address, or derivatives thereof.
 - Do not use more than two repetitive or sequential characters (for example, aaa or 123abc).
 - Do not reuse any of the last five passwords.
4. Configure your account settings, including your first and last name.
5. Set up an authenticator application on a mobile device and connect it to XClarity One to obtain the one-time passcode (OTP) that is needed each time you sign in. The following authenticator applications are supported.

- FreeOTP
- Google Authenticator
- Microsoft Authenticator

6. Sign in using your new user credentials and one-time passcode.

Corporate users

After logging in to your company's identity provider, you can access XClarity One portal without providing additional credentials.

Note: Multi factor authentication (MFA) using a one-time passcode is imposed by XClarity One for every user if your external IDP is not set up with MFA (does not have the "amr" claim with value "mfa" set in the JWT tokens).

You can update your personal information, change your password, and manage your authentication applications by clicking **User settings** from the user-account drop-down menu in the upper-right corner.

Resetting your password

If you forget your password, your user administrator can reset your password for you from the **Users** page and provide you with a temporary password. You must change this password the next time you sign in.

Terms, conditions, and Call Home agreements

When you sign in for the first time, you are asked to agree to the [End User License Agreement](#) and the [Call Home agreement](#) (privacy statement). Ensure that you read these agreements in their entirety before clicking **Accept**. You must accept the statements to sign in to XClarity One.

If you already agreed and want to withdraw your agreement, contact XClarity One support using the [Contact Us webpage](#).

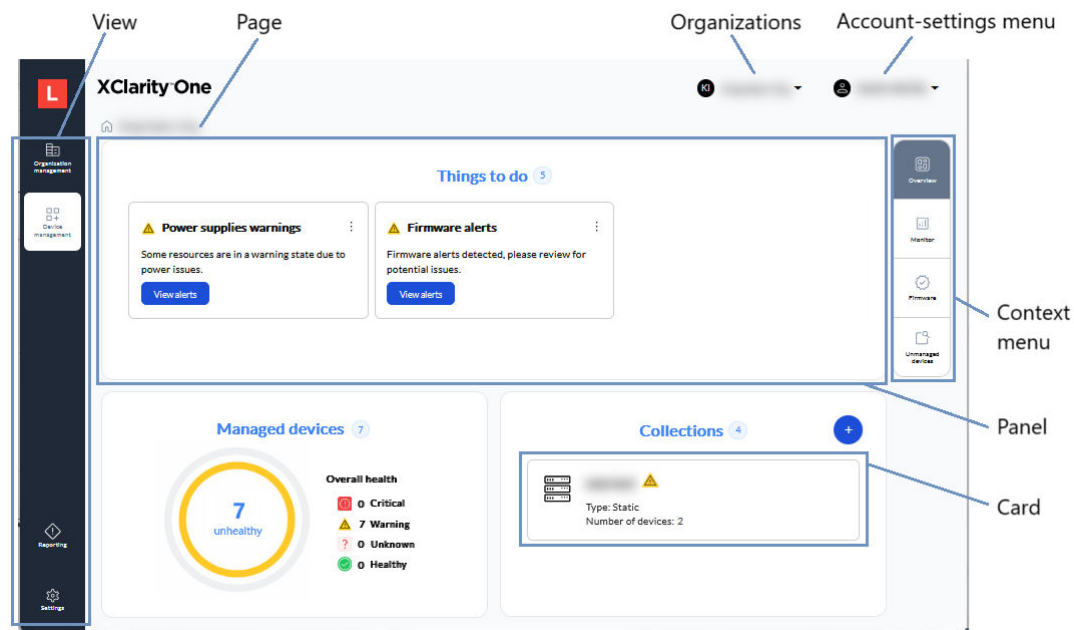
Chapter 3. Exploring the portal

Use this information to learn about accessibility features, terminology, and web interface layout.

Web interface elements

This documentation uses the following terms to describe the web interface.

- **View.** The user interface is organized by the types of data that you are interested in monitoring. You can navigate views using the left-hand menu.
- **Page.** Each view is organized into high-level pages.
- **Panel.** Large rectangular modules on a page that contain different types of information.
- **Card.** Small rectangular modules on a panel that contain a list of elements for that panel.
- **Context menu.** This menu changes the panels that are displayed based on the context of the page.
- **Organizations menu.** From this menu, you can navigate between organizations that you have access to.
- **Account-settings menu.** From this menu, you can manage your user account, view documentation, and provide feedback.



View, pages, and panels

Depending on your user role, you might have access to three possible views in the Lenovo XClarity One portal. As the organization owner, you have access to all these views by default.

- [Organization Management view](#)
- [Device Management view](#)
- [Reports view](#)
- [Settings view](#)

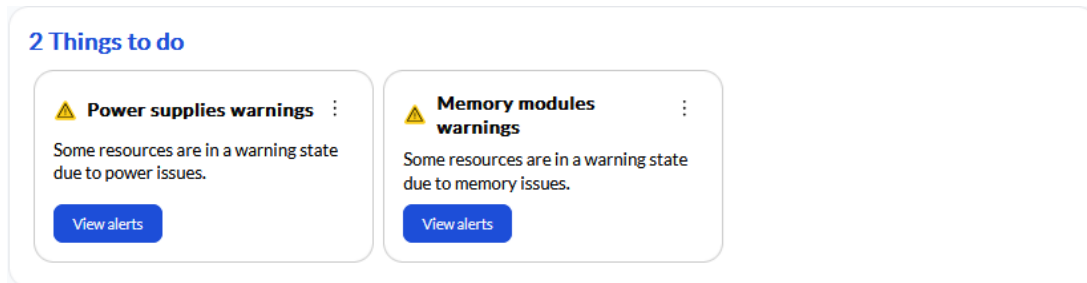
Organization Management view

This view shows information about the organization itself. It contains panels for users and management hubs.

- **Things to do panel**

This panel highlights items in your organization that require your attention. The first user to sign in might see a list of items directing you to add users and connect a management hub. Additional to-dos appear when organization-related issues occur.











You can dismiss todos from the **Things to do** panel. Click the **Things to do** title to display a complete list of all todos, including any to-dos that you dismissed.



- **Users panel**

This panel lists all users that belong to the organization and the roles for each user. Use this panel to invite new users, assign roles, enable or disable users, and delete users from the organization.

The screenshot shows the "Users" panel with a search bar and a table of users. The table has columns for Name, Status, Email, Role, and Last activity. There are three users listed. The first user is the Organization owner, User administrator, Hub administrator, and Device administrator, with a last activity of 29 minute(s) ago. The second and third users are User administrator, Hub administrator, and Device administrator, with a last activity of 8 month(s) ago.




Name	Status	Email	Role	Last activity
 			Organization owner User administrator Hub administrator Device administrator	29 minute(s) ago
			User administrator Hub administrator Device administrator	8 month(s) ago
			User administrator Hub administrator Device administrator	8 month(s) ago

- **Management hubs panel**

XClarity One monitors and manages devices in your datacenter through one or more light-weight device managers, called *management hubs*. Management hubs are installed on premises in your datacenter. They can be setup across multiple sites, where your devices are located.

At least one management hub must be installed and connected to XClarity One for each organization.

Note: The management hubs are the only resources that require direct communication with XClarity One.

Management hubs				
<input type="text" value="Search for anything"/>				
Name and Address	Status	Managed devices	Location	Services
 		2	Bermuda	Device management
<div> 0 selected Items displayed 10 1 - 1 of 1 </div>				

Device Management view

This view shows information about the devices within the organization that are managed by XClarity One. It contains panels for things to do, managed devices, and device collections.

Overview page


This page highlights the overall status of your environment.

- **Things to do panel**

This panel highlights items in your organization that require your attention. When you first sign in, you might see a list of items that highlight how to use the web interface or directing you to manage devices. Additional todos appear when hardware issues occur.


You can dismiss todos from the **Things to do** panel. Click the **Things to do** title to display a complete list of all todos, including any todos that you dismissed.

2 Things to do


Power supplies warnings

Some resources are in a warning state due to power issues.

View alerts

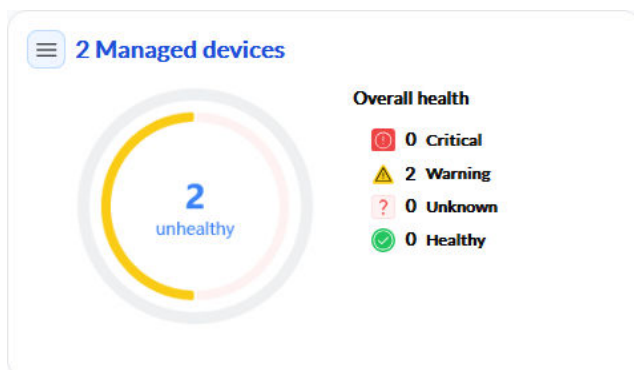

Memory modules warnings

Some resources are in a warning state due to memory issues.

View alerts

- **Managed devices panel**

This panel summarizes the health of all devices in your organization. The overall health of a device is based on the highest severity of all events that are associated with that device.



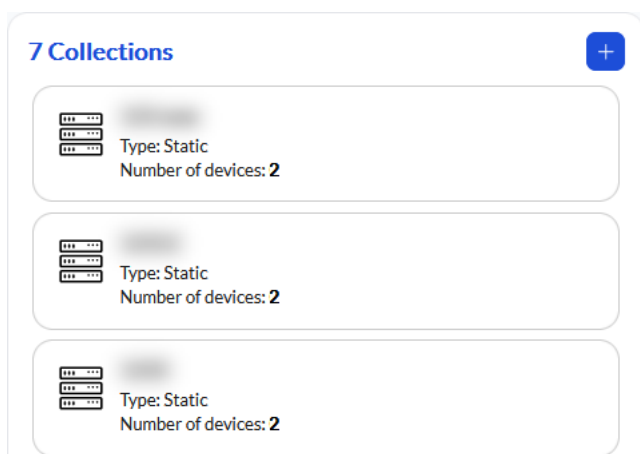
Click the **Managed devices** title to display the list of all managed devices, or click on a severity to display a filtered list of devices with that overall severity. The **Managed devices** page contains context menus for additional information.

- **Overview.** Provides a list of managed devices.
- **Management.** Provides system information about each managed device.
- **Firmware status.** Provides status of firmware that is installed on each managed device.
- **Vulnerabilities.** Provides information about vulnerabilities for each managed device.
- **Warranty information.** Provides warranty for each device.

- **Collections panel**

This panel lists all collections in this organization. A *collection* is a static grouping of devices that can be managed together. A device can belong to one or more collections.

Use this panel to add collections to the organization and to monitor the overall health of all devices in each collection. You can click the card title to list all devices in the collection and add or remove devices from the collection.



Monitoring page

This page shows you current and historical status of the alerts, events, vulnerabilities (CVEs), service tickets, and jobs in your organization. You can click on the card titles to get detailed information.

Configuration management

This page lists contains the resources that you can use to maintain the configuration of your managed devices. You can display the available resources from the context menu.

- **Firmware.** This page lists the current firmware that is available in the XClarity One repository, organized by device type.
- **Device settings** This page lists the device-settings configurations that were created in your organization.
- **Templates.** This page lists provisioning templates that were created in your organization. Templates contain a set of rules and criteria that define the desired configuration for a certain type of server. When you assign a template to a device, XClarity One monitors that device for compliance with the template. If it is out of compliance, you can use the template to update the device to bring it back into compliance.

Unmanaged devices page

This page lists the device that XClarity One discovered in your environment but are not being managed by XClarity One. From this page, you can manually discover new devices and managed device that have been discovered.

Reporting view

This view provides a menu from which you can create a report based on information on the current page and save it to the local system. Only pages with tables are supported, and only tabular data is included in the report.

You can choose which columns to include in the report and set filters to include only the information that interests you.

Reports can be saved in CSV or HTML format.

Settings view

This view shows information about global settings that affect the entire organization. This view lets you get to the following panels through the context menu.

- **Call Home.** This panel configures the default Call Home contact. When configured, Call Home is enabled to automatically opens a service ticket and sends service data to Lenovo Support when certain serviceable events occur on managed devices. For more information, see [Automatic problem notification \(Call Home\)](#).
- **Data forwarding.** This panel configures data forwarders to forward event data, based on specific criteria, to external services that you can then use to monitor and analyze the data. For more information, see [Data forwarders](#).
- **Functions.** This page list the device-management functions that can be enabled or disabled in the portal. Disabling the functions in the portal also disable the functions on the management hubs. Functions can be re-enabled only on the management hubs. For more information, see [Management functions](#).
- **User authentication.** This page configures an external identify provider (IDP) and you can use to authenticate users instead of using the default IDP in XClarity One. For more information, see [External identity provider](#).
- **Thresholds.** This page contains information about device-usage thresholds and custom alert rules for generating specific alerts that you are interested in based the frequency of events or based on user-defined thresholds for device usage metrics.
- **Licenses.** This page manages licenses for using basic and premium features in the XClarity One portal. For more information, see [Licenses](#).

Accessibility

You can navigate through interactive elements in the web interface by using standard keyboard keys.

- You can navigate through interactive elements in the web interface by using the **Tab** key.
- You can expand a menu bar using the **Enter** key and then navigate through the menu by using **arrow** keys.
- You can toggle options by using the **Enter** or **space** key.
- You can activate a link, button, or option using the **Enter** or **space** key.
- Close a dialog using the **Esc** key.

Chapter 4. Things to do

Lenovo XClarity One is a task-oriented interface that highlights items in your organization that require your attention.

Each todos has a button that takes you to a page with a list of filtered events that are related to that todo. You can continue to drill down to figure out the actions that are needed to resolve the issue. After the issue is resolved, the todo is deleted.

You can choose to dismiss todos for yourself or for everyone. Todos are dismissed relative to the page or panel from which you dismissed them. For example, if you dismiss a todo from a server's dedicated page, the todo is dismissed only for that server. If you dismiss a todo from a collection's dedicated page, the todo is dismissed for all devices in that collection.

The **Things to do** panel lists up to six cards for the highest severity todos. To view a list of all todos within the context of a page or panel, including dismissed todos, click the **Things to do** title.

Chapter 5. Security

Lenovo is committed to security. Review the information in this section to learn about the steps that Lenovo takes to ensure that your data is secure and how to lock down your organization in the event of a security emergency.

Data security

Lenovo is committed to security.

Lenovo XClarity One is designed with security as integral to the overall solution and seamless to the end-user experience. The solution is built with the premise of *zero trust* as a guiding strategy. Every component across the data flow is protected using best-in-breed security practices. End-to-end encryption provides the bedrock of the trust-but-verify architecture where every action is authenticated and authorized, both for users, and for machine-to-machine communication. Security in the Software Development Lifecycle provides continuous and immediate feedback to ensure the solution is built as securely as possible. Leveraging cloud security controls from the XClarity One Cloud Service Provider, Microsoft Azure®, the infrastructure running the solution workload is tightened to ensure the environment does not expose the solution to lateral attack. White Hat penetration testers regularly attack the environment from within and without, providing solid protection for customer data and control of customer critical data-center systems

Device data

The XClarity One portal and the locally-installed management hubs store hardware-specific data for all managed devices, including serial numbers, UUIDs, IP addresses and host names, hardware and firmware inventory, drive health, warranty, alerts and events raised by the devices, and usage and predictive failure analysis metrics.

Important:

- Device credentials are stored only on the management hubs in your datacenter. Device credentials are not stored in the cloud.
- Business and application-level data is never collected or stored on the management hubs or in the cloud.

Hardware data is transferred from the managed devices to the management hub and then to the XClarity One portal using HTTPS. Managed devices are not directly connected to the XClarity One portal.

Access to device data is restricted to users that have access to your organization, including service agents. The Lenovo XClarity Support team has administrative access to the XClarity One portal using internal identity management practices and role-based access control. All access to data is logged and audited.

Memory-diagnostic data

The XClarity Controller collects memory-diagnostic logs that are generated by the XCC for DDR4 SDRAM memory modules in managed ThinkSystem devices. Memory-diagnostic logs include current errors, metrics, and post package repair (PPR) data. XClarity One uses this data to improve future AI models that are used for memory predictive failure analysis (MPFA) to predict probable memory failures.

Attention: Memory-diagnostic logs are anonymized and do not contain customer identifiable information. The logs do contain some sensitive information, including device and memory-module serial numbers.

Memory-diagnostic logs are transferred to a database (and periodically pushed to a data lake) in the XClarity One portal as a base64 encoded binary string, using HTTPS, every 24 hours if new logs are available. The data is stored in binary format and is decoded only when pushed to the MPFA AI model infrastructure for

prediction analysis. Memory-diagnostic logs are stored for each managed device until the device is unmanaged.

Lenovo is committed to security. Access to memory-diagnostic data in the XClarity One portal is read-only and is restricted to authorized support personnel.

Service data

When enabled, Call Home automatically collects service data when a serviceable event occurs. You can also manually collect service data for a specific managed device. Service data includes data that is needed to help find the cause of the issue, including service information, inventory, and debug logs.

Attention:

- Service data includes sensitive information, including serial numbers, UUIDs, IP addresses, host names, and device locations. If needed, take appropriate steps to protect any service-data files that were saved to your local system.
- Service data is not stored in the management hubs or in the cloud.

Lenovo is committed to security. When service data is sent to Lenovo Support either automatically through Call Home or manually by you, the service-data archive is sent to Lenovo Upload Facility over HTTPS using TLS 1.2 or later. Your business data is never transmitted. Access to service data in the Lenovo Upload Facility is restricted to authorized service personnel.

Disaster recovery

XClarity One encompasses database-as-a-service, which disperses workloads across different availability zones to mitigate data loss and disaster recovery. After a disaster, you can recover your data when your data center comes back to normal.

Security emergency

Lenovo XClarity One provides the ability to lock portions of your organization, depending on the root of the security issue.

User lockdown

If a user is compromised, you can disable the user's account, which prohibits access to the organization, on the **Users** panel from the **Organization management** view. The **Disabled** icon (⊖) is shown next to the name of disabled users.

In certain circumstances, Lenovo can block users in the portal. Blocked users are prevented from accessing all organizations in the XClarity One portal. Blocked users are identified by the **Blocked** status icon (🔒) icon on the **Users** panel.

Management hub lockdown

If the management hub or managed devices in your organization becomes compromised, you can disable the hub, which blocks communication between the managed devices, management hubs, and XClarity One.

You can disable a management hub on the **Management hub** panel from the **Organization management** view.

Emergency lockdown of an organization

Lenovo can assist in the event of a security emergency that affects the entire organization by locking down your organization.

CAUTION:

When an emergency lockdown is initiated:

- **All management hubs that are managed by the organization are disabled, which blocks communication between the managed devices, management hubs, and XClarity One.**
- **All users are disabled from accessing the organization (except one or more organization owners). User's access to other organizations is not affected.**
- **Users in the pending state for the organization are removed.**

You can choose to keep one or more existing organization owners or user administrators active, or you can choose to create and activate an organization owner with User Administrator, Hub Administrator, and Device Administrator roles. The active users can then work through the security issues. After the security issues are resolved, all users and management hubs can be re-enabled to return to normal operation.

To initiate an emergency lockdown, the organization owner must send a written request to XClarity One support using the [Contact Us webpage](#).

Chapter 6. Portal configuration and management

When running Lenovo XClarity One as a local virtual machine, you can configure the portal settings including network, date and time, web proxy, and security certificates. You can also perform management tasks such as updating the portal software and collecting service data.

Portal network

Review these network considerations to help you set up the network in your datacenter to use Lenovo XClarity One as a virtual machine.

To configure network settings, click **Portal configuration** on the context menu from the **Settings** view.

Network interface (eth0)

XClarity One uses a single network interface (eth0) for management and data communication. Review the following considerations before configuring the network.

- The network interface is used for discovery and management. XClarity One must be able to communicate with all hubs and devices that you intend to manage.
- Some functions require an Internet connection, preferably through a firewall. If the network interface is not connected to the Internet, those functions will not work.

IPv4 address settings

XClarity One uses IPv4 network 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 Dynamic Host Configuration Protocol (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 the network interface.

If DHCP is used to obtain an IP address, the default gateway also uses DHCP.

Attention:

- IPv6 addresses are not supported.
- Network address translation (NAT), which remaps one IP address space into another, is not supported.
- Changing the IP address of the XClarity One virtual-appliance after the portal is up and running will cause connectivity issues with the management hubs. If you need to change the IP address, disconnect management hubs from the portal. After the IP address change is complete, reconnect management hubs to the portal..
- If the network interface is configured to use the DHCP, ensure that IP address changes are minimized by basing the DHCP address on a MAC address or configuring DHCP so that the lease does not expire to avoid communication issues. If the IP address changes when the DHCP lease expires, you must disconnect (delete) the management hub from the portal, and then connect it again.

DNS settings

XClarity One uses IPv4 network settings. You can configure the IP assignment method, up to two static DNS IPv4 addresses, and custom host name and domain.

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 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.

Note: If you choose to use a DHCP server to assign IPv4 address, ensure that the DHCP server is configured such that the DHCP address lease is permanent to avoid communication issues. If the IP address changes when the DHCP lease expires, the host name and domain that you provided are overwritten when the DHCP lease is renewed.

Firewalls

Ensure that the following DNS names and ports are open on the firewall for XClarity One and management hubs. Each DNS represents a geographically distributed system with a dynamic IP address.

Note: IP addresses are subject to change. Use DNS names when possible.

DNS name	Ports	Protocols
Send service data to Lenovo Support (Call Home)		
soaus.lenovo.com	443	https
esupportwebapi.lenovo.com	443	https
Retrieve warranty information		
supportapi.lenovo.com	443	https

Open ports

If management hubs are behind a firewall and if you intend to manage those hubs from an XClarity One instances that is outside of that firewall, you must ensure that all ports involved with communications between the XClarity One portal and each management hub are open.

Service or component	Outbound (ports open to external systems)	Inbound (ports open on target devices)
XClarity One	<ul style="list-style-type: none">• HTTPS - TCP on port 443• HTTPS - TCP on port 8443	<ul style="list-style-type: none">• HTTPS - TCP on port 443
XClarity Management Hub 2.0	<ul style="list-style-type: none">• DNS - UDP on port 53• NTP - UDP on port 123• HTTPS - TCP on port 443• SSDP - UDP on port 1900• DHCP - UDP on port 67	<ul style="list-style-type: none">• HTTPS - TCP on port 443• SSDP - UDP on ports 32768-65535
ThinkSystem and ThinkAgile servers	<ul style="list-style-type: none">• SFTP - TCP on port 115• HTTPS - TCP on port 443• SSDP discovery - UDP on port 1900• Firmware updates - TCP on port 6990	<ul style="list-style-type: none">• HTTPS - TCP on port 443

Portal date and time

Review these considerations to help you configure the date and time for the portal when running Lenovo XClarity One as a local virtual machine.

To configure date and time settings, click **Portal configuration** on the context menu from the **Settings** view, and then locate the **Date and time** panel.

Time zone

Choose the time zone where the portal host is located.

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

NTP server

You can set up one to four Network Time Protocol (NTP) servers to ensure time synchronization between the XClarity One portal, management hubs, and all managed devices.

Attention:

- If the timestamps are not synchronized between the portal and the authentication server, sign in requests using the one-time passcode might fail.
- If the timestamps are not synchronized between the portal and the management hub, you might lose connection to the management hub.
- The portal and its host must be set to synchronize to the same time source to prevent inadvertent time mis-synchronization. Typically, the host is configured to have its virtual appliances time-sync to it. If the portal is set to synchronize to a different source than its host, you must disable the host time synchronization between the portal and its host.

Each NTP server must be accessible over the network.

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

Security certificates

XClarity One uses SSL certificates to establish secure, trusted communications between the portal and management hubs, as well as communications with the portal by users or with different services. When running XClarity One as a virtual machine, the XClarity One portal and the management hubs use XClarity One-generated certificates that are self-signed and issued by an internal certificate authority by default.

Attention: Managing security certificates requires 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](#).

The default server certificate, which is uniquely generated in every instance of XClarity One provides sufficient security for many environments. You can choose to let XClarity One manage certificates for you, or you can take a more active role by customizing and replacing the server certificates. XClarity One 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 authorities to sign a custom certificate that can then be uploaded to the portal to be used as the 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 One provides several services that accept incoming SSL/TLS connections. When a client, such as a web browser, connects to one of these services, the portal 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 a portal certificate is not included in the client's list, the client disconnects from the portal to avoid exchanging any security-sensitive information with an untrusted source.

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

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 One security settings.

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 portal server certificate. It is automatically regenerated each time XClarity One detects that its IP address, hostname or domain name have changed to ensure that the certificate contains the correct addresses for the server.

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), signing the CSR using an private or commercial root certificate authority, and then importing the full certificate chain into the portal (see [Installing a trusted, externally-signed XClarity One 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 XClarity One server certificate into a web browser](#)).

Regenerating the self-signed XClarity One server certificate

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

Attention:

- If you regenerate the portal server certificate using a new root CA, XClarity One loses its connection to the managed devices, and you must re-manage the devices. If you regenerate the portal server certificate without changing the root CA (for example, when the certificate is expired), there is no need to re-manage the devices.
- The self-signed certificate is not secure. You are advised to generate and install your own externally-signed certificate (see [Installing a trusted, externally-signed management hub server certificate](#)).
- You cannot change the subject alternative names when regenerating the self-signed server certificate.

Server-certificate validity period

The server certificate that is currently in use, whether self-signed or externally-signed, remains in use until a new server certificate is generated, signed, and installed. By default, the server certificate expires after 365 days. To customize the validity period, complete the following steps.

1. Click **Portal configuration** from the context menu on the **Settings** view.
2. In the **Regenerate Self-signed Server Certificate** panel, change the number in the **Days** field.

Default self-signed server certificate

To regenerate a self-signed server certificate using default values, complete the following steps.

1. Click **Portal configuration** from the context menu on the **Settings** view.
2. In the **Regenerate Self-signed Server Certificate** panel, click **Reset Certificate**.

Custom self-signed server certificate

To regenerate a self-signed server certificate using custom values, complete the following steps.

1. Click **Portal configuration** from the context menu on the **Settings** view.
2. In the **Regenerate Self-signed Server Certificate** panel, provide values in each field, and then click **Regenerate Certificate**.
 - Organization is typically the legally incorporated name of a company that owns the certificate. Include suffixes, such as Ltd., Inc., or Corp (for example, ACME International Ltd.).
 - Organization unit is the division in the company that owns the certificate (for example, ABC Division).
 - Common name is typically the host name, 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.

Root certificate authority

You can download the root CA to your local system by clicking **Download root CA**.

Installing a trusted, externally-signed XClarity One server certificate

When running Lenovo XClarity One as a virtual machine, 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.

Considerations

Attention:

- If you install an externally-signed server certificate using a new root CA, the portal loses its connection to the managed devices, and you must re-manage the devices. If you install an externally-signed server certificate without changing the root CA (for example, when the certificate is expired), there is no need to re-manage the devices.
- If new devices are added after the CSR is generated and before the signed server certificate is imported, those devices must be restarted to receive the new server certificate.

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 for the portal.

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 One, 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 management hub server certificate into a web browser](#)).

After regenerating or resetting the server certificate, the web browser is refreshed automatically so that you can accept the new certificate.

Installing a trusted, externally-signed server certificate

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

1. Create a certificate signing request and save the file to your local system.
 - a. Click **Portal Configuration** from the context menu on the **Settings** view.
 - b. On the **Generate Certificate Signing Request (CSR)** panel, provide values in each field, and then click **Generate CSR file**.
 - Organization is typically the legally incorporated name of the company that owns the certificate. Include suffixes, such as Ltd., Inc., or Corp (for example, ACME International Ltd.).
 - Organization unit is the division in the company that owns the certificate (for example, ABC Division).
 - Common name is typically the same as 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 common name cannot exceed 63 characters.
 - You can customize the subject alternative names in the X.509 "subjectAltName" extension in the resulting CSR. If you provide one or more subject alternative names in the CSR, only the subject alternative names that you provided are stored in the CSR. You can provide subject alternative names for the following types. Ensure that the names that you specify are valid for the selected type. The specified subject alternative names are validated (based on the specified type) and added to the CSR only after you generate the CSR.
 - **DNS** (use the hostname or FQDN, for example, hostname.labs.company.com)
 - **IP address** (for example, 192.0.2.0)
 - **Email** (for example, example@company.com)

If no subject alternative names are provided, the default names and type from the portal are used.

- **IP Address**. Current portal IP address
- **DNS Name**. Portal hostname
- **DNS Name**. Portal FQDN, if the domain name is provided. Otherwise, this is empty.

Attention: The subject alternative names must include the hostname or fully-qualified domain name (FQDN), and IP address of the portal, and the subject name be set to the hostname or FQDN of the portal. Verify that these required fields are present and correct before beginning the CSR process to ensure that the resulting certificate is complete. Missing certificate data might result in connections that are not trusted when attempting to connect the portal to XClarity One.

Important:

- Before continuing, verify that the newly generated certificate contains the hostname or FQDN as part of the subject alternative names.
 - Ensure that the newly generated certificate is configured to be used as both a *server certificate* and as a *client certificate*.
2. Provide the CSR to a trusted certificate authority (CA). The CA signs the CSR and returns a server certificate.

Attention: All subject alternative names that are stored in the CSR must be used for signing the CSR and generating the web certificate.

3. Import the externally-signed server certificate and the CA certificate to XClarity One to replace the current server certificate.
 - a. On the **Generate certificate signing request (CSR)** panel, click **Import certificate** to display the **Import certificate** dialog.

- b. Insert the externally-signed server certificate, in PEM format. You must provide the entire certificate chain, beginning with the server certificate and ending in the root CA certificate.
- c. Click **Import** to store the server certificate in the portal trust store.

Attention: The subject alternative names that are stored in the CSR on the portal must exactly match the subject alternative names stored in the server certificate being imported. If there is a mismatch (for example, if the IP address from the CSR/signed certificate is not the same with the one from the portal), the importing and installing the server certificate will succeed, but might result in connections that are not trusted (such being unable to access the user interface).

Importing the XClarity One 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 to avoid security warning messages from your web browser when you access XClarity One.

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

1. Export the portal server certificate from the XClarity One portal.
 - a. Click **Portal Configuration** from the context menu on the **Settings** view.
 - b. In the **Self-signed Server Certificate** panel, and then click **Download certificate**.
2. Import the portal server certificate into the list of trusted root authority certificates for your web browser.

- **Chrome**

- a. From your Chrome browser, click the icon with three vertical dots in the upper-right corner of the window, and then, click **Settings** to open the **Settings** page.
- b. Click **Privacy and Security**, and then click **Security** to display the **Security** page.
- c. Scroll to the **Advanced** section, and then click **Manage device certificates**.
- d. Click **Import**, and click **Next**.
- e. Select the certificate file that you previous exported, and click **Next**.
- f. Choose where to store the certificate, and click **Next**.
- g. Click **Finish**.
- h. Close and reopen the Chrome browser, and then open portal web interface.

- **Firefox**

- a. Open the browser, and click **Tools → Settings**, and then click **Privacy & Security**.
- b. Scroll down to the **Security** section.
- c. Click **View certificates** to display the **Certificate Manager** dialog.
- d. Click the **Your Certificates** tab.
- e. Click **Import**, and browse to the location where the certificate was downloaded.
- f. Select the certificate, and click **Open**.
- g. Close the **Certificate Manager** dialog.

XClarity One service data

When running Lenovo XClarity One as a local VM, you can manually collect service data for XClarity One 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.

Online service-data collection

To collect and save XClarity One service data to the local system, click **Portal configuration** on the context menu from the **Settings** view, and then locate the **Service data** panel.

Important: Ensure that web browser does not block pop-ups for the XClarity One website when downloading service data.

Offline service-data collection

If XClarity One becomes unresponsive and cannot be recovered, you can collect service data for that portal instance by clicking **Offline Service File Collection** from the XClarity One Service Support Center portal. You can access the XClarity One Service Support Center portal by pointing your web browser to the XClarity One IP address and port 8443, for example `https://192.0.2.10:8443`.

Notes:

- If you specified a static IPv4 address during installation, use that IPv4 address to access the XClarity One Service Support Center portal.
- If a DHCP server is set up in the same broadcast domain as the VM host, use the IPv4 address that is displayed in the virtual-machine console to access the XClarity One Service Support Center portal.
- Access to the portal is through a secure connection. Ensure that you use **https**.

Specify the service-recovery password in the **Authentication Key** field, and select **Password** as the Authentication type.

Note: If six consecutive log-in attempts fail, within a 15-minute period, you must wait at least 1 hour before signing in again.

Service data is compressed into a single .tar.gz file to your local system. You can choose to collect all service files and management server logs or just the logs.

- **All Service Data.** Includes service logs, syslogs, and information about the virtual machine, operating system, network, processes, containers, and databases.
- **Logs Only.** Includes service logs, syslogs, and information about the virtual machine.

Note: Only the latest archive file is stored in the repository. The file is deleted when the next collection request is made.

Service-recovery password

The service-recovery password and the password-expiration interval were set during initial configuration.

This service-recovery password is needed to collect service data on an unresponsive XClarity One portal. By default, the password must be reset every 90 days. To set the service-recovery password and password-expiration interval (in days), click **Portal configuration** on the context menu from the **Settings** view, and then locate the **Service Recovery Password** panel..

Important: If six consecutive sign-in attempts fail within a 15-minute period or if consecutive sign-in attempts occur too quickly (within 1 second), your user account is locked for 60 minutes.

If you attempt to collect service data for an unresponsive XClarity One portal and the service-recovery password is expired, you are redirected to the **Reset Service Recovery Password** dialog to change the password.

The password must have **16 – 256** characters, including one or more uppercase and lowercase alphabetic characters, numbers, and special characters ; @ _ ! ' \$ & +

Attention: Ensure that you record the password for later use. You cannot recover an unresponsive management hub without using this password.

Portal backup and restore

Lenovo XClarity One does not include built-in backup and restore functions. When using XClarity One as a local virtual machine, use the backup functions that are available based on the virtual-host operating system on which XClarity One is installed.

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

- Before updating XClarity One
- After making any network changes
- After adding users to XClarity One local authentication server
- After managing new management hubs

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

Important:

- Ensure that XClarity One is in a healthy state and no jobs are running before you create a backup.
- Ensure that you back up XClarity One on a regular basis. If the host operating system shuts down unexpectedly, you might not be able to authenticate with XClarity One after the host operating system is restarted. To resolve this problem, restore XClarity One from the last backup.

Backing up and restoring data on a VMware ESXi host

When using Lenovo XClarity One as a local virtual machine, you might need to restore system data, settings, and imported files from a backup. Several alternatives are available to backup and restore an instance of Lenovo XClarity One 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 XClarity One running on VMware ESXi.

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

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 One 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.

Backing up XClarity One

To create a backup of XClarity One using VMware vSphere Client, complete the following steps.

1. Shutdown XClarity One.
2. Launch the VMware vSphere Client, and connect to the ESXi host on which XClarity One is located.
3. Create a new folder in the same datastore that is used by XClarity One.
 - a. Select XClarity One in the navigation tree, and click the **Datastores** tab in the right window.
 - b. Right-click the datastore used by XClarity One, and click **Browse Files**.
 - c. Select the root folder, and then create a new folder to contain a copy of the XClarity One files.
4. Click the XClarity One folder.
5. Select all the files in the folder, and copy the files to the backup folder that you just created.
6. Power on XClarity One.

Restoring XClarity One

To restore XClarity One 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 One is installed.
2. Right-click XClarity One in the left navigation tree, and then click **Power → Power Off**.
3. Right-click XClarity One in the left navigation tree again, and then click Remove from Inventory.
4. Delete the files from the XClarity One folder in the datastore that is used by the XClarity One.
 - a. Select the ESXi host in the navigation tree, and then click the **Datastores** tab in the right window.
 - b. Right-click the datastore used by XClarity One, and click **Browse Files**.
 - c. Select the XClarity One folder.
 - d. Select all files in the folder, and click the **Delete** button.
5. Select the folder where the backup files are stored.
6. Select all the files in the folder, and copy them to the XClarity One folder.
7. In the XClarity One folder, select the VMX file, and click **Register VM**.
8. Complete the wizard to add XClarity One data.
9. Power on XClarity One 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.

Portal restart

There are certain situations when you might need to restart Lenovo XClarity One, such as when regenerating or uploading a server certificate.

- Consider backing up the orchestrator server before restarting (see [Portal backup and restore](#)).
- Ensure that no jobs are currently running. To view the jobs log, see [Jobs](#).

When XClarity One restarts, it recollects inventory for each managed device. Wait approximately 30-45 minutes, depending upon the number of managed devices, before attempting to configure devices.

From the hypervisor

- **VMware ESXi**
 1. Connect to the host through VMware vSphere Client.
 2. Right-click the virtual machine, and click **Power → Reset**.
 3. Click the **Console** tab.

Portal updates

When using Lenovo XClarity One as a local virtual machine, it is important to keep the portal up to date with the latest release.

Manually updates

If XClarity One is not connected the Internet, you can manually update the portal by completing the following steps.

You can update XClarity One to only the next ordinal release, for example from v1.0 to v1.1 or v1.1 to v1.2. You cannot skip releases when updating the portal.

During the update process, all users are signed out of the portal when the portal restarts. Wait several minutes until the restart completes. Then, clear the web browser cache and refresh the web browser before signing in again.

Notes:

- You can update XClarity One to only the next ordinal release, for example from v1.0 to v1.1 or v1.1 to v1.2. You cannot skip releases when updating the portal.
- During the update process, all users are signed out of the portal when the portal restarts. Wait several minutes until the restart completes. Then, clear the web browser cache and refresh the web browser before signing in again.
- If you encounter a 413 error (entity too large) when you attempt to upload the portal update package, increase the number of processors on the VM. For example, if your VM has 2 processors, increase the VM to 4 processors.

Download the portal update package from the [XClarity One downloads webpage](#) to a workstation that has a network connection to the XClarity One host server. The update package is a .tar.gz or .tgz archive that contains the four required update files: update image (.tgz or .tar.gz), metadata (.xml), change log (.chg), and readme (.txt).

Import and install the update by clicking **Maintenance** from the context menu on the **Settings** view.

Importing the update files might take a while. When the import is complete, the update package is listed in the table on the portal update panel.

After the update completes, clear the web browser cache, and refresh the web browser.

Chapter 7. Authentication and authorization

You can sign in to the Lenovo XClarity One portal from any system that has access to the Internet.

Signing in to the portal for the first time

Local users

When using XClarity One in the cloud, after your user administrator adds you as a new user in the portal, you will receive an email from XClarity One that lets you know that you have access to an organization in the XClarity One portal. Click the **Get started** link in the email to configure your user account and sign in to XClarity One.

Notes:

- The **Get started** link in the email expires after 72 hours. If you do not click the link within that time, contact your user administrator to resend the invitation.
- When you are on the sign-in page, you have 1 hour to complete the sign-in process before you must start over.

When running XClarity One as a virtual machine, after your user administrator adds you as a new user in the portal, you can sign in to the portal by pointing your browser to the IP address of the XClarity One virtual appliance. If you specified an IPv4 address during installation, use that IPv4 address. If a DHCP server is set up in the same broadcast domain as XClarity One, use the IPv4 address that is displayed in the XClarity One virtual-appliance console.

`https://{IPv4_address}`

For example, `https://192.0.2.10`

During the setup, you are prompted to:

1. Read and accept the [End User License Agreement](#).
2. Configure your password. It is recommended that you use strong passwords of 16 or more characters. By default, passwords for local user accounts must have **8 – 256** characters, including one or more uppercase and lowercase alphabetic characters, numbers, and special characters. Consider the following recommendations when creating passwords.
 - Do not use known passwords obtained from earlier breaches, leaks, or hacks.
 - Do not use dictionary words.
 - Do not use context-specific words, such as the name of a service, an email address, or derivatives thereof.
 - Do not use more than two repetitive or sequential characters (for example, aaa or 123abc).
 - Do not reuse any of the last five passwords.
3. Configure your account settings, including your first and last name.
4. Set up an authenticator application on a mobile device and connect it to XClarity One to obtain the one-time passcode (OTP) that is needed each time you sign in. The following authenticator applications are supported.
 - FreeOTP
 - Google Authenticator
 - Microsoft Authenticator
5. Sign in using your new user credentials and one-time passcode.

Corporate users

After logging in to your company's identity provider, you can access XClarity One portal without providing additional credentials.

Note: Multi factor authentication (MFA) using a one-time passcode is imposed by XClarity One for every user if your external IDP is not set up with MFA (does not have the “amr” claim with value “mfa” set in the JWT tokens).

After your user settings are configured, you can sign in to the XClarity One portal by pointing your browser to xclarityone.lenovo.com.

Resetting your password

If you forget your password, your user administrator can reset your password for you from the **Users** page and provide you with a temporary password. You must change this password the next time you sign in.

Users

Users can be added by any user administrator in the organization.



[XClarity One: Users management](#)

Hover over an icon in the **Status** column on the **Users** panel to see details about the status of the user. Hover over an entry in the **Last Activity** column to see a time stamp for when the activity occurred.

You can update your personal information, change your password, and manage your authentication applications by clicking **User settings** from the user-account drop-down menu in the upper-right corner.

Username

The username is the same as the user’s email address. The email address is formatted as *{local-part}@{domain}*. The maximum length, including the local part and domain, is 320 characters.

The *local part* is case-sensitive and can contain hyphens, underscores, plus signs, and spaces in addition to letters and numeric characters in supported languages. If the local part contains special characters, you can enclose the local part in double quotes (for example, “John Doe”@company.com). You can also add a comment in parentheses (for example, john(some comment)@company.com).

The *domain* for all users (except service agents) in the same organization must be the same as the organization owner. Only service agents can have a different domain (see [Service agents on page](#)).

User roles

Each user can perform actions based on the roles that are assigned to them in the organization. Each user is assigned one or more of the following roles.

Important: If you change roles for a user that is currently signed in, that user must sign out and then sign in again to see the correct privileges.

- **User administrator**

User administrators manage users in the organization, including inviting new users, assigning roles, and enabling or disabling users.

An organization must have at least one active user administrator; however, at least two user administrators is highly recommended for redundancy and security.

- **Hub administrator**

Hub administrators manage management hubs in the organization, including adding (connecting), removing (disconnecting), and enabling or disabling hubs.

- **Device administrator**

Device administrators can manage devices in the organization, including viewing inventory and health, , managing device configuration (firmware and device settings), remotely accessing the management controller and server console, monitoring and forwarding events and alerts, monitoring jobs, collecting service data, and opening and monitoring service tickets related to those devices. They can also create and manage collections of devices, and monitor health and usage metrics for the entire collection.

Device administrators also have read-only access to the list of organization users and their associated roles and status.

- **Service agent**

The service agent role can be assigned to users that are members of a *service-provider organization* (see [Organizations](#)). This role permits users to be added to other organizations, even though their email domain is different than the email domain of the other organization owners. Note that the email domain for service-agent email addresses must be in the same domain as the service-provider organization owner.

This role does not give users the ability to perform any actions. When you add service-agent users to your organization, you assign additional roles to those users to determine what actions they are allowed to perform.


If the service-provider organization is disabled, all service agents in that organization are blocked from all other organizations to which they have access.

If the organization owner or user administrator of the service-provider organization removes the service-agent role from a user, that user is automatically blocked from all other organizations to which they have access.

If a service-agent user is disabled or removed from a non-service-provider organization, that user is disabled or removed from only that organization. If a service-agent user is disabled or removed from a service-provider organization, that user is automatically disabled or removed from all organizations, including non-service-provider and service-provider organizations.

Service agents are identified by the **Service Agent** icon () icon on the **Users** panel.

Organization owners

The user that submits the new-organization request becomes an *organization owner*. Organization owners, identified using the owner icon () , can manage users and configure organization-specific settings, such as the default Call Home contact, usage-metric thresholds, and data forwarders. In addition, the first organization owner also has full access to the organization by default, including hub and device administrator roles.

When running XClarity One as a virtual machine, organization owners can also configure the portal, including network, date and time, and security certification.

Note: Only organization owners can create local user accounts when your organization uses a corporate identity provider for authentication.

Each organization must have at least one active owner; however, at least two owners is highly recommended for redundancy and security.

Only an owner can add or remove the owner property from another user. Owners cannot remove the owner property from their user account.

Important: If you add or remove the owner property from a user that is currently signed in, that user must sign out and then sign in again to see the correct privileges.

If an owner leaves the company before assigning the ownership to another user, you may contact XClarity One support using the [Contact Us webpage](#) to request that the owner account be immediately disabled for 24 hours.

Disabled versus blocked users

A user administrator can disable any users (except themselves) in an organization. A disabled user is prevented from accessing that organization. Disabled users are identified by the **Disabled** status icon (⊖) icon on the **Users** panel.

In certain circumstances, Lenovo can block users in the portal. Blocked users are prevented from accessing all organizations in the XClarity One portal. Blocked users are identified by the **Blocked** status icon (⊘) icon on the **Users** panel.

Authentication

Lenovo XClarity One requires two-factor authentication using your user credentials and a one-time passcode from an authenticator application. You can configure the authentication methods to use to sign in to the XClarity One portal by clicking **Account settings** from the user-account drop-down menu in the upper-right corner.

Note: If five consecutive sign-in attempts fail within a 15-minute period or if consecutive sign-in attempts occur too quickly (within 1 second), your user account is locked for 60 minutes.

User credentials

Your username is your email address.

It is recommended that you use strong passwords of 16 or more characters. By default, passwords for local user accounts must have **8 – 256** characters, including one or more uppercase and lowercase alphabetic characters, numbers, and special characters. Consider the following recommendations when creating passwords.

- Do not use known passwords obtained from earlier breaches, leaks, or hacks.
- Do not use dictionary words.
- Do not use context-specific words, such as the name of a service, an email address, or derivatives thereof.
- Do not use more than two repetitive or sequential characters (for example, aaa or 123abc).
- Do not reuse any of the last five passwords.

Note: Passwords for local user accounts must be changed at least every 365 days. You can change your password by clicking **User settings** from the user-account drop-down menu in the upper-right corner, and then clicking **Account security** → **Signing in**.

One-time passcode (OTP)

You must setup an authenticator application on a device and connect to XClarity One to obtain the one-time passcode (OTP) that is required each time you sign in. The following authenticator applications are supported.

- FreeOTP
- Google Authenticator
- Microsoft Authenticator

If you have authenticator applications set up on multiple devices, you can provide a custom name for each device. During sign in, you can choose which device to use for the one-time passcode.

If you no longer have an active user session and you lose the authenticator application or the authenticator token in the application, contact the user administrator for your organization. User administrators can reset the multi-factor authenticator to remove all authenticator applications for another user in the same organization. After your multi-factor authenticator is reset, you must setup a new authenticator application the next time you log in.

If you have an active user session and can access your account settings, you can set up a new authentication application by clicking **User settings** from the user-account drop-down menu in the upper-right corner, and then clicking **Account security → Signing in**.

User sessions

Each user can have up to three user sessions.

A user session expires after 2 hours of active use or after 30 minutes of idle time. When a user session expires, you are signed out automatically and must sign in again to continue your work.

You can view a list of active user sessions and sign out of any unfamiliar sessions. Click **User settings** from the user-account drop-down menu in the upper-right corner, and then click **Account security → Active user sessions**.

Notes:

- If your web browser is set up to use a popup blocker, configure the popup blocker to allow the xclarityone.lenovo.com website.
- Ensure that you are using one of the following supported web browsers.
 - Chrome 120 or later
 - Firefox ESR 115.6 or later
 - Microsoft Edge 123 or later
 - Safari 17.2 or later

External identity provider

Lenovo XClarity One uses an internal identity-management system to authenticate local users. You can choose to set up federation using your company's existing identity provider (IDP) to provide seamless access to the XClarity One portal using corporate credentials without the need for additional user-account creation or management, while maintaining strong identity and access management practices.

You can configure XClarity One portal to use a federation IDP that supports OIDC/OAuth and SAML protocols. The following IDPs are supported. If your identity provider is not listed, open a service ticket using the [Submit an eTicket webpage](#).

- Amazon Cognito IAM
- Auth0 (by OKTA)
- Google Cloud IAM
- Microsoft Entra ID
- OKTA
- OneLogin
- Ping One (by Ping Identity)

To configure an external IDP for your organization, click **User Authentication** in the context menu of the **Settings** view, click **Set up** in the **Federated sign-in information** section, and follow the steps in the wizard.

After XClarity One is set up to use your external IDP, sign-in requests from the XClarity One portal are redirected to your external IDP for authentication, based on the email domain for the user. After the user is authenticated, the web browser is redirected back to the XClarity One portal.

After you set up an external IDP, you can edit the mappers and secrets but not the protocol. If you need to change the protocol, remove the configuration by clicking **Remove** from the **User Authentication** card, and then click **Set up** to configure the external IDP.

Email domain

The external IDP is setup based on your company's email domain. If your company has multiple organizations that use the same email domain, the external IDP is available to all organizations with the same domain.

Multi factor authentication

XClarity One requires multi-factor authentication to prevent malicious attacks in the XClarity One portal within your organization and across organizations. If multi-factor authentication is not already setup in your federation identity provider, XClarity One will handle it for you.

Local vs corporate users

When users are added to XClarity One, including the initial organization owner, a local user account is created in the internal identity-management system. After your company's external IDP is set up for your organization, those users might also have a corporate user account in the external IDP. The first time a user with both local and corporate (federated) user accounts attempts to sign in, the user is prompted to link the two accounts. Those users can then choose whether to authenticate using their local or corporate user account. If you chose to use your corporate user account, and later you want to use your local account, press Alt + . from the corporate-account sign in page to get redirected to the local-account sign in page.

Notes:

- When using the XClarity One cloud portal, an email is sent to you to link your corporate and local user accounts.
- When using a XClarity One local portal, the web interface prompts you to sign in again using your credentials and one-time passcode to link your corporate and local user.

After logging in to the corporate IDP, corporate users can access the XClarity One portal without providing additional credentials. In addition, XClarity One requires multifactor authentication by providing a one-time passcode (OTP) from an authenticator application that is connected to XClarity One.

If the corporate IDP is disabled or removed, all corporate users are disabled. Users with local user accounts can still sign in using local XClarity One credentials.

Chapter 8. Licenses

Lenovo XClarity One is a for-fee cloud or virtual machine offering. You must acquire appropriate licenses to use XClarity One.

You can use XClarity One for free to manage a maximum of 50 devices for up to 30 days using the free-trial license; however, after the free trial expires, you must purchase and install appropriate licenses to continue using applicable XClarity One functions and to get XClarity One service and support.

Notes:

- For XClarity One in the cloud, contact your authorized Lenovo representative to request a free trial.
- Licenses are tied to specific organizations but are not tied to specific managed devices in the organization.
- Ensure that the customer number used to purchase the licenses matches the customer number for your organization.

You can view information about your licenses by clicking **Licenses** in the context menu of the **Settings** view. XClarity One supports the following types of licenses.

- **Managed-device licenses**

A managed-device license is required for *every managed device* to use basic monitoring and management functions in the XClarity One portal and entitlement for XClarity One service and support. The licenses that you need depend on whether you are using XClarity One in the cloud or running it as a virtual machine in your datacenter (on premises).

- **XClarity One – Managed Device, Per Endpoint**
- **XClarity One – On-Premises – Managed Device, Per Endpoint**

License compliance is determined based on the total number of managed devices in the organization. The number of managed devices must not exceed the total device limit for all active managed-device licenses.

After the free trial, if the Manage Device licenses become non-compliant (for example, when licenses expire or when newly managed devices exceed the total device limit for all active basic licenses), an alert is raised and a todo is added to the **Things to do** panel. You have a short grace period to acquire new licenses.

Attention:

- You use the **XClarity One – Upgrade - Managed Device, Per Endpoint** licenses to convert your active **XClarity Pro** licenses to **XClarity One – Managed Device, Per Endpoint** licenses. The number of licensed devices and expiration date for the upgraded licenses will be the same as the **XClarity Pro** licenses.
- To remotely access to the baseboard-management controller in your managed devices without having a VPN connection to your datacenter or edge where your devices are located, you must purchase and install **XCC Platinum** or **XCC Premium** licenses on your managed devices.

- **Premium licenses**

You can optionally purchase separate licenses to enable any of the following premium functions. The licenses that you need depend on whether you are the cloud-based or local-based (on premises) XClarity One portal.

- **Memory Predictive Failure Analytics licenses**

You can optionally purchase **XClarity One – Memory PFA MD Option** or **XClarity One – On-Premises – Memory PFA MD Option** licenses to monitor and analyze memory errors and failure predictions to ensure that your devices are operating at peak performance.

Important: Memory predictive failure analytics (MPFA) supports only DDR4 SDRAM memory modules in certain devices. For a list of supported devices, see the [XClarity Management Hub 2.0 Support for Servers webpage](#).

When you purchase a premium license, XClarity One creates a *licensed collection* for the premium license type. You can choose which devices can use the premium license by adding or removing devices from the licensed collection. The number of devices in the licensed collection must not exceed the total device limit for all active premium licenses of that type.

If premium licenses become non-compliant (for example, when licenses expire or when the number of devices in the licensed collection exceed the total device limit), an alert is raised and a todo is added to the **Things to do** panel. You have a short grace period to acquire new licenses. If you do not purchase a new license with the appropriate device limit before the grace period ends, the function is disabled.

- **Managed service provider licenses**

If you are a business that provides IT solutions and services to other companies, you can change your organization to a *managed service-provider* (MSP) organization. To become an MSP in XClarity One, you must first purchase an **XClarity One – MSP enablement** license for each customer that you service and then contact Lenovo XClarity Support ([Contact Us webpage](#)).

After purchasing the MSP enablement license, contact Lenovo XClarity Support ([Contact Us webpage](#)) to add the service-provider flag to your organization.

Note: This license is available only for XClarity One in the cloud.

Purchasing licenses

Contact your Lenovo sales representative or authorized Business Partner to purchase licenses for XClarity One based on whether you are using cloud-based or local-based (on premises) XClarity One portal, the functions that you want to enable and the number of devices that you want to manage.

For XClarity One in the cloud, purchased licenses are automatically applied to your organizations based on your Lenovo customer number.

- If you have not yet requested an organization, your purchased licenses are automatically applied after the organization request is made (see [Requesting a new organization](#) in the XClarity One online documentation).
- If you have one or more active organizations, your purchased licenses are automatically applied to your oldest active organization. If there are no active organizations with the same customer number, licenses are applied to the oldest pending or requested organization. If none are pending or requested, licenses are applied to the oldest disabled organization.

For XClarity One running as a local VM, you must download and import the licenses into the portal.

Note: Licenses with the same name and expiration date are considered the same license with an aggregated usage or units limit.

Attention: When your license purchase is complete, you will receive a proof-of-entitlement email containing your Lenovo customer number.

- If you have issues and you used a Business Partner, contact your Business Partner to verify the transaction and entitlement.

- If you did not receive your electronic proof of entitlement, if the licenses were sent to wrong person, or if the licenses are listed in the portal for your organization, contact one of the regional representatives, based on your geography.
 - ESDNA@lenovo.com (North American countries)
 - ESDAP@lenovo.com (Asia Pacific countries)
 - ESDEMEA@lenovo.com (European, Middle Eastern, and Asian countries)
 - ESDLA@lenovo.com (Latin American countries)
 - ESDChina@Lenovo.com (China)
- If information about your entitlement is not correct, contact Lenovo Support at SW_override@lenovo.com and include the following information.
 - Order number
 - Your contact information, including email address
 - Your physical address
 - Changes that you want made

License status

You can determine the status of your licenses by clicking **Licenses** in the context menu of the **Settings** view.

- **healthy.** License is active and the number of managed devices is within the limit of the license.
- **warning.** The license will expire in less than 3 months or when the number of managed devices exceeds the license limit by less than or equal 5% or 100 devices (whichever comes first).
- **critical.** The license expired or the number of managed devices exceeds the license limit by more than 5% or 100 devices.

Importing and activating licenses

After purchasing licenses for XClarity One, you need to import the licenses to activate functions in the portal.

Important:

- Ensure that you purchased the correct licenses, depending on whether you are using XClarity One in the cloud or as a local virtual machine. For more information, see [Licenses](#).
- Ensure that the customer number used to purchase the licenses matches the customer number for your organization.

To import and activate XClarity One licenses, complete the following steps.

1. Retrieve your authorization code.

When the license purchase is complete, an authorization code is sent to you in an *electronic proof of entitlement* email. You can also retrieve the authorization code from the [Lenovo Features on Demand web portal](#) by clicking **Retrieve authorization code**. If you do not receive the email and you purchased the license through a Business Partner, contact your Business Partner to request the authorization code.

The authorization code is a 22-character alphanumeric string. You will need the authorization code to complete the next step.

2. Retrieve the activation keys for the licenses.

• Creating activation keys from an authorization code

- Open the [Lenovo Features on Demand web portal](#) from a web browser, and log in to the portal using your email address as your user ID.
- Click **Request activation key**.
- Select **Input a Single Authorization Code**.
- Enter the 22-character authorization code, and click **Continue**.
- Enter your Lenovo customer number in the **Lenovo Customer Number** field.

- f. Enter the number of licenses that you want to redeem in the **Redeem Quantity** field, and then click **Continue**. To redeem all the available licenses in this key, match the number in **Available licenses** field.

If you redeem a subset of available licenses, you can redeem the remaining licenses in another activation key using the same authorization code.

- g. Follow the prompts to enter product details and contact information, and click **Continue** to generate the activation key.
- h. Optionally specify additional recipients to receive the activation keys.
- i. Click **Submit** to send the activation keys. The person assigned to the purchase order and the additional recipients will receive an email with the activation key. The activation key is a file in .KEY format.

Note: You can also download activation keys (individually or in batch) from the [Lenovo Features on Demand web portal](#) by clicking **Download link**.

- **Downloading existing activation keys**

- a. Open the [Lenovo Features on Demand web portal](#) from a web browser, and log in to the portal using your email address as your user ID.
 - b. Click **Retrieve History**.
 - c. Select "Search history via Lenovo Customer Number" as the **Search type**.
 - d. Enter your Lenovo Customer number in the **Search Value** field. The customer number format is 121XXXXXXX.
 - e. Click **Select all** to download all activation keys or select individual activation keys from the list.
 - f. Click **Email** to email the keys to you, or click **Download** to download the keys to your local system.
3. Import and apply licenses in XClarity One by clicking **Licenses** from the context menu on the **Settings** view. Follow the instructions in the wizard to complete the import process.
 4. If you applied the valid licenses after functions were disabled, log out and then log in again to enable the applicable functions.

Chapter 9. Organizations

Your view of Lenovo XClarity One is based on the organizations that you are part of.

When using XClarity One in the cloud, an *organization* is typically created for your entire company or one or more departments in your company. If you set up multiple organizations for your company, you can give users access to one or more of your organizations. Users can switch between organizations at any time from the organization menu on top bar of the web interface.

When running XClarity One as a virtual machine,, you can set up only a single organization during initial setup. You cannot request additional organizations, disable the organization, or delete the organization.

Only the organization owners and users that are assigned to the organization can access management hubs, devices, and data within the realm of that organization.

The user that submits the new-organization request becomes an *organization owner*. Organization owners, identified using the owner icon (★), can manage users and configure organization-specific settings, such as the default Call Home contact, usage-metric thresholds, and data forwarders. In addition, the first organization owner also has full access to the organization by default, including hub and device administrator roles.

When running XClarity One as a virtual machine, organization owners can also configure the portal, including network, date and time, and security certification.

Requesting a new organization

When using XClarity One in the cloud, you can submit a request for a new organization by clicking the **Request a new organization** link at the bottom of the **Sign In** dialog or by going directly to the **Request a new organization** dialog using xclarityone.lenovo.com/#/register. You need your Lenovo customer number to associate with the organization. If you do not have your Lenovo Customer Number, check the proof of entitlement email that was sent to you when you purchased your XClarity One licenses or contact your local Lenovo Sales Representative to get it.

If you purchased licenses before requesting an organization, the organization request is approved immediately, and the licenses are automatically applied to the organization. If you have not yet purchased licenses, the organization is not created until the request is approved by Lenovo, which is typically done within one business day. When your organization request is approved, XClarity One sends you an email to get started. Click the link in the email to sign in to XClarity One and then configure your new organization.

Notes:

- The link in the email expires after 48 hours. If you do not click the link within that time, contact XClarity One support using the [Contact Us webpage](#) to resend the email.
- If you already purchased licenses and the organization was not automatically approved, contact your Lenovo sales representative to ensure that your Lenovo customer number matches the Lenovo customer number for our XClarity One organization.

Important: Organizations are associated with the email domain of the initial user (organization owner).

- Requests to create organizations from certain popular email domains will be denied, including gmail.com, yahoo.com, hotmail.com, aol.com, and msn.com.
- Users that you invite to your organization must use the same email domain as the organization owner, with the exception of service agents (see [Organizations for managed service providers](#)).

Updating organization properties

You can update the organization name, location, and Lenovo customer number by clicking the **Settings** tab on the left navigation and then clicking the **General** tab in the context menu.

Disabling or deleting an organization

When using XClarity One in the cloud, only Lenovo can disable or delete an organization. If you created organizations that you want to disable or delete, contact Lenovo Support for assistance.

When an organization is disabled:

- All information about the organization and resources is retained in XClarity One.
- Communication is blocked between the XClarity One and management hubs. Communication is not blocked between the management hubs and managed devices. The management hubs continue to monitor devices; however, management operations cannot be performed on the devices.
- Users can sign in to the portal but cannot have access to the disabled organization.

When an organization is deleted:

- All information about the organization and resources is deleted, except the audit event stating who removed the organization and when.
- Management hubs are disconnected, and information about the hub and its managed devices are deleted from the portal
- The users that are members of only this organization (and no other organizations) are removed.
- If licenses are assigned to the organization and there are no other organizations with the same customer number, the licenses are still available for use. If a new organization is created with the same customer number, the licenses are assigned automatically to that new organization.

If licenses are assigned to the organization and there are one or more other organizations with the same customer number, the licenses are moved to the oldest active organization. If there are no active organizations with the same customer number, licenses are moved to the oldest pending or requested organization. If none are pending or requested, licenses are assigned to the oldest disabled organization.

Cannot access an organization

If you cannot access an organization, your user account might be disabled, or the organization might be disabled.

- Contact your organization owner or user administrator.
- If they cannot determine the cause or correct the issue, contact Lenovo Support for assistance.

Organizations for managed service providers

If you are a business that provides IT solutions and services to other companies, you can change your organization to a *managed service-provider* (MSP) organization.

To become a managed service provide (MSP) in XClarity One, you must first purchase an **XClarity One – MSP enablement** license for each customer that you service and then contact XClarity One support using the [Contact Us webpage](#). For more information about purchasing licenses, see [Licenses](#).

MSP organizations can have users that are assigned the *service-agent* role. Service agents can be added to organizations for the companies that they serve. Service agent are the only users that are not required to be in the same email domain as the organization owner. Note that the service-agent role does not give users the ability to perform any actions. The service agent must be given additional roles based on the actions that they are allowed to perform within the company's organization.

If the MSP organization owner or user administrator removes the service-agent role from a user, that user is automatically blocked from all other organizations to which they had access.

Notes:

- Only Lenovo can add or remove the MSP from an organization. If Lenovo removes the MSP flag, or if a MSP organization is disabled, all service agents in that organization are automatically blocked from *all other* organizations to which they had access. In addition, if Lenovo removes the MSP flag, the service-agent role is disabled, but not removed, from all service-agent users in the MSP organization.
- If a service agent is locked or when the service-agent's MSP organization is locked, the service agent cannot be added to customer organizations. The service-agent user can join another organization in the same MSP domain, but not as a service agent.

Chapter 10. Management hubs

Management hubs are light-weight device managers that act as a secure bridge between the Lenovo XClarity One portal and your on-premises devices. The management hubs are the only devices that communicate directly with the XClarity One portal..



XClarity One: Management hubs

The management hubs are installed on premise in your data centers. They can be set up across multiple sites, where your devices are located.

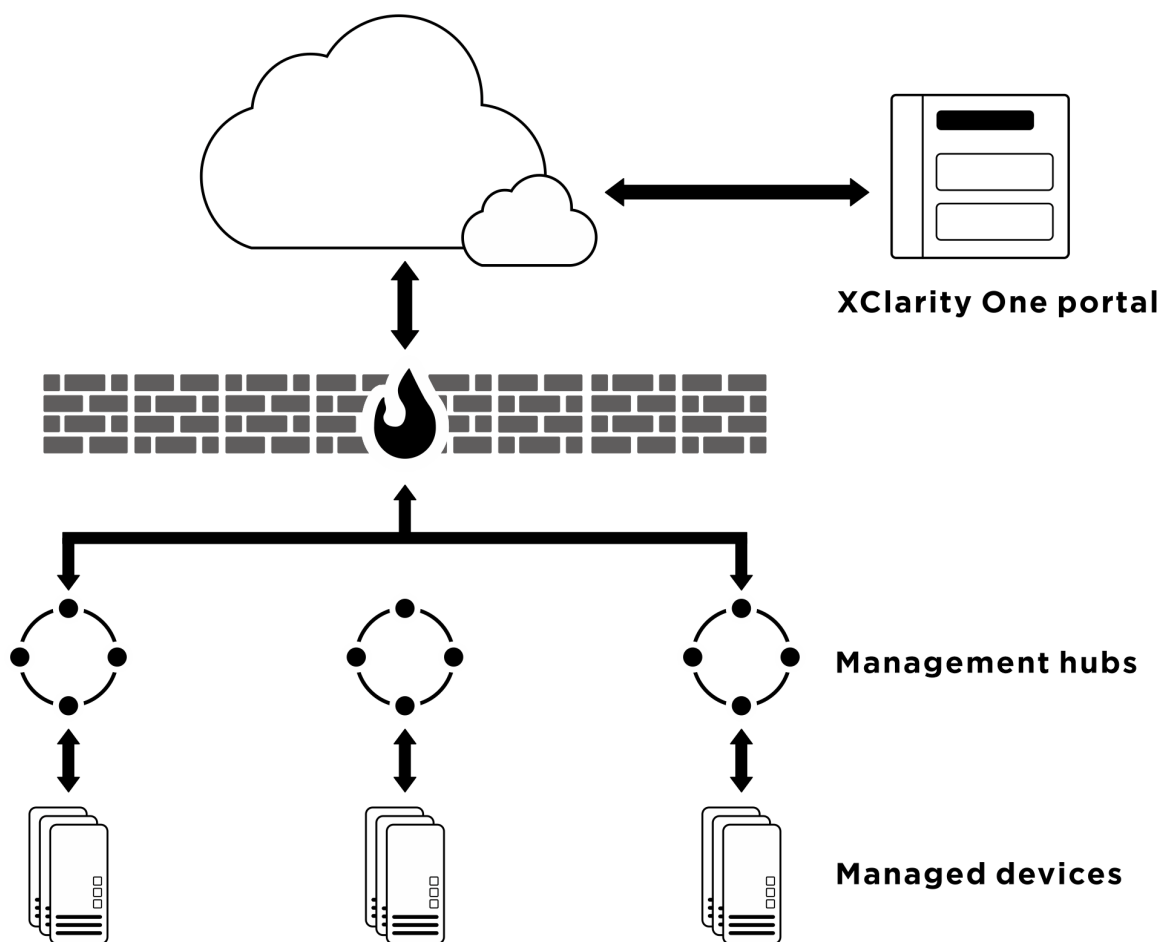
The following management hub is supported.

- **Lenovo XClarity Management Hub 2.0** manages, monitors, and provisions up to 5,000 devices, depending on the resources allocated to the virtual machine. For information about supported devices, see [Devices](#).

Management hub connection and management

Lenovo XClarity One monitors and manages devices through one or more light-weight device managers, called *management hubs*. Management hubs are installed on premise in your data centers. They can be set up across multiple sites, where your devices are located. The management hubs are the only devices that communicate directly with the XClarity One portal.

Management hubs are installed on premise in your data centers and then connected to XClarity One. They can be located across multiple sites where your devices are located.



Note: At least one management hub must be installed and connected to XClarity One for each organization.

Before you add (connect) a management hub to the XClarity One portal, ensure that:

- The management hub is installed and configured (see [Setting up a management hub](#) in the XClarity One online documentation).
- Ensure that the management hub is online and reachable on the network from XClarity One.
- Ensure that you have the correct privileges to add a hub. You must be a hub administrator.

Adding a management hub to XClarity One is a two-step process that involves installing a registration key from the hub to the XClarity One portal and installing a registration key from the XClarity One portal to the hub (see [Connecting the management hub to XClarity One](#) in the XClarity One online documentation).

When you add a management hub, XClarity One retrieves information about all devices that are managed by the management hub.

When you remove (disconnect) a management hub, XClarity One deletes information about the hub and its managed devices from its own data repository. However, the management hub itself retains information about its managed devices and continues to manage those devices.

When you disable a management hub, information about the hub and its managed devices is retrained; however, the management hub and its managed devices are not accessible to XClarity One.

If XClarity One loses connection to a management hub (for example, if there are network issues or if you use the XClarity Management Hub 2.0 web interface to disconnect the management hub from XClarity One), XClarity One is unable to retrieve the latest information from the management hub, including job progress,

until the connection between the management hub and XClarity One is reestablished (network issues are resolved or you reconnect the management hub).

Signing in to the management-hub web interface

You can launch the Lenovo XClarity Management Hub 2.0 web interface from any system that has network connectivity to the XClarity Management Hub 2.0 virtual machine.

Access the XClarity Management Hub 2.0 web interface by pointing your web browser to the XClarity Management Hub 2.0 IP address (for example, `https://192.0.2.10`).

The IP address that you use depends on how your environment is set up.

- If you specified a static IPv4 address during installation, use that IPv4 address to access XClarity Management Hub 2.0.
- If a DHCP server is set up in the same broadcast domain as the management hub, use the IPv4 address that is displayed in the virtual-machine console to access XClarity Management Hub 2.0.

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

Ensure that you are using one of the following supported web browsers.

- Chrome 115 or later
- Firefox ESR 102.12 or later
- Microsoft Edge 115 or later
- Safari 16.6 or later

User sessions

Each user can have up to five user sessions.

After 30 minutes of inactivity, you can continue to view data; however, you must log in again to perform other actions. The management hub automatically logs out user sessions after 24 hours, regardless of activity.

If five consecutive log-in attempts fail, you must wait at least 15 minutes before logging in again.

After changing your password, you must wait at least an hour to change it again.

Signing in

If you are signing in for the first time:

- For XClarity Management Hub 2.0 v1.0, enter the default username **USERID** and password **PASSWORD** (using a zero), and then immediately change the password.
- For XClarity Management Hub 2.0 v1.1 and later, you are prompted to create a new username and password.

XClarity Management Hub 2.0 supports multi-factor authentication using user credentials and a one-time passcode from an authenticator application. The authenticator application is set up on a mobile device and connected to XClarity Management Hub 2.0 to obtain a one-time passcode (OTP) that is needed each time you sign in. The following authenticator applications are supported.

- FreeOTP
- Google Authenticator
- Microsoft Authenticator

You can update your personal information, change your password, and manage your authentication applications by clicking **User settings** from the user-account drop-down menu in the upper-right corner.

It is recommended that you use strong passwords of 16 or more characters. By default, passwords must have **8 – 256** characters, including one or more uppercase and lowercase alphabetic characters, numbers, and special characters ; @ _ ! ' \$ & +. Consider the following recommendations when creating passwords.

- Do not use known passwords obtained from earlier breaches, leaks, or hacks.
- Do not use dictionary words.
- Do not use context-specific words, such as the name of a service, an email address, or derivatives thereof.
- Do not use more than two repetitive or sequential characters (for example, aaa or 123abc).
- Do not reuse any of the last five passwords.

Resetting your password

If the management hub has two or more users, and you forget your password, another user can reset your password for you from the **Users** page.

However, if you are the only user and you forget your password, you can reset your password through the virtual-machine console.

1. Restart the virtual machine.

At the end of the management-hub boot process, you can choose to reset the user password by entering **4** when prompted. The prompt is available for 150 seconds, until the login prompt is displayed. To proceed to the login prompt without delay, enter **x** at the prompt.

2. Enter **4** when prompted to reset your password.
3. Enter your username, email address, and new temporary password.
4. Choose whether to also reset the multi-factor authentication settings.

After your password is reset, it is highly recommended that you change your new password and multi-factor authentication (if applicable) from the **Users** page.

Management-hub health summary and details

You can view detailed information about a specific management hub, including things to do, overall health, hub details, and a list of managed and unmanaged devices.

Note: Only hub administrators can view the management hub details.

View detailed information for a specific management hub by clicking on the hub from the **Management hubs** page.

Health summary

The **Status** panel shows the overall health of the management hub. The **Managed Devices** panel shows the overall health of each device that is managed through that hub. Overall health is calculated based on the highest severity of all events that are associated with the device.

- **Healthy.** No critical or warning events.
- **Warning.** One or more warning events.
- **Critical.** One or more critical events, and possibly warning events.

Discovered and managed devices

You can view a list of all devices that are managed by the management hub from the **Managed Devices** panels.

The **Unmanaged Devices** panel lists devices that were discovered but not yet managed through the management hub. You can select specific devices and then click the **Add** icon (⊕) to bring those devices under management by the management hub.

Management-hub metrics and trends

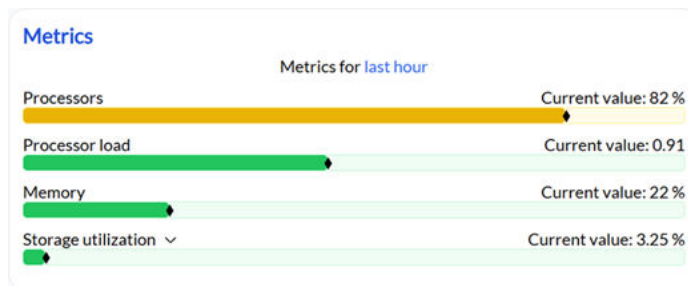
You can monitor usage metrics for the management hub from the main dashboard. Metrics are graphically displayed on the **Metrics** panel.

Metrics are available for the following resources.

- **Processors.** Processor usage, as a percentage
- **Processor load.** Processor load
- **Memory.** Memory usage, as a percentage
- **Storage usage.** Processor usage, as a percentage

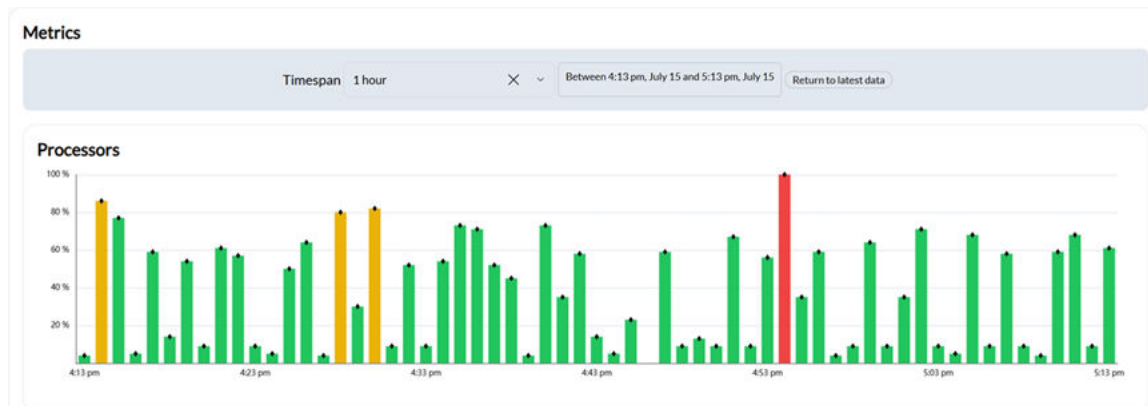
Current usage metrics

The **Metrics** panel shows the current usage (vivid color) and the amount available (pale color) for each component. Hover over the bar for each component to view more usage details.



Historical usage metrics

Click the **last hour** link in **Metrics** panel to display the **Metrics** page that has charts showing with usage metrics over the last hour for each device component. Hover over any bar in the chart to view more usage details. Click **Return to latest data** to refresh the charts with current data.



Function enablement

You can enable and disable certain management-hub specific functions by clicking **Functions** from the context menu on the **Security** view from the XClarity Management Hub 2.0 web interface.

Management hub functions

The following management-hub function is supported.

- **Hub power actions.** This function is used to power off and restart the management hub.

This function is enabled by default.

Device functions

Lenovo XClarity One leverages management hubs to perform management functions on managed devices. You can control whether to allow XClarity One and XClarity Management Hub 2.0 to perform management function on your devices. If all management functions are disabled, XClarity One only monitors your devices and is not permitted to make changes to your devices.

Notes:

- When you disable a function from the XClarity One portal, the function is also disabled on all management hubs in the organization.
- When you enable a function from the XClarity One portal, the function is enabled only in the portal. Be aware that the XClarity One portal settings might not match the setting on the management hubs. It is your responsibly to enable the function on each management hub that has managed devices that you want to access remotely.

The following device functions are supported.

- **Device power actions.** This function is used to power on, power off, and restart managed devices from the XClarity One portal.
This function is disabled by default.
- **Firmware updates.** This function is used to update and maintain appropriate firmware levels on managed devices from the XClarity One portal.

This function is disabled by default.

- **Device-settings updates.** This function is used to update and maintain appropriate device-settings on managed devices from the XClarity One portal.

This function is disabled by default.

- **Remote Server Access.** This function is used to launch the baseboard management-controller interface from the XClarity One cloud portal without having a direct connection between the web browser and the management controller. The connection does not require virtual private network (VPN) to the device. This feature allows seamless interaction with managed devices from any locations while upholding data security protocols. For more information, see [Remote sever access](#).

This function is disabled by default.

This function is not available when the management hub is connected to an XClarity One that is running as a local virtual machine.

- **Remote Server Console Access.** This function is used to launch the remote server console from the XClarity One portal. This feature allows you to remotely view and interact with the server console from any location while upholding data security protocols. This feature also allows you to mount a disk image (ISO or IMG file) as a virtual drive on the device. For more information, see [Remote sever access](#).

This function is disabled by default.

Management-hub power actions

You can immediately restart or power off the management hub directly from the management hub web interface.

From the management hub web interface ,click power actions that you want to perform from the context menu on the **Maintenance** view.

Management-hub security certificates

Lenovo XClarity Management Hub 2.0 uses SSL certificates to establish secure, trusted communications between the management hub and its managed devices, as well as communications with management hub by users or with different services. By default, XClarity Management Hub 2.0 and the XClarity One portal use XClarity One-generated certificates that are self-signed and issued by an internal certificate authority.

Attention: Managing security certificates requires 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](#).

The default server certificate, which is uniquely generated in every instance of XClarity Management Hub 2.0 provides sufficient security for many environments. You can choose to let XClarity Management Hub 2.0 manage certificates for you, or you can take a more active role by customizing and replacing the server certificates. XClarity Management Hub 2.0 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 authorities to sign a custom certificate that can then be uploaded to the management hub to be used as the 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 Management Hub 2.0 provides several services that accept incoming SSL/TLS connections. When a client, such as a web browser, connects to one of these services, the management hub 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 a management-hub server certificate is not included in the client's list, the client disconnects from the management hub to avoid exchanging any security-sensitive information with an untrusted source.

XClarity Management Hub 2.0 acts as a client when communicating with managed devices and external services. When this occurs, the managed device or external service provides its server certificate to be verified by the management hub. The management hub maintains a list of certificates that it trusts. If the *trusted certificate* that is provided by the managed device or external service is not listed, the management hub disconnects from the managed device or external service to avoid exchanging any security sensitive information with an untrusted source.

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 Management Hub 2.0 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 self-signed management hub 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 management-hub server certificate. It is automatically regenerated each time XClarity Management Hub 2.0 detects that its IP address, hostname or domain name 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 self-signed management hub 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), signing the CSR using an private or commercial root certificate authority, and then importing the full certificate chain into the management hub (see [Installing a trusted, externally-signed management hub 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 management hub server certificate into a web browser](#)).

Device certificate chains

XClarity Management Hub 2.0 acts as a client when communicating with managed devices. When this occurs, the managed device provides its server certificate to be verified by the management hub. The management hub maintains a list of certificates that it trusts. If the *trusted certificate* that is provided by the managed device is not listed, the management hub disconnects from the managed device to avoid exchanging any security sensitive information with an untrusted source.

You can manage servers using non-standard certificate configurations by importing custom certificate authorities (CAs) and intermediate CAs within the management hub to allow the management hub to trust the connection to those devices. The management hub validates the combination of the intermediate CAs and the root CA to ensure the chain of trust.

Notes:

- The intermediate CAs must be signed by the trusted root CA or other intermediate CA in the chain.
- You cannot upload intermediate CAs without the root CA because the root CA is needed to establish trust.

To add certificate chains to the truststore, click **Security** from the context menu on the **Truststore** view, and click the **Add** icon (+). Follow the steps in the wizard to complete the import.

To delete a certificate chain from the truststore, click **Security** from the context menu on the **Truststore** view, select the certificate, and click the **Delete** icon (III).

Regenerating the self-signed management hub server certificate

You can generate a new server certificate to replace the current self-signed Lenovo XClarity Management Hub 2.0 server certificate or to reinstate a management-hub-generated certificate if XClarity Management Hub 2.0 currently uses a customized externally-signed server certificate. The new self-signed server certificate is used by the management hub for HTTPS access.

Attention:

- If you regenerate the management-hub server certificate using a new root CA, XClarity Management Hub 2.0 loses its connection to the managed devices, and you must re-manage the devices. If you regenerate the management-hub server certificate without changing the root CA (for example, when the certificate is expired), there is no need to re-manage the devices.
- The self-signed certificate is not secure. You are advised to generate and install your own externally-signed certificate (see [Installing a trusted, externally-signed management hub server certificate](#)).
- You cannot change the subject alternative names when regenerating the self-signed server certificate.

Server-certificate validity period

The server certificate that is currently in use, whether self-signed or externally-signed, remains in use until a new server certificate is generated, signed, and installed. By default, the server certificate expires after 365 days. To customize the validity period, complete the following steps.

1. Click **Certificates** from the context menu on the **Security** view.

2. In the **Regenerate Self-signed Server Certificate** panel, change the number in the **Days** field..

Default self-signed server certificate

To regenerate a self-signed server certificate using default values, complete the following steps.

1. Click **Certificates** from the context menu on the **Security** view.
2. In the **Regenerate Self-signed Server Certificate** panel, click **Reset Certificate**.

Custom self-signed server certificate

To regenerate a self-signed server certificate using custom values, complete the following steps.

1. Click **Certificates** from the context menu on the **Security** view.
2. In the **Regenerate Self-signed Server Certificate** panel, provide values in each field, and then click **Regenerate Certificate**.
 - Organization is typically the legally incorporated name of a company that owns the certificate. Include suffixes, such as Ltd., Inc., or Corp (for example, ACME International Ltd.).
 - Organization unit is the division in the company that owns the certificate (for example, ABC Division).
 - Common name is typically the host name, 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.

Root certificate authority

You can regenerate the root certificate authority (CA) using the management hub IP address and FQDN settings. When you regenerate the root CA for the management hub, the HTTPS certificate for each device that is managed by the hub is also regenerated.

To regenerate the root CA, complete the following steps.

1. Click **Certificates** from the context menu on the **Security** view.
2. In the **Root certificate authority (CA)** panel, provide values in each field, and then click **Reset Root CA**.

You can download the root CA to your local system by clicking **Download root CA**.

Installing a trusted, externally-signed management hub 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.

Considerations

Attention:

- If you install an externally-signed server certificate using a new root CA, the management hub loses its connection to the managed devices, and you must re-manage the devices. If you install an externally-signed server certificate without changing the root CA (for example, when the certificate is expired), there is no need to re-manage the devices.
- If new devices are added after the CSR is generated and before the signed server certificate is imported, those devices must be restarted to receive the new server certificate.

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 for the management hub.

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 Management Hub 2.0, 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 management hub server certificate into a web browser](#)).

The web browser is refreshed automatically to accept the new certificate.

Installing a trusted, externally-signed server certificate

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

1. Create a certificate signing request and save the file to your local system.
 - a. Click **Certificates** from the context menu on the **Security** view.
 - b. In the **Generate Certificate Signing Request (CSR)** panel, provide values in each field, and then click **Generate CSR File**.
 - Organization is typically the legally incorporated name of the company that owns the certificate. Include suffixes, such as Ltd., Inc., or Corp (for example, ACME International Ltd.).
 - Organization unit is the division in the company that owns the certificate (for example, ABC Division).
 - Common name is typically 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.
 - You can customize the subject alternative names in the X.509 "subjectAltName" extension in the resulting CSR. If you provide one or more subject alternative names in the CSR, only the subject alternative names that you provided are stored in the CSR. You can provide subject alternative names for the following types. Ensure that the names that you specify are valid for the selected type. The specified subject alternative names are validated (based on the specified type) and added to the CSR only after you generate the CSR.
 - **DNS** (use the hostname or FQDN, for example, hostname.labs.company.com)
 - **IP address** (for example, 192.0.2.0)
 - **email** (for example, example@company.com)

If no subject alternative names are provided, the default names and type from the management hub are used.

- **IP Address.** Current management-hub IP address
- **DNS Name.** Management-hub hostname
- **DNS Name.** Management-hub FQDN, if the domain name is provided. Otherwise, this is empty.

Attention: The subject alternative names must include the hostname or fully-qualified domain name (FQDN), and IP address of the management hub, and the subject name be set to the hostname or FQDN of the management hub. Verify that these required fields are present and correct before beginning the CSR process to ensure that the resulting certificate is complete. Missing certificate data might result in connections that are not trusted when attempting to connect the management hub to Lenovo XClarity One.

Important:

- Before continuing, verify that the newly generated certificate contains the FQDN and IP address as part of the subject alternative names.
- Ensure that the newly generated certificate is configured to be used as both a *server certificate* and as a *client certificate*.

2. Provide the CSR to a trusted certificate authority (CA). The CA signs the CSR and returns a server certificate.

Attention: All subject alternative names that are stored in the CSR must be used for signing the CSR and generating the web certificate.

3. Import the externally-signed server certificate and the CA certificate to XClarity Management Hub 2.0 to replace the current server certificate.
 - a. In the **Certificate signing request (CSR)** panel, click **Import certificate** to display the **Import certificate** dialog.
 - b. Insert the externally-signed server certificate, in PEM format. You must provide the entire certificate chain, beginning with the server certificate and ending in the root CA certificate.
 - c. Click **Import** to store the server certificate in the management-hub trust store.

Attention: The subject alternative names that are stored in the CSR on the management hub must exactly match the subject alternative names stored in the server certificate being imported. If there is a mismatch (for example, if the IP address from the CSR/signed certificate is not the same with the one from the management hub), the importing and installing the server certificate will succeed, but might result in connections that are not trusted (such being unable to access the user interface).

Importing the management hub 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 to avoid security warning messages from your web browser when you access Lenovo XClarity Management Hub 2.0.

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

1. Export the management-hub server certificate.
 - a. From the XClarity Management Hub 2.0 portal, click **Certificates** from the context menu on the **Security** view.
 - b. In the **Self-signed server certificate** panel, and then click **Download Certificate**.
2. Import the management-hub server certificate into the list of trusted root authority certificates for your browser.
 - **Chrome**
 - a. From your Chrome browser, click the icon with three vertical dots in the upper-right corner of the window, and then, click **Settings** to open the **Settings** page.
 - b. Click **Privacy and Security**, and then click **Security** to display the **Security** page.
 - c. Scroll to the **Advanced** section, and then click **Manage device certificates**.
 - d. Click **Import**, and click **Next**.
 - e. Select the certificate file that you previous exported, and click **Next**.
 - f. Choose where to store the certificate, and click **Next**.
 - g. Click **Finish**.
 - h. Close and reopen the Chrome browser, and then open management-hub user interface.
 - **Firefox**
 - a. Open the browser, and click **Tools → Settings**, and then click **Privacy & Security**.
 - b. Scroll down to the **Security** section.
 - c. Click **View certificates** to display the **Certificate Manager** dialog.
 - d. Click the **Your Certificates** tab.
 - e. Click **Import**, and browse to the location where the certificate was downloaded.
 - f. Select the certificate, and click **Open**.
 - g. Close the **Certificate Manager** dialog.

Management-hub service data

You can manually collect service data for Lenovo XClarity Management Hub 2.0 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.

Online service-data collection

To collect and save management-hub service data to the local system, click **Service data** from the context menu on the **Administration** view from the XClarity Management Hub 2.0 web interface.

Important: Ensure that web browser does not block pop-ups for the management-hub website when downloading service data.

Offline service-data collection

If XClarity Management Hub 2.0 becomes unresponsive and cannot be recovered, you can collect service data for that management-hub from the XClarity Management Hub 2.0 Service Support Center portal by clicking **Offline Service File Collection**.

You can access the XClarity Management Hub 2.0 Service Support Center portal by pointing your web browser to the XClarity Management Hub 2.0 IP address and port 8443, for example:
`https://192.0.2.10:8443`

Notes:

- If you specified a static IPv4 address during installation, use that IPv4 address to access the XClarity Management Hub 2.0 Service Support Center portal.
- If a DHCP server is set up in the same broadcast domain as the management hub, use the IPv4 address that is displayed in the virtual-machine console to access the XClarity Management Hub 2.0 Service Support Center portal.
- Access to the portal is through a secure connection. Ensure that you use https.

Specify the service-recovery password in the **Authentication Key** field, and select **Password** as the **Authentication type**.

Note: If six consecutive log-in attempts fail, within a 15 minute period, you must wait at least 1 hour before signing in again.

Service data is compressed into a single .tar.gz file to your local system. You can choose to collect all service files and management server logs or just the logs.

- **All Service Data.** Includes service logs, syslogs, and information about the virtual machine, operating system, network, processes, containers, and databases.
- **Logs Only.** Includes service logs, syslogs, and information about the virtual machine.

Note: Only the latest archive file is stored in the management hub repository. The file is deleted when the next collection request is made.

Service-recovery password

The service-recovery password and the password-expiration interval were set during initial configuration. This service-recovery password is needed to collect service data on an unresponsive management hub. By default, the password must be reset every 90 days.

Important: If six consecutive sign-in attempts fail within a 15-minute period or if consecutive sign-in attempts occur too quickly (within 1 second), your user account is locked for 60 minutes.

If you attempt to collect service data for an unresponsive management hub and the service-recovery password is expired, you are redirected to the **Reset Service Recovery Password** dialog to change the password.

You can also change the password and expiration interval at any time from the **Service Support Recovery Password** card by clicking **Service data** from the context menu on the **Administration** view from the XClarity Management Hub 2.0 web interface.

The password must have **16 – 256** characters, including one or more uppercase and lowercase alphabetic characters, numbers, and special characters ; @ _ ! ' \$ & +

Attention: Ensure that you record the password for later use. You cannot recover an unresponsive management hub without using this password.

Management-hub updates

It is important to keep Lenovo XClarity Management Hub 2.0 up to date with the latest release.

Before you begin

Lenovo XClarity Management Hub 2.0 v1.1 and later supports automated updates. You must manually update from v1.0 to v1.1 to get this feature by following the steps in the “When the hub is not connected to a portal” section below.

You can update Lenovo XClarity Management Hub 2.0 to only the next ordinal release, for example from v1.0 to v1.1 or v1.1 to v1.2. You cannot skip releases when updating the management hub.

During the update process, all users are signed out of the management hub when the hub restarts. Wait several minutes until the restart completes. Then, clear the web browser cache and refresh the web browser before signing in again.

Note: If you encounter a 413 error (entity too large) when you attempt to upload the management-hub update package, increase the number of processors on the VM. For example, if your VM has 2 processors, increase the VM to 4 processors.

Procedure

To update the management hub, complete one of the following steps.

- **When the hub is connected to XClarity One**

XClarity Management Hub 2.0 v1.1 and later makes it easy to keep the management hub software up to date by retrieving the latest updates packages as soon as a new update is released and then automatically installing updates at the preferred time.

By default, updates are installed at midnight GMT0. You can configure installation time from the XClarity Management Hub 2.0 web interface by clicking click **Updates** from the context menu on the **Maintenance** view.

You can delay installing the management-hub update up to 14 days after the latest applicable update. After 14 days, the updates are installed immediately. From the **Update configuration** dialog, select **Schedule update**, and specify the date and time.

An event is raised an hour before the installation process starts.

After the update completes, clear the web browser cache, and refresh the web browser.

- **When the hub is not connected a portal**

When the management hub is not connected to a portal, you can manually update the management hub, by completing the following steps.

1. Download the management-hub update package from the [XClarity Management Hub 2.0 downloads webpage](#) to a workstation that has a network connection to the XClarity Management Hub 2.0 host server.

The update package is a .tar.gz or .tgz archive. This archive file contains the four required update files: update image (.tgz or .tar.gz), metadata (.xml), change log (.chg), and readme (.txt).

2. From the XClarity Management Hub 2.0 web interface, click **Updates** from the context menu on the **Maintenance** view.
3. Import the update package by clicking **Import an update** (if there are no updates in the repository) or the **Import** icon (📁) to display the Import an update dialog
4. Select the update package, and click **Import**.

Importing the update files might take a while. When the import is complete, the update package is listed in the table on the **Management hub update** panel.

5. Select the update package that you want to apply, and click the **Install Update** icon (✅).
6. Wait for the update to complete. The update process might take a while.
7. Clear the web browser cache, and refresh the web browser.

When completed, the **Status** column changes to **Installed**.

Uninstalling a management hub

Complete these steps to uninstall a Lenovo XClarity Management Hub 2.0 virtual appliance.

Procedure

To uninstall a management-hub virtual appliance, complete the following steps.

Step 1. Unmanage all devices that are currently managed by the management hub from the XClarity One portal.

Step 2. Uninstall the management hub, depending on the operating system.

- **ESXi using VMware vCenter**

1. Connect to the host through VMware vCenter.
2. Right click the Lenovo XClarity Management Hub 2.0 virtual machine in the **VMware Host** Client inventory, and select **Guest OS** from the pop-up menu.
3. Click **Shut down**.
4. Right click the virtual machine in the **VMware Host** Client inventory, and select **Guest OS** from the pop-up menu.
5. Click **Delete**.

- **ESXi using VMware vSphere**

1. Connect to the host through the VMware vSphere Client.
2. Right-click the Lenovo XClarity Management Hub 2.0 virtual machine, and click **Power** → **Power Off**.
3. Right-click the virtual machine again, and click **Delete from Disk**.

- **Hyper-V**

1. From the **Server Manager** dashboard, click **Hyper-V**.
2. Right-click the server, and click **Hyper-V Manager**.
3. Right-click the Lenovo XClarity Management Hub 2.0 virtual machine, and click **Shut down**.
4. Right-click the virtual machine again, and click **Delete**.

- **KVM**

1. Connect to the host using the Virtual Machine Manager.
2. Right-click the Lenovo XClarity Management Hub 2.0 virtual machine, and click **Shut Down** → **Force off**.
3. Right-click the Lenovo XClarity Management Hub 2.0 virtual machine again, and click **Delete**. The Delete confirmation dialog box is displayed.
4. Select all check boxes, and click **Delete**.

Chapter 11. Devices

Lenovo XClarity One supports a wide range of devices. You can find a complete list of supported devices and options (such as I/O, DIMM, and storage adapters), minimum required firmware levels, and limitations from the following Lenovo XClarity Support webpages.

- [Lenovo XClarity Support webpage](#), then click the **Compatibility** tab

For general information about hardware configurations and options for a specific device, see the [Lenovo Server Proven webpage](#).



[XClarity One: Device management](#)

Device discovery and management

Lenovo XClarity One can manage supported devices that were discovered by XClarity Management Hub 2.0.

Discovering devices

Devices must be discovered by a management hub before they can be managed by XClarity One. Devices can be discovered in the following ways.

- **Automatically discover devices**

The management hubs automatically discover supported devices in your environment every five minutes by probing for manageable devices that are in *the same IP subnet* as the management hub using the SSDP protocol.

Important: Ensure that SSDP is enabled on the baseboard management controller on each device as well as routers in your environment. For ThinkSystem devices, click **BMC Configuration → Network** from the Lenovo XClarity Controller web interface.

- **Use a DNS service to discover devices**

You can use a DNS service to discover ThinkSystem and ThinkEdge servers by manually adding a service record (SRV record) to your domain name server (DNS), and then enabling DNS discovery on the Lenovo XClarity Controller (click **BMC Configuration → Network** from the XClarity Controller web interface, click the **DNS and DDNS** tab, select **Use DNS to discover**, and then select the resource manager from the **XClarity Manager** list).

Ensure that the service record includes the following information for ADS-based DNS.

Property	Value
Domain	Your root domain
Service	_lxca
Protocol	_tcp
Priority	0
Weight	0
Port number	443
Host offering this service	Fully-qualified domain name (not the IP address)

- **Manually discover devices**

From the XClarity One portal, you can manually discover supported devices *in other subnets* using specific IPv4 addresses, full-qualified domain names, range of IP addresses, or by probing for manageable devices on specific IP subnets.

To discover devices, click the **Add** icon (+) from the **Unmanaged Devices** panel, which you can view by clicking **Unmanaged Devices** tab in the context menu from the **Device management** view. Follow the steps in the wizard to identify the devices that you want to discover and the management hub that you want to use for the discovery.

Managing devices

The discovered devices are listed on the **Unmanaged Devices** panel in the XClarity One portal. To manage discovered devices, select the target devices, click the **Add** icon (+), and follow the steps in the wizard.

If a device is discovered by more than one management hub, the device is listed on the **Unmanaged Devices** page for each management hub that discovered it, ordered based on the discovery timestamp. When managing a device, you can choose the device that was discovered by the management hub you want to use for management. A device can be managed by XClarity One through *only one* management hub.

Before managing devices:

- Ensure that the devices that you want to manage are supported by the management hub. You can find a complete list of supported devices, minimum required firmware levels, and limitations from the [XClarity Management Hub 2.0 Support for Servers webpage](#).
- Ensure that the latest firmware is installed on each device that you want to manage.
- Ensure that all required switch and firewall ports are open before you attempt to manage devices.

During the management process, the portal:

- Creates a management user account named **XC1_MGR_{last 8 chars of hub UUID}** with an encrypted password on the baseboard management controller for the device. The password is rotated automatically on a regular basis.

After the management process is complete, the management hub uses this **XC1_MGR_*** user account to connect to the device for management purposes. The credentials that you provided during the management process are no longer used by the management hub.

- Adds subscriptions to the device for sending event and metric data to the management hub.
- Collects inventory and vital product data.
- Collects metric data, including memory predictive failure analysis (MPFA).
- Saves sensitive information in the vault.
- Regenerates the HTTPS certificate on the server if the current HTTPS certificate is either self-signed or signed by another management hub. The HTTPS certificate is valid for 90 days. The management hub regenerates the HTTPS certificate on the server again 45 days before it expires.

Note: If the HTTPS certificate is signed by a third party, the management hub sends an event and alert to XClarity One seven days before the expiration date.

Attention: If you try to manage a device that is already managed through a management hub, XClarity One unmanages the device from the current management hub without the management hub acknowledgement and then manages the device again through the new management hub. After this process, the device remains as managed through the first management hub, but the device no longer sends data to it. Be aware that you must manually remove the devices from the first management hub through the connected portal.

After the devices are managed, the management hub polls each managed device every 24 hours to collect and send inventory data to XClarity One.

- If XClarity One loses communication with a device (for example, due to power loss or network failure) 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 One to poll the device for inventory or manually refresh inventory on the device.
- If the IP address of a managed device changes, you must unmanage the device, and then manage it again.
- You can use other management software (such as VMware vRealize Operations Manager) in tandem with XClarity One to *monitor* but *not manage* devices that XClarity One manages.

Unmanaging devices

You can unmanage devices in your organization. Click the **Managed devices** panel title from the **Device management** view, select the devices that you no longer want to managed, and click the **Unmanage** icon (



During the management process:

- The management user account (**XC1_MGR_***), and event and metric subscriptions are removed from the device.
- Sensitive information in the vault, inventory, vital product data, event forwarders between the device and the management hub, and events and alerts that were raised by the device are discarded on the management hub.
- Events there were raised for the device by the management hub are kept on the management hub.

Device considerations

ThinkSystem servers

Some ThinkSystem servers support two XCC IP addresses. If two XCC IP addresses are present:

- Ensure that each XCC IP address is configured on separate subnets.
- The management hub can use only one XCC IP address to manage a server. If the management hub discovers two XCC IP addresses for the same server, only the IP address with the smaller number is listed in the discovered devices table.
- The IP address that you use to manage the server becomes the *management IP address*. If there is a connectivity issue with the IP address, the management hub *does not failover* to use the second XCC IP address.

ThinkSystem V4 servers

Ensure that the management-controller date and time is synchronized with the NTP servers that are used by the management hub. From the XCC user interface, click the **Clock** icon on the upper right corner to configure NTP settings.

Ensure that the LDAP setting on the XCC is set to **LocalOnly** before attempting to manage the devices. For more information, see [Cannot manage a device](#) in the XClarity One online documentation.

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 efishell at least once so that the management hub 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.

Device health summaries

You can view a summary of the current health of all devices in your organization by clicking **Overview** in the context menu from the **Device management** view. By default, only the overall health is displayed. Click the **Managed devices** title to show additional summaries.



XClarity One: Device summary

Each summary includes a circular graph and statistics about the health of all managed devices. You can hover over each colored bar in the graph to see the total number of devices in that state. You can also click on the statistics to open the Devices page with a list of all devices in that state.

Overall health

A summary of the overall health of all managed devices, calculated based on the highest severity of all events that are associated with each device, is displayed graphically in the **Managed devices** panel by default.

- **Healthy.** Devices have no critical or warning events.
- **Warning.** Devices have one or more warning events.
- **Critical.** Devices have one or more critical events, and possibly warning events.

Click the **Managed devices** title to show the **Managed Devices** page with a list of all devices. The **Status** column identifies the overall health of each device. This column can contain multiple icons based on current conditions. If a device is in an unhealthy state, use the alerts log to help identify and resolve the issues (see [Alerts and events](#)).

A device is considered healthy when it is powered on, online, and has no warning or critical events. The following icons are displayed when the device is unhealthy.

- Power status identifies whether the device is powered on or off.
 - **Off**
- Connectivity status identifies the connection status between the device and the Lenovo XClarity One portal.
 - **Offline.** The portal cannot connect to the device.
 - **Partial**
 - **Pending**
- Overall health status identifies the highest severity of all events and alerts for the device.
 - **Warning.** Devices have one or more warning events, but no critical events.
 - **Critical.** Devices have one or more critical events, and possibly warning events

Vulnerabilities

A summary of devices that have common vulnerabilities and exposures (CVEs), by severity, is displayed graphically in the **Managed devices** panel by clicking the panel title and then clicking **Vulnerabilities**.

- **Critical.** Devices that have critical and possibly high, medium, and low vulnerabilities.
- **High.** Devices that have high vulnerabilities and possibly medium and low vulnerabilities.
- **Medium.** Devices that have medium and possibly low vulnerabilities.
- **Low.** Devices that have low vulnerabilities.
- **None.** Devices that have no vulnerabilities.

Management functions

Lenovo XClarity One leverages management hubs to perform management functions on managed devices. You can control whether to allow XClarity One and XClarity Management Hub 2.0 to perform management

function on your devices. If all management functions are disabled, XClarity One only monitors your devices and is not permitted to make changes to your devices.

You can enable and disable these functions on a specific management hub by clicking **Functions** from the context menu on the **Security** view from the XClarity Management Hub 2.0 web interface.

Organization owners can enable or disable these functions in XClarity One by clicking **Functions** from the context menu on the **Settings** view from the XClarity One web interface.

- When you disable a function from the XClarity One portal, the function is disabled on the portal and on all management hubs in the organization.
- When you enable a function from the XClarity One portal, the function is enabled only in the portal. Be aware that the XClarity One portal settings might not match the setting on the management hubs. It is your responsibility to enable the function on each management hub that has managed devices that you want to access remotely.

The following device-management functions are supported.

- **Device power actions.** This function is used to power on, power off, and restart managed devices through the portal.

This function is disabled by default.

- **Firmware updates.** This function is used to update and maintain appropriate firmware levels on managed devices from the portal.

Note: When this option is disabled, firmware cannot be pushed to or updated on devices managed by the management hubs. You can continue to use XClarity One manage the firmware repository, create templates with firmware rules and assign to devices, and monitor devices for compliance. For more information, see [Firmware](#).

This function is disabled by default.

- **Device-settings updates.** This function is used to update and maintain appropriate device-settings on managed devices from the portal.

Note: When this option is disabled, device settings cannot be updated on devices managed by the management hubs. You can continue to use XClarity One to manage the device-settings repository, create templates with device-settings configurations and assign to devices, and monitor devices for compliance. For more information, see [Device settings](#).

This function is disabled by default.

- **Remote Server Access.** When using XClarity One in the cloud, this function is used to launch the baseboard management-controller interface from the portal without having a direct connection between the web browser and the management controller. The connection does not require virtual private network (VPN) to the device. This feature allows seamless interaction with managed devices from any locations while upholding data security protocols. For more information, see [Remote sever access](#).

This function is disabled by default.

This function is not available when running XClarity One as a local virtual machine.

- **Remote Server Console Access.** This function is used to launch the remote server console from the portal. This feature allows you to remotely view and interact with the server console from any location while upholding data security protocols. This feature also allows you to mount a disk image (ISO or IMG file) as a virtual drive on the device. For more information, see [Remote sever access](#).

This function is disabled by default.

Usage metrics and trends

You can monitor usage metrics for a specific device by clicking the **Managed devices** panel title from the **Device management** view, and then click the name of the device in the table to display the device details page. Usage metrics are graphically displayed on the **Metrics** panel.

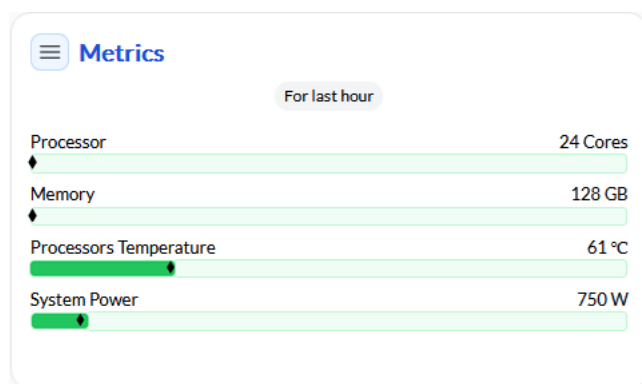
You can customize the panel to show data for metrics that interest you the most and the time period by clicking the **Settings** icon (☰) next to the panel title.

- **Memory.** (default) Memory usage, as a percentage
- **Memory Power.** Power consumption, in Watts, by all memory modules
- **Processors.** (default) Processor usage, as a percentage
- **Processor Power.** Power consumption, in Watts, by all processors
- **Processor Temperature.** (default) Temperature, in Celsius, for all processors
- **System Power.** (default) Power consumption, in Watts, by the device

Current usage metrics

The **Metrics** panel shows the maximum (pale color), highest usage (vivid color), and average usage (black diamond) for each component during the last hour.

Hover over the bar for each component to view more usage details.



The bar color indicates whether the usage exceeds the thresholds.

- **Green.** The actual usage is less than the warning threshold. The default threshold is 80% of the available amount.
- **Amber.** The actual usage is between the warning and critical threshold.
- **Red.** The actual usage is greater than the critical threshold. The default threshold is 90% of the available amount.

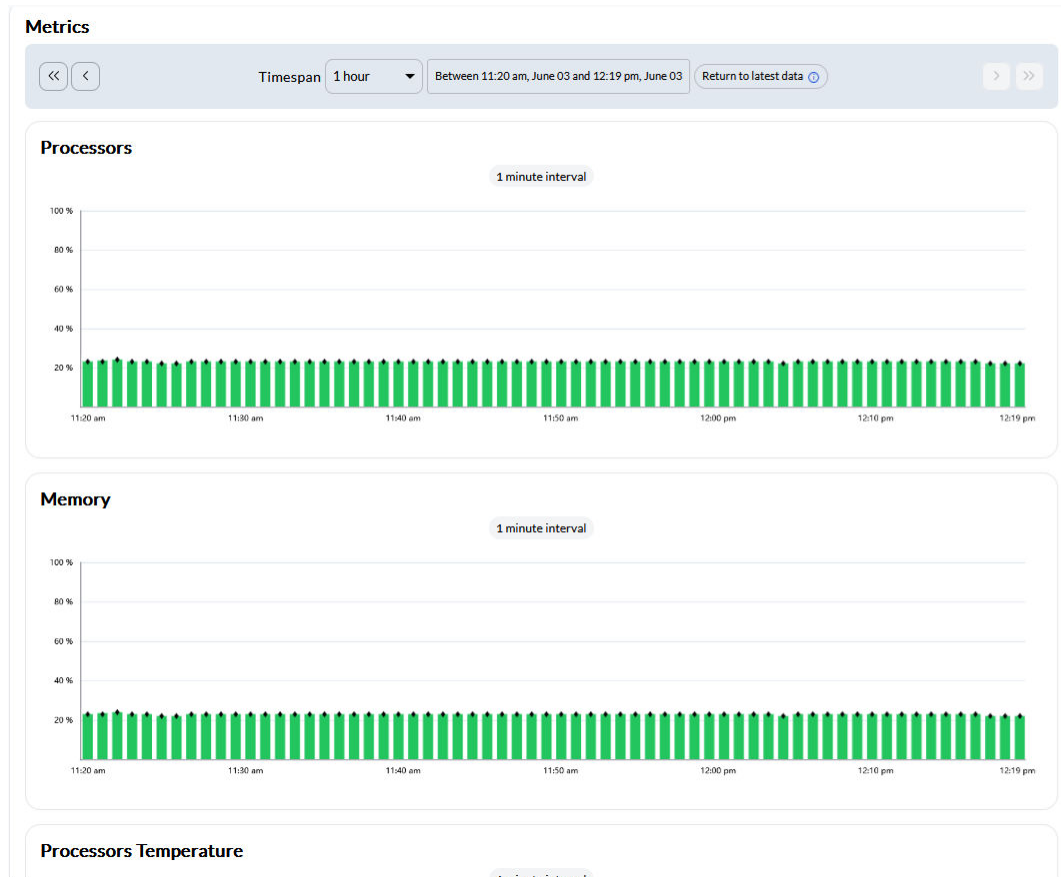
Usage trends over time

Data for each metric is kept for the last 90 days.

You can see the maximum usage trends over time by clicking the **Metrics** panel title to display the **Metrics** page. This page shows minimum, maximum, and average (black diamond) usage for each component over time. The color (green, amber, or red) indicates whether the maximum usage exceeds the thresholds.

Usage during the last minute is displayed by default. You can change the time span to show usage during the last hour, 24 hours, 30 days, or 90 days. You can also scroll forwards and backwards in time, based on the selected period, using the scroll icons.

Data is aggregated and assigned to the next unit of time. For example, hourly data from 10:00 – 10:59 is aggregated and assigned to 11:00, and daily data from May 2 24:00 – 23:59 is aggregated and assigned to May 3.



Usage-metric thresholds

Thresholds for these usage metrics are enabled by default. When enabled, an alert is raised when a component meets or exceeds its warning or critical threshold for the alert duration. The *alert duration* is the number of minutes during a specific period that the threshold value must be met or exceeded. For example, if processor usage has a warning threshold of 80% and alert duration of 4 of 10 minutes, then an alert is raised when the processor usage exceeds 80% for 4 or more minutes within a 10-minute period.

The minimum interval is 2 minutes within a 5-minute period.

You can set warning and critical usage thresholds and the alert duration for the certain components by clicking the **Alert rules** tab on context menu from the **Settings** view and then clicking the row for the component that you want to change.

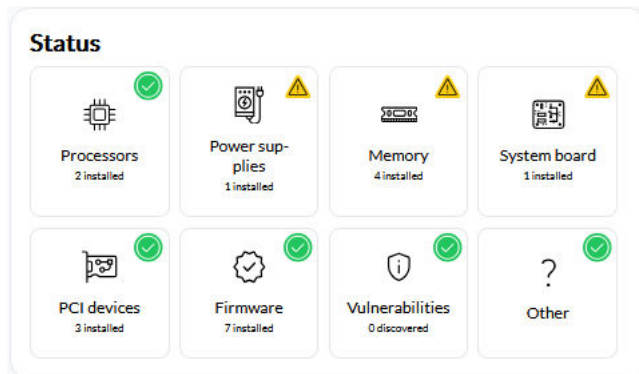
Device details

You can view detailed information about a specific device by clicking the **Managed devices** panel title from the **Device management** view, and then click the name of the device in the table to display the device details page. The device details page includes device-specific todos, component status, usage metrics, system information, and actions that you can take on the device. From this page, you can drill down to see jobs, events and alerts, firmware, and hardware inventory.

Component status

The **Status** panel shows the health of each component in the device.

- **Hardware components.** Based on the highest severity of all events that are associated with each component, such as processors, memory, fans, and PCI devices.
- **Firmware.** Based on age and number of vulnerabilities.
- **Vulnerabilities.** Based on whether the component firmware has warning or critical vulnerabilities.
- **Other.** Based on the highest severity of all events of other categories, such as warranty.



Usage metrics and trends

You can monitor usage metrics for a specific device from the device details page. Usage metric data is graphically displayed on the **Usage** panel. For more information, see [Usage metrics and trends](#).

Alerts and events

You can monitor all alerts and events for a specific device by clicking **Monitors** in the context menu on the device-details page. For more information about events and alerts, see [Alerts and events](#).

Vulnerabilities

You can monitor all vulnerabilities for a specific device by clicking **Monitors** in the context menu on the device-details page. For more information about events and alerts, see [Vulnerabilities](#).

Jobs

You can monitor all jobs for a specific device by clicking **Monitors** in the context menu on the device-details page. For more information about jobs, see [Jobs](#).

Service tickets

You can monitor all service tickets for a specific device by clicking **Monitors** in the context menu on the device-details page. For more information about service tickets, see [Service tickets](#).

Hardware inventory

You can view a list of hardware components (such as processors, memory, drives, power supplies, fans, add-in and onboard cards, and system board) that is in a specific device by clicking **Hardware inventory** in the context menu on the device-details page.



[XClarity One: Device inventory](#)

Firmware

You can view a list of firmware that is installed on a specific device by clicking **Firmware** in the context menu on the device-details page. For more information about service tickets, see [Firmware](#).

Collections

A *collection* is a static group of devices that can be monitored and together. A device can belong to one or more collections. Each collection can have up to 400 devices.

You can add collections to the organization and to monitor the overall health of all devices in each collection. You can click the collection card title to list all devices in the collection and add or remove devices from the collection.

Usage metrics and trends

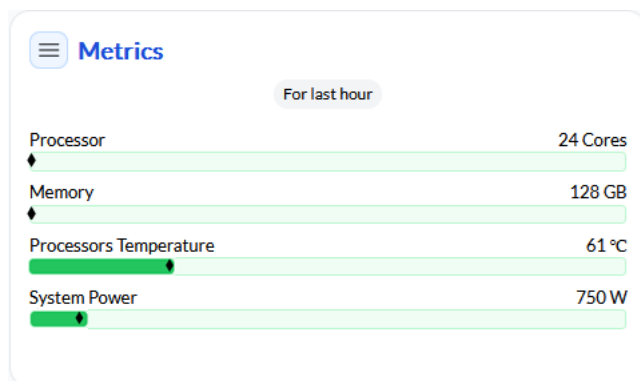
You can monitor usage metrics for all devices in a specific collection from the Usage panel by clicking the **Collections** panel title from the **Device management** view.

You can customize the panel to show data for metrics that interest you the most and the time period by clicking the **Settings** icon (☰) next to the panel title.

- **Memory.** (default) Memory usage, as a percentage
- **Memory Power.** Power consumption, in Watts, by all memory modules
- **Processors.** (default) Processor usage, as a percentage
- **Processor Power.** Power consumption, in Watts, by all processors
- **Processor Temperature.** (default) Temperature, in Celsius, for all processors
- **System Power.** (default) Power consumption, in Watts, by the device

The **Metrics** panel shows the maximum (pale color), highest usage (vivid color), and average usage (black diamond) for each component during the last hour.

Hover over the bar for each component to view more usage details.



The bar color indicates whether the usage exceeds the thresholds.

- **Green.** The actual usage is less than the warning threshold. The default threshold is 80% of the available amount.
- **Amber.** The actual usage is between the warning and critical threshold.
- **Red.** The actual usage is greater than the critical threshold. The default threshold is 90% of the available amount.

You can see the maximum usage trends over time by clicking the **Metrics** panel title to display the **Metrics** page. This page shows minimum, maximum, and average (black diamond) usage for each component over time. The color (green, amber, or red) indicates whether the maximum usage exceeds the thresholds.

Call Home contacts

When Call Home is configured and a serviceable event is triggered that automatically creates a service ticket, Lenovo Support might need to reach out to someone regarding the event. The primary or secondary contact that is configured for Call Home is contacted by default. However, you can choose to assign a different Call Home contact to all devices in a specific collection.

If a contact is assigned to a collection, and you add more devices to that collection, the preferred contact is also assigned to the new devices.

If you assign a contact to a collection, and some devices in that collection are also in another collection to which a contact was assigned, you can choose whether to change the assignment to the new contact or to keep the existing contact.

You can change the assigned contact for a specific device from the **Actions** panel on **Device** page by clicking **Service** → **Preferred contact**. You can choose from a list of contacts that were assigned to the collections in which the device is a member.

If you delete a collection that has an assigned contact, the preferred contact for each device in the collection resets to the default Call Home contact.

Remote sever access

A device administrator can remotely connect a specific managed device through the Lenovo XClarity One portal, allowing seamless interaction with management controller from any locations while upholding data security protocols.

Note: You can open a remote-server connection to a single device at a time from the same web browser. To open a connection to another device at the same time, use a different web browser.

Remote access to a management controller

You can launch the management-controller web interface for a specific device from the device details page. Click the **Managed devices** panel title from the **Device management** view, and then click the name of the device in the table to display the device details page. Then, click the **Remote** card on the **Actions** panel. You can connect to the management-controller web interface in the following ways.

- **Connect directly**

You can remotely access a management controller through a direct connection through your local network or virtual private network (VPN).

You must manually sign-in to the web interface using your management-controller credentials. Single sign-on is not supported.

- **Connect through the portal**

When using XClarity One in the cloud you can also remotely access a management controller without having a VPN connection to your datacenter or edge where your devices are located by using the portal connection. Traffic goes from the web browser to the portal, to the management hub, and then to the management controller.

You must manually sign-in to the web interface using your management-controller credentials. Single sign-on is not supported.

This function is disabled by default. To use this function, the organization owner must enable it in the XClarity One portal, and the hub administrator must enable it in the management hub web interface (see [Management functions](#)).

Attention: To use this function, you must purchase and install **XCC Platinum** or **XCC Premium** licenses on your managed devices.

This function is not available when running XClarity One as a virtual machine.

Remote access to a server console

You can remotely view and interact with the server console for a specific managed device and to mount a disk image (ISO or IMG file) as a virtual drive on the device. To access the server console, click the **Managed devices** panel title from the **Device management** view, and then click the name of the device in the table to display the device details page. Then, click the **Remote** card on the **Actions** panel.

For more information about using the remote console, see your Lenovo XClarity Controller online documentation.

Attention: Review these requirements for using the remote console feature.

- An XClarity Controller Platinum license is required on your managed devices to use the remote console function.
- The device must be in the Online state.
- 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.
 - You cannot power on or power off a server from a remote-control session.






Power operations

You can use Lenovo XClarity One to perform power operations on your managed devices.

Attention: By default, performing powering operations on managed devices is disabled. You must enable it from the XClarity One portal and from the management hub that manages that target devices. For more information, see [Management functions](#).

You can determine the current power status of your devices from the **Managed devices** panel title from the **Device management** view. From this panel, you can also perform a soft power off or power on by clicking the Power icon (⏻).

You can also perform the following power operations on a specific device. From the **Managed devices** panel, click the name of the device in the table to display the device details page. Then, click the **Power** card on the **Actions** panel, and select the power operation that you want to perform.

-  **Power On** powers on the device.
-  **Soft power off** shuts down the operating system (if applicable) and then powers off the device.
-  **Hard power off** powers off the device immediately.
-  **Soft restart** shuts down the operating system (if applicable) and then restarts the device.
-  **Hard restart** restarts the device immediately.
- **Restart system setup** restarts the device to BIOS/UEFI (F1) Setup.
- **Restart management controller** restarts the baseboard management controller

Device configuration

You can use Lenovo XClarity One to quickly setup and maintain your device configurations by deploying firmware and device settings to your managed devices using *templates*. XClarity One uses the templates that

are assigned to each managed device to ensure that those devices maintain a consistent configuration. When devices are out of compliance, their health status changes to Critical. You can use the deployment templates to bring the devices back into compliance.

Important: You must have device-administrator privileges to deploying firmware and device settings on target devices.

Firmware

You can use Lenovo XClarity One to maintain firmware on your managed devices. You can use the health summaries to identify the firmware health of your devices, view the firmware status to know what firmware versions are available for each device, and update the desired firmware version on target devices.

Available firmware in XClarity One

Lenovo ensures that the latest firmware versions are available in XClarity One in the cloud. You can view the list of available firmware by clicking the **Configuration management** tab in the context menu from the **Device management** view, and then clicking the **Firmware** tab. The firmware is organized by device types, components, and then available versions. Each firmware version has a status based on its age and number of vulnerabilities.

- **Critical.** (red) A later firmware version that fixes critical or high vulnerabilities.
- **Warning.** (amber) A later firmware version that fixes non-critical (medium or low) vulnerabilities.
- **Normal.** (green) The latest firmware version, or a later firmware version that has a new feature but no vulnerabilities.

You can view details about a specific firmware version, including the release date and list of fixed vulnerabilities, by clicking the firmware version.

You can see the number of devices that have the specific version of firmware installed. Click the number to see a filtered list of devices with that firmware version.

Firmware inventory for a specific device

You can see a list of firmware that is installed on a specific device by clicking the **Managed devices** panel title from the **Device management** view, and then click the name of the device in the table to display the device details page. Then, click **Firmware status** from the context menu.

This page lists the current firmware version, firmware status, and latest available update for each managed device.

Firmware health

You can see a summary of firmware health of all managed devices in your organization by clicking **Overview** in the context menu from the **Device management** view.

You can also view the firmware health of each managed device and their components by clicking the title of the **Managed devices** card on the **Overview** page, and select **Firmware status** from the context menu

XClarity One uses the firmware age and highest severity vulnerabilities to determine the firmware status of each component in your managed devices.


- **Up to date.** The device has firmware that is less than 1 year old and has no warning or critical vulnerabilities.
- **Available updates.** The device has firmware that is 1 – 2 years old or has warning vulnerabilities but no critical vulnerabilities.
- **Critical updates.** The device has firmware that is greater than 2 years old or has critical vulnerabilities.

For devices with assigned templates, you can determine whether the firmware on each device is compliant with the rules and criteria in the template by clicking the template name from the **Template** column in the table.

Firmware packages

For XClarity One in the cloud, Lenovo ensures that the latest firmware versions are available. However, there might be cases where limited availability fixes (LAFixes) might be created by Lenovo specifically for you and need to be manually imported into the cloud portal for your organization.

For XClarity One as a local virtual machine, you need to manually download update packages from the [Lenovo Data Center Support website](#) and then import them into XClarity One.

To manually import firmware packages, click **Configuration management** tab in the context menu from the **Device management** view, click the **Firmware** tab, and then click the **Add** icon () from the **Firmware** page.

Notes:


- You can import only firmware packages that were created and signed by Lenovo.
- On the **Firmware Package** page, you can receive metadata for firmware packages released from 2023 and later. To use the updates, you must import the metadata files along with the payload files.
- You must import all required files base on the resource type.
 - For ThinkSystem V3 and V4 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 ThinkSystem V1, ThinkSystem V2, and ThinkEdge servers, import the payload (.zip, .uxz, .tar.gz, .tar, .bin), metadata (.xml), change log (.chg) and readme (.txt).
- The maximum size of a single file is 2 GB.
- These firmware packages are only available to the organization that you were in when you import the files.

Firmware updates

Lenovo XClarity One uses the management hubs to apply firmware updates to your managed devices. When you initiate a firmware update from the XClarity One portal, XClarity One pushes the required update packages to the appropriate management hub and then sends a request to the hub to apply the update on the target devices. The management hub sends status, progress, and log data back to the XClarity One portal during the update process so you can monitor progress.

The **Things To Do** panel displays a card when new firmware updates are available. From the todo, you can view the alerts for each new firmware update.

You can install firmware updates on one or more devices using templates. For more information, see [Device templates](#).

You can also install firmware updates on a specific device from the **Managed devices** page or from a specific device's **Firmware inventory** page by clicking the **Update** icon (). If the target devices have an assigned template, review the updates that are selected based on the template rules to complete the installation. If no template is assigned, follow the steps in the wizard to complete the installation.

Attention:

- Some components require the device to be restarted to complete the firmware update, such as unified extensible firmware interface (UEFI), network cards, RAID adapters, and disks. During the update process, the server might be restarted automatically one or more times until the entire process is complete. Ensure that any running workloads have either been stopped or moved to a different server.

- Performing firmware updates, device settings updates, and power operations on managed devices are disabled by default. Before updating firmware, ensure that you enable this function from the XClarity One portal and from the management hub that manages that target devices. For more information, see [Management functions](#).

During the update process, if one component fails, the management hub continues to apply updates on the remaining components for the device and for other devices in the same job.

Prerequisite firmware

In some cases, prerequisite firmware might be needed to install the intended firmware version. XClarity One automatically installs prerequisite firmware, when available.

Firmware rules and criteria

You can choose a default update rule to use generally for all device types and components. Then, you can then optionally select a custom rule for each type of device and component. If you do not select a custom rule, the device type inherits the default rule, and the components inherit the device-type rule. Changing the device-type rule also changes the components that inherit that rule.

The following default rules are available.

- **No default rule.** You must select a custom rule for each device and component.
- **By tagged version.** The following tags are supported.
 - **Latest version.** Firmware on the device is compared to the latest firmware version that is available in the firmware-updates repository.

You can choose the one of the following custom rules.

- **No rules.** (default) The device or component type is not included in the template and is not checked for compliance.
- **Latest version.** (default) Firmware on the device is compared to the latest firmware version that is available when the template is created.

Important: The version does not change when a later firmware update becomes available after the template is created.

- **Specific version.** Firmware on the device is compared to the selected version, regardless of what is available in the repository. You can choose any version that is available in the repository.


Immediate vs prioritized updates

Some components (such as unified extensible firmware interface (UEFI), network cards, RAID adapters, and disks) require the device to be restarted to complete the firmware update. Devices with these components are restarted automatically one or more times during the update process.

By default, devices are restarted immediately to complete the update process.

You can choose to wait to update firmware on components that require a restart until you manually restart the device by selecting the **Prioritized activation** option. Additional restarts are then performed until the update-process completes. With this option, firmware that can updated without a restart are completed immediately. Only firmware updates on components that require a restart are delayed.

When **Prioritized activation** is enabled, a todo is raised to notify you that devices need to be restarted to complete the update process.

You can find a list of devices that must be restarted from the Managed devices page by filtering for devices in the **Pending** state. These devices are identified by the **Restart Required** icon ()

Important:

- Ensure that any running workloads are stopped or moved to a different device before performing updates that require a restart or before manually restarting a device to complete the update process.
- After a prioritized update completes, it might take several minutes before the correct firmware level is reflected in the portal.
- When enabled, the Wake-on-LAN boot option can interfere with XClarity One operations that power off the server if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.

Device settings

You can use Lenovo XClarity One to quickly configure and maintain device settings on your managed devices by learning the device-settings configuration from an existing device and then applying that configuration to your other servers. You can use the health summaries to identify the device-settings health of your devices, use templates to identify the target settings-configuration that you want to maintain on each device, and update target devices to match the target configuration.

If a device-settings configuration or template is assigned to a device, you can view the device-settings compliance for that device by clicking the **Managed devices** panel title from the **Device management** view, clicking the device, and then clicking **Configuration** from the context menu.

Attention:

- Devices must be running firmware that was released January 2024 or later.
- Updating device settings is not supported for ThinkSystem SR635 and SR655 servers.

You can use device-settings configurations to configure system information, boot order, baseboard management controller, and Unified Extensible Firmware Interface (UEFI) settings on managed servers.

You cannot configure the following settings.

- Local storage and SAN zoning
- I/O adapters
- Local user accounts
- LDAP servers
- VLAN configuration
- System OOB custom
- Trusted computing group
- Ethernet interface configuration
- SNMP (sensitive authentication values are not supported)
- SMTP (sensitive authentication values are not supported)
- Server-specific information (name and location)

Attention: XClarity One does not assign IP and I/O addresses to individual servers when the device settings are deployed.

Device-settings configurations

XClarity One creates a device-settings configuration by learning the settings on a golden master device that has the correct firmware level and device settings that you want to apply on target devices. You can then assign and apply the device-settings configuration to target devices that have the same machine type and specifications (such as processors, memory, storage, and features-on-demand keys) as the golden master device.

- Currently, you cannot view the device settings for a specific device from the XClarity One portal.
- You cannot change the settings in a learned device-settings configuration. Instead, change the desired settings on the golden-master device before learning the configuration.
- Update the firmware on target devices to match the firmware levels on the golden master device before applying the device-settings configuration to the target devices.

You can see a list of device-settings configurations clicking the **Lifecycle Management** on the context menu from the **Device management** view, and then clicking **Device settings** from the context menu.

This page lists the device-settings configurations by device type and the number of templates that use each configuration. You can click a number in the **Templates** column to see a filtered list of templates that use a specific configuration.

Compliance checks

XClarity One checks the compliance status of devices by comparing the current settings on the target device with the settings that are defined by its assigned device-settings configuration.

Note: Currently, you cannot view the compliance details.

The compliance status can be one of the following.

- **Compliant.** No action is required. The device complies with the assigned device settings configuration.
- **Not Compliant.** Target device is not compliant to the assigned device settings configuration. Apply a configuration or template to target device to make it compliant.
- **Not Applicable.** Target device is not applicable with the assigned device settings due to mismatched or conflict setting definitions. In this case, the assigned device-setting configuration *cannot* be applied to target device.

The settings on a device might not be applicable with its assigned device-settings configuration in the following instances.

- Device firmware on the target device is different than the golden-master device that was used to generate the device-settings configuration.

If the target device has different firmware levels than the golden-master device, upgrade the firmware on the target devices to match the golden master device before applying the device-settings configuration

- Device has different machine type or hardware specifications (such as processors, memory, storage, and features-on-demand keys) than the with the device from which the device-settings configuration learned.
- **Calculating.** The compliance status is being calculated.
- **Unknown.** The portal failed to calculate the compliance status. Check the events logs for details.

The compliance check is run on a device when:

- When a template is initially assigned to the device or the template assigned is changed.
- When the assigned template is modified.
- When the server inventory or device settings are changed.
- When a power action is performed on the device.
- One week has passed since the last compliance check

The settings on a device can become out of compliance with its assigned device-settings configuration in the following instances.

- Firmware was updated, which changed device settings and definitions.
- Device settings were changed directly on the server.

- An issue occurred during configuration deployment, such as a firmware issue or an invalid setting.

Device-settings updates

Lenovo XClarity One uses the management hubs to apply device settings to your managed devices. When you initiate a device-settings update from the XClarity One portal, XClarity One pushes the configuration to the appropriate management hub and then sends a request to the hub to apply the configuration on the target devices. The management hub sends status, progress, and log data back to the XClarity One portal during the update process so you can monitor progress.

You can update device settings on one or more devices using templates. For more information, see [Device templates](#).

You can also update device settings on a specific device from the **Managed devices** page by clicking the **Deploy template** icon (🔄). If the target devices have an assigned template, review the updates that are selected based on the template rules to complete the installation.

Attention:

- Some components require the device to be restarted to complete the configuration update, such as unified extensible firmware interface (UEFI).

During the update process, if one component fails, the management hub continues to apply updates on the remaining components for the device and for other devices in the same job.

Immediate vs prioritized updates

When you update a device-settings configuration on a device, the device settings are written to shared memory on the target devices and are then activated.

Some device settings, such as baseboard management controller and Unified Extensible Firmware Interface (UEFI) settings, require the device to be restarted to complete the update.

By default, the *prioritized activate* option is selected. This option activates the configuration changes that require a restart after you manually restart the device. The **Restart Required** icon (🔔) is displayed in the device status to notify you that the device needs to be restarted to complete the update process.

You can select the *immediate activation* option to restart target devices immediately to complete the update process.

Important:

- Use **Soft restart** to restart the server to continue the update process. *Do not* use **Hard restart**.
- Ensure that any running workloads are stopped or moved to a different device before performing updates that require a restart or before manually restarting a device to complete the update process.
- After a prioritized update completes, it might take several minutes before the correct device settings are reflected in the portal.
- When enabled, the Wake-on-LAN boot option can interfere with XClarity One operations that power off the server if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.

Device templates

Lenovo XClarity One makes it easy to quickly setup and maintain your devices by deploying firmware and device settings on your managed devices using templates. *Device templates* consist of a set of rules and criteria that define the desired configuration for a certain type of device and identifies which managed

devices are monitored for compliance. If a device is out of compliance, you can use the templates to update the device to match the desired profile.

You can create a template by clicking the **Lifecycle Management** tab in the context menu from the **Device management** view, clicking the **Templates** context menu, and then clicking the **Add** icon (+). Follow the steps in the wizard to create the template and assign the template to one or more devices.

Important: A single template can support at most six different firmware collections.

You can view template details, criteria, and assigned devices by clicking the template name in the table.

Template assignment

You can assign a template to one or more servers when you create the template using the **Create template** wizard. You can also assign a template to a server in the following ways.

- From the **Template** page by selecting a template and clicking the **Assign** icon (📄).
- From the **Template** details page by clicking the **Add** icon (+) from the devices table.
- From the **Managed devices** page by selecting one or more devices and clicking the **Assign** icon (📄).

Each device can have only one assigned template or no assigned template. When a server has an assigned template, compliance is based on the rules and criteria that is defined in the template. If a server has no assigned template, compliance is based on the latest available version.

Ensure that the template is applicable to the type of server to which it is assigned. If a template is not applicable, then individual component compliance status might be "Not Assigned" even when the overall device compliance is "Compliant."

Applicability and compliance checks

XClarity One checks the compliance status of devices by comparing the device profile with the rules that are defined by its assigned template. The compliance check is run on a device when:

- When a template is initially assigned to the device, or when the template assigned is changed.
- When the assigned template is modified.
- When the server inventory is changed.
- When a power action is performed on the device.
- 24 hours has passed since the last compliance check (for firmware)
- One week has passed since the last compliance check (for device settings)

Template deployment

Important: Firmware and device settings update functions must be enabled before you can deploy a template to devices. For more information, see [Management functions](#).

While a template deployment is in progress, the target servers are locked. You cannot initiate other management tasks on the target servers until the deployment process is complete.

When servers are not compliant with their assigned template, you can make the devices compliant by deploying the assigned template to those devices. Deploying the template updates non-compliant firmware and device settings to the desired version based on the template rules.

You can deploy a template to one or more servers when you create and assign the template using the **Create template** wizard. You can also deploy a template to assigned server in the following ways.

- From the **Template manager** page by clicking the **Add** icon (+) from the devices table.

- From the **Things to do** pane, click **Update** from the **New non-compliant devices** card, and follow the wizard.
- From the **Managed Devices** page by clicking **Firmware status** from the context menu, and then selecting the devices and clicking the **Deploy** icon (🔄).

In some cases, prerequisite firmware might be needed to install the intended firmware version. XClarity One automatically installs prerequisite firmware, when available.

Currently, you need to deploy the template once for each component of the template. If a template includes updates for firmware and device settings, the first time you deploy the template, XClarity One updates only firmware. You need to deploy a second time to update the device settings.

Attention:

- Some components require the device to be restarted to complete the firmware update, such as unified extensible firmware interface (UEFI), network cards, RAID adapters, and disks. During the update process, the server might be restarted automatically one or more times until the entire process is complete. Ensure that any running workloads have either been stopped or moved to a different server.
- Performing firmware updates, device settings updates, and power operations on managed devices are disabled by default. Before updating firmware, ensure that you enable this function from the XClarity One portal and from the management hub that manages that target devices. For more information, see [Management functions](#).

During the update process, if one component fails, the management hub continues to apply updates on the remaining components for the device and for other devices in the same job.

Delayed deployment

Some updates require the target devices to be restarted, which could disrupt work on those devices. To minimize the disruption, you can choose to delay the deployment process until after the target device is restarted by selecting **Prioritized activation**.

When the device needs to be restarted:

- **ThinkSystem V4 servers:** The deployment job enters a waiting state and waits for the device to be restarted to continue. After the device is restarted, the job resumes automatically and completes the update.
- **ThinkSystem V1/V2/V3 servers:** If target firmware requires a restart, the deployment job enters a waiting state and waits for the device to be restarted to continue. If target firmware does not require a restart, the job completes with a warning, and you are notified to manually restart the device to activate the pending firmware.

Firmware rules and criteria

You can choose a default update rule to use generally for all device types and components. Then, you can then optionally select a custom rule for each type of device and component. If you do not select a custom rule, the device type inherits the default rule, and the components inherit the device-type rule. Changing the device-type rule also changes the components that inherit that rule.

The following default rules are available.

- **No default rule.** You must select a custom rule for each device and component.
- **By tagged version.** The following tags are supported.
 - **Latest version.** Firmware on the device is compared to the latest firmware version that is available in the firmware-updates repository.

You can choose the one of the following custom rules.

- **No rules.** (default) The device or component type is not included in the template and is not checked for compliance.
- **Latest version.** (default) Firmware on the device is compared to the latest firmware version that is available when the template is created.

Important: The version does not change when a later firmware update becomes available after the template is created.

- **Specific version.** Firmware on the device is compared to the selected version, regardless of what is available in the repository. You can choose any version that is available in the repository.

Device settings configurations

You can choose the device-settings configuration to deploy to the target devices. You can select an applicable configuration to apply to all devices of a specific machine type.

If you do not want to change the device settings on the target devices, choose **No rule**.

Vulnerabilities

Firmware updates often have fixes for common vulnerabilities and exposures (CVEs). You monitor the which managed devices have firmware updates that fix these vulnerabilities.



[XClarity One: Monitoring details](#)

Devices with vulnerabilities

You can view a summary of devices that have critical vulnerabilities and exposures (CVE)s from the **Managed devices** panel by clicking **Overview** in the context menu from the **Device management** view. The **Managed devices** panel summarizes the data about devices that have vulnerabilities, including the following data. Vulnerabilities status is based the vulnerabilities with the highest severity.

- A circular graph representing the percent of devices with vulnerabilities in each severity: critical, high, medium, low, or none (protected). Hover over each colored bar in the graph to see the total number of vulnerabilities for the specific severity.
- Total number of devices with vulnerabilities, by severity. Click a number to open the **Managed devices** page with a list of all devices that have unapplied vulnerabilities of that severity.

You can view the total number of vulnerabilities and the number of vulnerabilities of each severity for the firmware that is currently installed on each device by clicking **Overview** in the context menu from the **Device management** view, and then clicking the **Managed devices** panel title. This **Managed devices** page lists the total number of vulnerabilities and the number of vulnerabilities of each severity for the firmware installed on each device.

Vulnerabilities over time

You can monitor vulnerabilities that affect your devices, by severity, over time by clicking **Monitor** in the context menu from the **Device management** view. The **Vulnerabilities** panel summarizes the number and severity of vulnerabilities over the past year. Vulnerabilities status is based the vulnerabilities with the highest severity.

- A circular graph representing the percent of vulnerabilities by severity: critical, high, medium, low. Hover over each colored bar in the graph to see the total number of vulnerabilities for the specific severity.
- Total number of vulnerabilities by severity. Click a number to open the **Vulnerabilities** page with a list of all vulnerabilities for that severity.

- A bar graph representing the number of vulnerabilities, over time during the last twelve months. Hover over each colored bar in the graph to see the number of vulnerabilities by severity.
- Total number of vulnerabilities, by severity, that are older than one year.

Vulnerability summary

You can view a summary of vulnerabilities, by severity, for all devices in the organization. Click **Monitor** in the context menu from the **Device management** view, and then click the **Vulnerabilities** panel title. The **Vulnerabilities Overview** card summarizes the total number of vulnerabilities per severity. The **Vulnerabilities** table provides detailed information about each vulnerability.

- A circular graph representing the percent of vulnerabilities by severity: critical, high, medium, low. Hover over each colored bar in the graph to see the total number of vulnerabilities for the specific severity.
- Total number of vulnerabilities by severity. Click a number to filter the list of vulnerabilities in the table below.
- Table that lists details about each vulnerability, including a description, when the vulnerability was published, the severity, and the number of devices that are affected by the vulnerability.

Click on the number of devices associated with a specific vulnerability to display the Managed Devices page with a filtered list of devices that have firmware with that vulnerability.

Vulnerability details

Can you view detailed information about a vulnerability by clicking **Monitor** in the context menu from the **Device management** view, and then clicking the **Vulnerabilities** panel title. From the table on the **Vulnerabilities** page, click the name of a specific vulnerability to find detailed information about that vulnerability in the [National Vulnerabilities Database webpage](#).

Warranties

You can determine the warranty status of the managed devices from the Lenovo Support website.

You can look up the warranty information, including extended warranties, for your devices from the [Lenovo Warranty Lookup webpage](#).

By default, an event is raised to warn you 90 days before and again 60 days before the warranty expires on a device. Between 30 days and the expiration date, an alert and event are raised.

For devices that are under warranty, you can choose to have Lenovo automatically ship replacement parts to you, for free, when a customer-replaceable part fails and generates a serviceable event. For more information, see [Automatic problem notification \(Call Home\)](#).

Call Home contacts

When Call Home is configured and a serviceable event is triggered that automatically creates a service ticket, Lenovo Support might need to reach out to someone regarding the event. The primary or secondary contact that is configured for Call Home is contacted by default. However, you can choose to assign a different Call Home contact to all devices in a specific collection.

If a contact is assigned to a collection, and you add more devices to that collection, the preferred contact is also assigned to the new devices.

If you assign a contact to a collection, and some devices in that collection are also in another collection to which a contact was assigned, you can choose whether to change the assignment to the new contact or to keep the existing contact.

You can change the assigned contact for a specific device from the **Actions** panel on **Device** page by clicking **Service → Preferred contact**. You can choose from a list of contacts that were assigned to the collections in which the device is a member.

If you delete a Call Home contact, the default Call Home contact is used for all devices that were assigned the deleted contact.

Service data

When there is a problem with a device that requires assistance to resolve, you can manually collect service data that is needed to help identify the cause of the issue (including service information, inventory, and logs) and then send the service-data file to Lenovo Support.

Attention:

- Service data includes sensitive information, including serial numbers, UUIDs, IP addresses, host names, and device locations. If needed, take appropriate steps to protect any service-data files that were saved to your local system.
- Service data is not stored in the management hubs or in the cloud.

The following conditions are required to manually collect and upload service data for a managed device.

- You must accept the [Call Home agreement](#) in the web interface before you can collect and upload service data.
- Call Home must be configured (see [Automatic problem notification \(Call Home\)](#)).
- The device must be online.
- Another service-data collection job must not be running on the device.

You can also send other files from your local system to Lenovo support. Local files can be no more than 2 GB.

You can collect and upload service data or you can send files from your local system to Lenovo Support for a specific device. From the **Device management** view, click the **Managed Device** panel title, and click the name of the device in the table to display the managed-device details page. Then, from the **Actions** panel, click **Service → Upload data to Lenovo Support**.

Attention: You must accept the [Call Home agreement](#) in the web interface before you can collect and upload service data (see [Automatic problem notification \(Call Home\)](#)).

When you manually collect service data, you can automatically upload the service-data file to Lenovo Support. From the **Device management** view, click the **Managed Device** panel title, and click the name of the device in the table to display the managed-device details page. Then, from the **Actions** panel, click **Service → Collect and Upload data**.

When you manually collect service data, you can save the service-data file as an archive in tar.gz format to your local system, which you can then send to Lenovo Support. You can send other files from your local system to Lenovo support, as well. Local files can be no more than 2 GB. From the **Device management** view, click the **Managed Device** panel title, and click the name of the device in the table to display the managed-device details page. Then, from the **Actions** panel, click **Service → Upload data to Lenovo Support**.

Lenovo is committed to security. When service data is sent to Lenovo Support either automatically through Call Home or manually by you, the service-data archive is sent to Lenovo Upload Facility over HTTPS using TLS 1.2 or later. Your business data is never transmitted. Access to service data in the Lenovo Upload Facility is restricted to authorized service personnel.

For information about setting up Call Home to automatically send service data when serviceable events occur on managed devices, see [Automatic problem notification \(Call Home\)](#).

Service tickets

You can monitor service-ticket metrics by clicking **Monitor** in the context menu from the **Device management** view.

The Service tickets panel summarizes the data about tickets that were raised by managed devices, including the following data.

- A circular graph representing the percent of tickets by status (low, medium, high, critical). Hover over each colored bar in the graph to see the total number of tickets for the specific severity.
- Total number of tickets by status. Click a number to open the Service Tickets page with a list of all tickets in that status.
- A line graph representing the number of tickets, over time in the last month. Hover over each colored bar in the graph to see the number of tickets by status.
- Total number of tickets, by status, in last month and in the past year.

Chapter 12. Alerts and events

You can use Lenovo XClarity One to monitor the alert and event history of your managed devices.

 [XClarity One: Monitoring details](#)

You can view active alerts and events and monitor metrics by clicking **Monitor** in the context menu from the **Device management** view.

Active alerts

Alerts are events that represent a problem that requires investigation and user action.

Alerts exist only while they are active. When an alert is raised (asserted), an identical event is added to the event log. When an alert is removed (de-asserted), an event is added to the event log that states that the problem no longer exists.

The management hub sends new active alerts to the XClarity One portal as soon as they are raised and removes alerts in XClarity One portal as soon as they are resolved. XClarity One also synchronizes alerts with the management hubs every six hours to ensure consistency.

If alerts cannot be forwarded (such as when connectivity is down), the management hub stores alerts until they can be pushed successfully, for up to 24 hours. If connectivity is down for more than 24 hours, only the last 24 hours of alerts are pushed when connectivity is restored.

Alerts regarding water-cooled systems are raised using the "fan" category.

Events

XClarity One stores a historical list of all resource and audit events in a single *events log*. A maximum of **10,000** events are stored for each organization. When the maximum number of events is reached, the oldest event is discarded when the next event is received.

- **Resource events**

A *resource event* identifies a condition that occurred on a managed device, management hub, or XClarity One that is not related to direct user action (for example, a connectivity issue between a device and the management hub). You can use these events to track and analyze hardware and management related issues.

- **Audit events**

An *audit event* is a record of user activities that were performed from a management hub or XClarity One (such as a user performing a power action on a device). Each audit event includes the username (email address) and IP address of the user that performed the action. You can use these audit events to track and analyze authentication-related issues and user activity.

The management hub sends events to the XClarity One portal as soon as they are raised. XClarity One also synchronizes alerts with the management hubs every six hours to ensure consistency.

If events cannot be forwarded (such as when connectivity is down), the management hub stores events until they can be pushed successfully, for up to 24 hours. If connectivity is down for more than 24 hours, only the last 24 hours of events are pushed when connectivity is restored.

Metrics and trends

The **Alerts** panel and **Events** panel summarize the data about active alerts and events that were raised by managed devices, including the following data.

- A circular graph representing the percent of alerts/events by severity (critical and warning). Hover over each colored bar in the graph to see the total number of alerts/events for the specific severity.
- Total number of alerts/events by severity. Click a number to open the Alerts page or Events page with a list of all alerts/events in that severity.
- A line graph representing the number of alerts/events, over time in the last month. Hover over each colored bar in the graph to see the number of alerts/events by severity.
- Total number of alerts/events, by severity, during last month and during the last year.

Custom alerts

Lenovo XClarity One raises alerts based on known hardware and firmware issues. You can create alert rules for raising custom alerts that you are interested in based the occurrence or frequency of certain events or based on metric thresholds.

Event-based alerts

You can define custom alert rules to raise an alert when specific events occur on any device or management hub.

- **Event occurrence.** An alert is raised when one or more events occur based on one of the following criteria.
 - When all the target events occur at least once during a certain period of time
 - When any of the target events occur collectively the specified number of times (count) during a certain period of time. For example, if you have custom rules for three events that are monitored for two occurrences in a 10-minute period, if one of the events occurs twice in that period, the alert is raised.
 - Every time one of the target events occur
 - When each of the target events occur in sequence during a certain period of time
- **Event frequency.** An alert is raised when one or more target events occur a specific number of times (count) during a certain period of time based on the following criteria.
 - Every time one of the target events occur
 - When any of the target events occur a specific number of times (count) during a certain period of time
- **Metric thresholds.** An alert is raised when the metric value exceeds the device threshold based one of on the following criteria.
 - When the average value of the metric exceeds 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).
 - When the metric exceeds 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).
 - When the metric exceeds the threshold (based on the comparator) for a certain cumulative sub-interval out of specific given maximum 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 cumulative 30 minutes out of 120 minutes period (maxInterval).
 - When the metric exceeds 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).

You can create alert rules for an event that already occurred by clicking **Monitor** in the context menu from the **Device management** view, and then click the title of the Events card. Select the event, and then select the **Create alert rule** icon (+).

You can generate an alert rule for any event by clicking the **Alert rules** tab on context menu from the **Settings** view, and then clicking the **Create alert rule** icon (+). For a list of event codes, see [Event messages](#) in the XClarity One online documentation.

Important: Each event rule can apply to only one resource type. You cannot add event codes for multiple resource types to a single alerts rule. For example, you cannot add an event code for devices (FQXSP*) and an event code for management hubs (FQXMH*) to the same rule.

Metric-based alerts

You can edit alert rules for usage-metric thresholds, but you cannot create new alert rules for them.

Currently XClarity One supports threshold alerts for processors and memory.

Thresholds for these usage metrics are enabled by default. When enabled, an alert is raised when a component meets or exceeds its warning or critical threshold for the alert duration. The *alert duration* is the number of minutes during a specific period that the threshold value must be met or exceeded. For example, if processor usage has a warning threshold of 80% and alert duration of 4 of 10 minutes, then an alert is raised when the processor usage exceeds 80% for 4 or more minutes within a 10-minute period.

The minimum interval is 2 minutes within a 5-minute period.

You can set warning and critical usage thresholds and the alert duration for the certain components by clicking the **Alert rules** tab on context menu from the **Settings** view and then clicking the row for the component that you want to change.

Data forwarders

Lenovo XClarity One can forward data about events that occur in your environment, based on criteria (filters) that you select, to external services that you can then use to monitor and analyze the data. Every generated event is monitored to see if it matches the criteria. If it matches, the event is forwarded to the specified destination using the appropriate protocol.

To create a data forwarder, click **Data forwarding** in the context menu of the **Settings** view, click the **Add** icon (+), and then follow instructions in the wizard.

Important: Only the organization owners can create, modify and delete data forwarders.

You can test the connection to the external service from the **Configure** tab in the wizard before saving the data forwarder. When you click **Test connection**, a test event is sent using the provided configuration settings.

Event criteria

Use the search field to choose the events to forward based on the following types of criteria. If you do not provide criteria, data is forwarded for all events that are generated by all resources (managed devices, management hubs, and XClarity One portal).

- Name of resources and device components that generated the events
- Event severity

Forwarder destinations

You can forward event data to the following destinations.

- **Email**

For XClarity One in the cloud, you can forward event data to email addresses for one or more users in the organization. You cannot forward event data to external users.

New events that match the selected criteria are forwarded via email every hour. The emails are sent from noreply@xc1mail.lenovo.com with the subject "Buffered Event Forwarding."

If you change the filter criteria for the forwarder, events that were buffered before the changes were saved will match the previous filter criteria, and events that were buffered after the changes were saved will match the latest filter criteria. So, the email that is sent after the changes were save might have some events that match the previous filter criteria.

Events are listed in tabular format, one row per event.

- **Web service**

You can forward event data to ServiceNow Cloud. Other user-defined REST web services are not supported.

New events that match the selected criteria are forwarded over the network to the web service as soon as the events are raised, using the HTTPS protocol. Port **443** is used by default.

Attention:

- Ensure that ServiceNow Cloud is configured to accept valid incoming traffic.
- Ensure that ServiceNow Cloud uses a trusted CA-signed certificate. Self-signed certificates are not supported.
- Ensure that you test the connection to the web service by clicking **Test Connection** in the Data Forwarder wizard. During the test-connection process, XClarity One imports and validates the certificate chain from the web service. After the certificate is validated, XClarity One sends a sample event to the web service.

Events are forwarded in JSON format. The following example shows event data that is forwarded to an email or web service.

```
{
  "id": 3395,
  "action": "new",
  "category": "drives",
  "description": "When a hardware event is detected by the Lenovo XClarity Controller on the
                  server, the Lenovo XClarity Controller writes that event in the system-event
                  log on the server.",
  "eventClass": "service",
  "eventCode": "FQXSPSD0001L",
  "flags": [],
  "fruType": "drives",
  "manager": {
    "id": "B0018518B16549398A088862CAF1F705",
    "ipAddress": "10.241.36.230",
    "name": "DEV HUB 2757",
    "type": "XClarity Management Hub"
  },
  "message": "Drive Drive 0 in the enclosure has been disabled due to a detected fault.",
  "messageArgs": [ "Drive 0" ],
  "service": "serviceable",
  "severity": "critical",
  "source": {
    "id": "AE9FBDF62F911E988453A68DD01A3F7-B0018518B16549398A088862CAF1F705",
    "groups": [],
    "name": "J100CVZW",
    "type": "server"
  },
}
```

```

"targetResource": {
  "id": "AE9FBDF62F911E988453A68DD01A3F7-B0018518B16549398A088862CAF1F705",
  "groups": [],
  "name": "J100CVZW",
  "type": "server"
},
"timestamp": "2025-02-18T12:32:06.419Z",
"userAction": "Complete the following steps until the problem is solved: \n1) Reboot the system
               and confirm that the drive is still in failed state.\n2) Collect Service Data
               log.\n3) Contact Lenovo Support.",
"_links": {
  "rel": "self",
  "uri": "/api/v1/monitoring/events/3395"
}
}

```

Chapter 13. Jobs

Jobs are long-running tasks that run asynchronously in the background. If a long-running task targets multiple resources, a separate job is created for each resource.











[XClarity One: Monitoring details](#)

While a job is running, the Jobs dialog uses a progress bar to show the current progress. You can hover over the progress bar to see the current status and percent (if the job is running). If you close the dialog, you can monitor the status of all jobs that are currently running from the **Jobs** panel that is accessed from the **Monitor** tab.

To view a list of *all* jobs, click **See jobs** from the **Jobs** panel to display the **Jobs** page. You can drill down to view detailed information about a specific job by clicking the job in the table to display the job details page. From this page, you can see information about each subtask in the job. Click the job or subtask on this page to display more details in the **Job Logs** panel.

A job can be in one of the following states.

-  This job is in the process of waiting or pending another action.
-  The job is running without issues. This includes jobs that are initializing, investigating, uploading, validating, or running.
-  The job is running but some warnings have occurred.
-  The job is running but some errors have occurred.
-  The job ended with warnings. This includes jobs that were stopped, completed, canceled, or interrupted.
-  The job ended with errors. This includes jobs that were stopped, completed, canceled, or interrupted.
-  The job ended without issues. This includes jobs that are resolved or completed.
-  The job was stopped. This includes jobs that were stopped, skipped, interrupted, expired, blocked, aborted, canceled or being canceled.

Jobs that are running for more than 24 –36 hours are stopped and placed in the **Expired** state.

Only jobs that are completed or expired can be manually deleted.

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

Chapter 14. Service and support

Lenovo XClarity One provides a set of tools that you can use to collect and send service-data files to Lenovo Support, set up automatic notification to Lenovo Support when serviceable events occur on specific devices, monitor service-tickets, and view warranty information. You can contact Lenovo Support to get help and technical assistance when you run into problems.

Automatic problem notification (Call Home)

Call Home can be used to automatically notify Lenovo Support when a serviceable event occurs on a specific device that is under warranty and to ship replacement parts if needed.

Important: Lenovo is committed to security. When service data is sent to Lenovo Support either automatically through Call Home or manually by you, the service-data archive is sent to Lenovo Upload Facility over HTTPS using TLS 1.2 or later. Your business data is never transmitted. Access to service data in the Lenovo Upload Facility is restricted to authorized service personnel.

Call Home agreement

You must agree to the [Call Home agreement](#) (privacy statement) to use Call Home, to manually upload files to Lenovo Support, and to attach notes and files to a service ticket. If you disable the Call Home agreement, those functions are also disabled.

Call Home contacts

When you set up Call Home, you provide the names and contact information for people that Lenovo Support can contact when an automatic service ticket is opened for a serviceable event that is generated by one of the managed devices. You must provide a primary contact and can optionally provide a secondary contact.

You can also assign a contact to all devices in a specific collection. If a device does not have an assigned contact, the primary contact that is provided for Call Home is used.

Note: You must test the connect to Call Home before you can apply the Call Home contact information and enable Call Home.

Service tickets

If Call Home is configured, when a serviceable event occurs on a specific device (such as such as an unrecoverable memory), Lenovo XClarity One *automatically* opens a service ticket with Lenovo Support, collects service-data files for the managed device, and attaches the collected data to the ticket.

Attention:

- Service data includes sensitive information, including serial numbers, UUIDs, IP addresses, host names, and device locations. If needed, take appropriate steps to protect any service-data files that were saved to your local system.
- Service data is not stored in the management hubs or in the cloud.

If Call Home is not configured, you can manually open a service ticket and send service files to the Lenovo Upload Facility by following the instructions on the [Submit an eTicket webpage](#).

To configure Call Home, click the **Settings** tab in the left navigation and then click **Call Home** in the context menu.

- Ensure that [Call Home agreement](#) is accepted. This is required to open service tickets and send data to the Lenovo Support Center.

- Specify your default Lenovo customer number to use when reporting problems. If you do not have your Lenovo Customer Number, contact your local Lenovo Sales Representative to get it.
- Specify the contact and location information for the default primary and secondary personnel that can be contacted by Lenovo Support.

Attention: When contacts are in the following countries, Call Home needs a Lenovo Premier Support contract. For more information, contact your Lenovo representative or authorized business partner.

- Qatar
- Saudi Arabia
- United Arab Emirates

Call Home is enabled when contact information is filled in. To disable Call Home, clear the configuration information by clicking **Reset to default**.

Replacement parts

When you configure Call Home, you provide a general address where Lenovo is to ship replacement parts.

If you enable automatically shipping replacement parts and a device that is under warranty detects a faulty customer-replaceable part, Lenovo automatically ships a replacement part, for free, to speed up your time to resolution and minimize your downtime. Only parts that you can install yourself are shipped.

If you enable automatically shipping replacement parts and a device that *is not* under warranty detects a faulty customer-replaceable part, you will be contacted by Lenovo Support about shipping a replacement part for a fee.

If you assign a preferred contact to all devices in a specific collection, replacement parts are shipped to the preferred contact's shipping address. If a contact is not assigned, parts are shipped to the default primary contact using the general shipping address that you configured on the **Call Home** page.

Service tickets

Opening a service ticket starts the process of determining a resolution to your device 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 a service ticket is opened.

If Call Home is configured, Lenovo XClarity One automatically opens a service ticket in the Lenovo Support Center when a serviceable event occurs on a device, such as such as an unrecoverable memory (see [Automatic problem notification \(Call Home\)](#)).

If Call Home is configured, you also can manually open a service ticket for a specific device, from the **Actions** panel on device details page by clicking **Service → Create a service ticket**. When you can manually open a service ticket, XClarity One opens a service ticket with Lenovo Support, collects service-data files for the managed device, and attaches the collected data to the ticket.

Use the following definitions when selecting the severity for the service ticket.

- **Low.** The problem causes little or no impact to your operations, or you have implemented a reasonable workaround.
- **Medium.** You can use the product with minor features unavailable. However, these restrictions do not have a critical impact on operations.
- **High.** You can use the product, but your operations are severely limited by the problem.
- **Critical.** You cannot use the product, resulting in a critical impact to your operations. This condition requires an immediate solution.

You can add additional information to a service ticket in the In Progress state at any time by adding notes and by uploading new service-data files. You can collect and upload new server data (inventory, vital product data, and event logs) for a specific device or upload an existing (local) service-data file that is no more than 2 GB.

Service ticket status in XClarity One 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.

You can view service ticket detail in the Lenovo Support ticketing system by clicking the service ticket number.

Attention: You must accept the [Call Home agreement](#) from the web interface and Call Home must be configured and enabled before service ticket data can be synchronized with the Lenovo Support Center.

Technical assistance

If you run into problems and need technical assistance with Lenovo XClarity One, you can contact XClarity One support using the [Contact Us webpage](#).

Chapter 15. Troubleshooting and resolving problems

Use this information to resolve issues that might occur with Lenovo XClarity One or with resources that are managed by XClarity One.

Troubleshooting Organization issues

Use this information to troubleshoot issues with organizations.

Cannot access an organization

If you cannot access an organization, your user account might be disabled, or the organization might be disabled.

- Contact your organization owner or user administrator.
- If they cannot determine the cause or correct the issue, contact Lenovo Support for assistance.

Troubleshooting management-hub issues

Use this information to troubleshoot issues with a management hub.

Cannot connect to a management hub

Lenovo XClarity Management Hub 2.0 regularly checks the connectivity status for each management hub. If the XClarity One portal cannot connect to a management hub, the connectivity status for that hub changes to Offline.

- Ensure that the management hub is supported by XClarity One (see [Hardware and software requirements for XClarity Management Hub 2.0](#) in the XClarity One online documentation).
- Check the event log for any network events, and resolve the issues, if any.
- Ensure that the network hardware is functioning correctly for the connection path to the management hub.
- Ensure that the correct switch and firewall ports are enabled for the management hub. For information about required ports, see [Configuring the management hub network](#) in the XClarity One online documentation).
- Ensure that the management hub has a valid network configuration by verifying that the IP address is valid for the network. You can also ping the management hub to test if it is visible on the network.
- Ensure that the registration key that was generated by management hub is installed in XClarity One, and ensure that the registration key was generated by XClarity One is installed in management hub. If the registration key is not valid, generated and install a new key (see [Connecting the management hub to XClarity One](#) in the XClarity One online documentation).

If the management hub encountered an error while attempting to install the registration key, contact Lenovo Support for assistance.

- If the management hub's server certificate is signed by an external certificate authority, ensure that the subject alternative names include the fully-qualified domain name (FQDN) or IP address of the management hub, and the subject name be set to the FQDN of the management hub.
- Collect service data for the unresponsive management hub using the **XClarity Management Hub 2.0 Service Support Center** portal (see [Management-hub service data](#) in the XClarity One online documentation).
- Attempt to re-manage the hub from the XClarity One portal.

Sudden connectivity loss to a management hub

XClarity One regularly checks the connectivity status for each management hub. If XClarity One cannot connect to a management hub, the connectivity status for that hub changes to Offline.

Connectivity issues are typically related to a network problem.

- Check the event log for any network events, and resolve the issues, if any.
- Ensure that the network hardware is functioning correctly for the connection path to the device.
- Restart the management hub.

Troubleshooting device issues

Use this information to troubleshoot issues with device management, inventory, and health.

Cannot manage a device

Use the information in this topic to troubleshoot issues when managing devices.

- ThinkSystem V4 devices

Ensure that the LDAP setting on the XCC is set to **LocalOnly** before attempting to manage ThinkSystem V4 devices.

When managing a new device, Lenovo XClarity Management Hub 2.0 uses the account and credential that you provide to create a new local user account, which is used to manage the device. For ThinkSystem V4 devices, if the XCC3 is configured to use an LDAP settings other than **LocalOnly**, the creation of new user account fails and therefore the device-management process fails.

Sudden connectivity loss to a device

Lenovo XClarity Management Hub 2.0 checks the connectivity status for each device every hour. If the management hub cannot connect to a device, the connectivity status for that device changes to Offline.

Connectivity issues are typically related to a network problem.

- Check the event log for any network events, and resolve the issues, if any.
- Ensure that the network hardware is functioning correctly for the connection path to the device.
- Ensure that the correct switch and firewall ports are enabled for the device. For information about required ports, see [Configuring the management hub network](#) in the XClarity One online documentation.
- Ensure that the device has a valid network configuration by logging in directly to the device and verifying that the IP address is valid for the network. You can also ping the device to test if it is visible on the network.
- Attempt to re-manage the device using the current management hub or another management hub.
- For managed ThinkSystem V4 servers running BMC firmware from November 2024, the servers will go offline if you change the server's IP address. Upgrade to BMC firmware December 2024 or later and managed the server again.

Troubleshooting firmware-update issues

Use this information to troubleshoot issues with firmware updates.

Cannot deploy firmware

Use this information to troubleshoot issues when deploying firmware updates.

- Unable to deploy a firmware updates for Lenovo Boot Device (M.2/U.2) firmware component for the ThinkSystem M.2 with Mirroring Enablement Kit.

This is a current limitation. It is recommended that you unmanage any devices that have this component.

Troubleshooting template issues

Use this information to troubleshoot issues with creating and deploying templates.

Cannot create or edit a template

Use this information to troubleshoot issues with creating and editing templates.

- Unable to create or edit template for that includes firmware updates for Lenovo Boot Device (M.2/U.2) firmware component for the ThinkSystem M.2 with Mirroring Enablement Kit.

This is a current limitation. It is recommended that you unmanage any devices that have this component.