Lenovo XClarity One
Getting Started 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)

Contents

Summary of changes

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

For information about changes in earlier releases, see What's new in the in the XClarity One online documentation.

Additional hardware support

The following hardware is supported by Lenovo XClarity Management Hub 2.0.

- ThinkAgile HX360 V2 (7DJD)
- ThinkAgile HX630 V4 (7DG3)
- ThinkAgile HX650 V4 (7DG4)
- ThinkAgile HX650a V4 (7DG4)
- ThinkAgile MX450 (7DG7)
- ThinkAgile MX630 V4 (7DFG)
- ThinkAgile MX650 V4 (7DFH)
- ThinkAgile MX455 V3 (7DGP)
- ThinkAgile MX650 V3 (7DKB)
- ThinkAgile MX650a V4 (7DFH)
- ThinkAgile VX630 V4 (7DG5)
- ThinkAgile VX650 V4 (7DG6)
- ThinkAgile VX650a V4 (7DG6)
- ThinkEdge SE100 (7DGR)
- ThinkSystem SC750 V4 (7DDJ)
- ThinkSystem SR630 V4 (7DGA, 7DGB, 7DG8, 7DG9, 7DLM)
- ThinkSystem SR650 V4 (7DGC, 7DGD, 6DGE, 7DGF, 7DLN)
- ThinkSystem SR650a V4 (7DGC, 7DGD, 6DGE, 7DGF, 7DLN)
- ThinkSystem SR680a V3 (7DM9)

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 considerations from the XClarity Management Hub 2.0 Support for Servers webpage.

Terms of use changes

Changes were made to the Lenovo XClarity One Terms of Use, **Changes to the Terms** section. At a glance, here's what this update means for you. If you have any further questions regarding the updates to our terms, please do not hesitate to reach out to Lenovo Customer Support.

- **Introduce the On-Premises Version**. For the sake of clarity, we made changes to naming convention of the XClarity One set of products, now referred to as "Platform" as well as introduced the new on-premises version of the Platform which can be installed as a virtual machine in your local datacenter.
- **Grant of License**. We made changes to the language to clarify existing commitments.
- **Lenovo and your responsibilities**. We made changes to the language to introduce new responsibilities in relation to your use of the on-premises version of the Platform as well as clarified existing commitments.
- **Data Collection & Use by Lenovo**. We updated the language to make the data processing activities clearer in relation to the use of the on-premises version.
- **Artificial Intelligence**. We clarified existing commitments and how these apply in relation to the on-premises version and updated the language to reflect how Lenovo may use AI and analytics.
- **Other changes**. We made minor changes to the language to make it easier to understand what to expect from the Platform as you use our Services, mainly in relation to the use of the on-premises version.

These new terms go into effect on **August 5, 2025**. When logging into the Platform for the first time after the changes are in effect, you are prompted to review and accept the new terms. If you do not agree with the new terms, you will not be able to use the using XClarity One Platform. If we do not hear from you, we assume you agreed to the terms and want to keep using Platform as usual.

If you use XClarity One Platform to manage an account for someone else, please take some time to talk to them and inform them about these changes.

Software enhancements

This version supports the following planning or installation enhancements to the management software.

For a list of vulnerabilities that were fixed in this release, see the online documentation.

Function	Description
General	You can install XClarity One v1.0 as a virtual machine in your local datacenter. It includes the same infrastructure and management functions that you have when using XClarity One in the cloud (see Setting up XClarity One as a local VM).
Organizations	If you purchased licenses before requesting an organization, the organization request is approved immediately, and the licenses are automatically applied to the organization (see Requesting a new organization).

Chapter 1. Getting started

You can install and configure Lenovo XClarity One as a virtual machine in your local datacenter. Note that some functions are available not available when deployed as a local virtual machine.

Procedure

Complete the following steps to get started using XClarity One.

1. Purchase licenses for each managed device, based on the functions you want to use.
2. Set up XClarity One, either in the cloud or as a virtual machine in your local datacenter.
3. Set up and connect the management hubs to XClarity One.
4. Discover and manage devices.

Chapter 2. Acquiring 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

Chapter 3. Setting up XClarity One in the cloud

Use this information to set up your datacenter to use Lenovo XClarity One in the cloud.

Procedure

Complete the following steps to set up XClarity One.

1. Request a new organization.
2. Sign in to the XClarity One portal.
3. Create additional users.
4. Configure automatic problem notification (Call Home).

Requesting a new organization

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

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 are a vendor that provides solutions and services to other companies, you can contact XClarity One support using the Contact Us webpage to add the service-provider flag to your organization. *Service-provider organizations* can have users with the *service agent* flag enabled. The service-agent users can then be added to organizations for the companies that they serve. Service-agent users are the only users that are not required to be in the same email domain as the organization owner.

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.

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.

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.

Signing in to the XClarity One cloud portal

You can sign in to the Lenovo XClarity One portal (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.

Adding users

The user that requested the organization is designated as the *organization owner* and can manage users, management hubs, and devices, and configure organization-wide settings. Each organization requires at least one organization owner; however, at least two owners is highly recommended for redundancy and security.

Consider adding at least one more organization owner and other users with more limited privileges.

Add local users

To add local users to the portal, click **Overview** in the context menu from the **Organization management** view. Then, click the **Add** icon (+) in the **User** panel.

An email is sent to each new user to invite them to the organization with a link to get started signing in to the Lenovo XClarity One portal.

For information about roles that can be assigned to users, see Users in the XClarity One online documentation.

Add corporate users through an external identity provider

You can set up XClarity One to use 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.

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.

For more information, see External identity provider in the XClarity One online documentation.

Configuring 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.

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.

Chapter 4. Setting up XClarity One as a local VM

You can install and configure Lenovo XClarity One as a virtual machine in your local datacenter. It includes the same infrastructure and management functions that you have when using XClarity One in the cloud.

Complete the following to install and configure XClarity One as a virtual machine.

1. Review the hardware and software prerequisites to ensure that you have what you need to get started.
2. Install XClarity One on a local system.
3. Launch the setup wizard to configure essential settings.
4. Sign in to the XClarity One portal and accept the end-user license agreement.
5. Complete the portal configuration. For more information, see Portal configuration and management in the XClarity One online documentation).

Hardware and software requirements for XClarity One virtual machine

XClarity One runs as a virtual appliance on a host system that is installed locally in your datacenter. The following requirements must be met.

Host requirements

Host environment

The following hypervisors are supported for running XClarity One as a virtual appliance.

- VMware ESXi 8.0 or later (.ova)

Hardware requirements

The following table lists the *minimum recommended* configurations for the XClarity One virtual appliance based on the number of managed devices. Depending on your environment and use of provisioning functions (such as firmware updates and device settings), additional resources might be needed for optimal performance.

- 8 virtual processor cores
- 16 GB memory
- 768 GB storage, across two attached disks.
  - 256 GB minimum for the virtual appliance (disk 0)
  - 512 GB minimum for the repository (disk 1)

Software requirements

XClarity One requires the following software.

- **Lenovo XClarity Management Hub 2.0**

  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 communicate directly with the XClarity One portal and managed device. Managed devices communicate only with the management hubs. They cannot communicate directly with XClarity One portal.

  Attention:

  - When used in conjunction with XClarity One in the cloud, XClarity Management Hub 2.0 supports a maximum of **5,000** devices.
  - When used in conjunction with XClarity One as a local VM, XClarity Management Hub 2.0 supports a maximum of **1,000** devices.

- **NTP server**

  A Network Time Protocol (NTP) server is required to ensure that timestamps for all events and alerts that are received from managed devices are synchronized with XClarity One. Ensure that the NTP server is accessible over the management network (typically the Eth0 interface).

  Consider using the host system on which XClarity One is installed as the NTP server. If you do, ensure that the host system is accessible over the management network.

- **Authentication server**

  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)

Manageable resources

XClarity One can support an unlimited number of resource managers that collectively manage a maximum of total devices.

- **Lenovo XClarity Management Hub 2.0 v1.4 and later**

  XClarity One manages and monitors devices that are under management by XClarity Management Hub 2.0 Each XClarity Management Hub 2.0 instance can manage up to 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 considerations from the XClarity Management Hub 2.0 Support for Servers webpage.

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

Web browsers

The XClarity One web interface works with the following web browsers.
- Chrome 115 or later
- Firefox ESR 102.12 or later
- Microsoft Edge 115 or later
- Safari 16.6 or later

Installing XClarity One as a virtual machine

Follow these steps to install XClarity One as a virtual machine on a local system.

Before you begin

Ensure that you have reviewed the prerequisites, including hardware requirements and recommendations, for XClarity One (see Hardware and software requirements for XClarity One virtual machine).

You can set up XClarity One on any device that meets the requirements, including a managed server. If you use a managed server for the virtual-machine host:

- Ensure that the host server is set to automatically power on.
- Do not use the XClarity One portal to apply firmware updates to the host server. Even when only some firmware is applied with immediate activation, XClarity One forces the host server to restart, which would make XClarity One unavailable to complete the updates on the host system.
- By default, XClarity One uses gateway **192.168.255.1** for its internal network (CNI).
- By default, XClarity One uses subnet **192.168.255.0/24** for its internal network (CNI).

About this task

You can assign the virtual-appliance IP address using a static IP address on the eth0 port during configuration.

If you do not assign the IP address during configuration, IP settings are assigned using Dynamic Host Configuration Protocol (DHCP) by default when you initially start the virtual appliance. You can configure the XClarity One IP settings when you initially start the virtual appliance. Ensure that you have the required IP information before starting. You have a maximum of 60 seconds to enter settings at each prompt.

- For static IPv4 settings, you can change the IP address, subnet mask, gateway IP address, DNS 1 IP address (optional), and DNS 2 IP address (optional).
- For DHCP settings, you can change the primary and loopback interface settings (auto lo, iface lo inet loopback, auto eth0, and iface eth0 inet dhcp).

Attention: Changing the IP address of the XClarity One virtual-appliance after it is up and running will cause connectivity issues with the management hubs and managed devices. If you need to change the IP address, disconnect all management hubs from the portal before changing the IP address. After the IP address change is complete, reconnect the management hubs. For more information about setting IP addresses, see Portal network in the XClarity One online documentation.

Procedure

To install the XClarity One virtual appliance, complete the following steps.

Step 1. Download the XClarity One image to a client workstation from the XClarity One downloads webpage.

Step 2. Install and configure the virtual appliance on the host system.

- **For ESXi using VMware ESXi Host Client**
  1. Connect to the host through ESXi Host Client.
  2. Right-click **Virtual Machines → Create/Register VM → Deploy a virtual machine from an OVF or OVA file**.
  3. Complete each step in the VM creation wizard. Keep the following considerations in mind as you progress through the wizard.

- **OVF and VMDK files**. Choose a unique virtual machine name, and select the OVA file.
- **Storage**. Choose a datastore that has at least 768 GB storage available.
- **Deployment Options**. Specify the resources available to this virtual machine.
  - Specify 8 virtual processor cores.
  - Specify 16 GB memory.
  - Choose the disk format that meets the needs of your organization. Select **Thin Provision** if you are unsure.
- **Additional Settings**. Optionally update the network configuration for the virtual-appliance.
  - For the static IPv4 network, specify the IP address, netmask, gateway, and DNS1/DNS2.
  - For the CNI interface, specify the CNI subnet and gateway.

- **For ESXi using VMware vCenter Server**
  1. Connect to the host through VMware vCenter Server.
  2. Under **Hosts and groups**, right-click the host, and click **Deploy OVF Template**.
  3. Complete each step in the VM creation wizard. Keep the following considerations in mind as you progress through the wizard.
     - **OVF template**. Select an OVF template from remote URL or local file system.
     - **Name and folder**. Choose a unique name and select a location for the virtual machine.
     - **Compute resource**. Select the destination compute resource for this operation. Confirm “Compatibility checks succeeded.”
     - **Review details**. Verify template information, including publisher, product , vendor, and download size.
     - **Configuration**.
       - Specify 8 virtual processor cores.
       - Specify 16 GB memory.
     - **Storage**. Choose a datastore that has at least 768 GB storage available.
     - **Networks**. Select a destination network for each source network.
     - **Customize template**. Optionally update the network configuration for the virtual-appliance.
       - For the static IPv4 network, specify the IP address, netmask, gateway, and DNS1/DNS2.
       - For the CNI interface, specify the CNI subnet and gateway.
  4. If you plan to set a static IPv4 address during the deployment process, *do not* select the option to power on the virtual machine automatically after deployment. Instead, in the **Customize template** step, fill in all required IPv4 network information, including the **IP address**, **netmask**, **gateway**, and **DNS1/DNS2**.

     After the deployment is complete, follow the following steps **before powering on** the virtual appliance.

     a. Select the VM in the Inventory.

     b. Click **Configure → vApp**, and then select **Enable vApp Options**.

     c. After it is enabled, click **Edit vApp Options**.

     d. On the **IP Allocation** tab, select **OVF environment** for the IP allocation scheme.

     e. On the **OVF Details** tab, select **VMware Tools** for the **OVF environment transport**.

Step 3. Power on the virtual appliance.

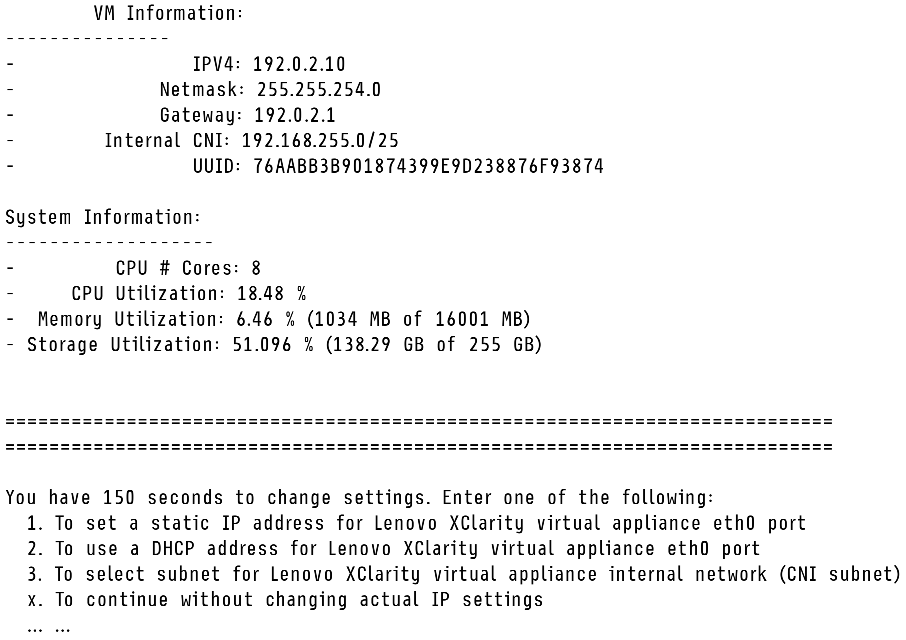
When the virtual appliance is started, the IPv4 address that was assigned by DHCP is listed for the eth0 network interface, as shown in the example below.

The eth0 management port uses a DHCP IP address by default. At the end of the boot process, you can choose to set a static IP address for the eth0 management port by entering `1` 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.

Important:

- If you specify invalid values when changing an option, an error is returned. You have up to four attempts to enter valid values.
- When changing the static IP address settings, you have a maximum of 60 seconds to enter the new settings. Ensure that you have the required IP information before continuing (IPv4 address, subnet mask, and gateway IP address).
- If you change the IP address settings from the console, XClarity One is restarted to apply the new settings.
- By default, XClarity One uses gateway **192.168.255.1** for its internal network (CNI).
- By default, XClarity One uses subnet **192.168.255.0/24** for its internal network (CNI).

After powering on the XClarity One virtual appliance, the following console output is displayed.



```
        VM Information:
---------------
-                IPV4: 192.0.2.10
-             Netmask: 255.255.254.0
-             Gateway: 192.0.2.1
-        Internal CNI: 192.168.255.0/25
-                UUID: 76AABB3B901874399E9D238876F93874

System Information:
-------------------
-         CPU # Cores: 8
-     CPU Utilization: 18.48 %
-  Memory Utilization: 6.46 % (1034 MB of 16001 MB)
- Storage Utilization: 51.096 % (138.29 GB of 255 GB)


===========================================================================
===========================================================================

You have 150 seconds to change settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  3. To select subnet for Lenovo XClarity virtual appliance internal network (CNI subnet)
  x. To continue without changing actual IP settings
  … …
```

Step 4. Optional: Configure the virtual-appliance IP settings. If you do not make a selection within the specified time or if you enter `x`, the initial startup continues using the IP settings that are assigned by default.

- **Assign static IP addresses for the eth0 port**. Enter `1`, and then follow the prompts to change the settings.
- **Assign new IP addresses for the eth0 port using DHCP**. Enter `2`, and then follow the prompts to change the settings.
- **Select the subnet for the virtual appliance internal network**. Enter `3`, and then follow the prompts to change the settings.

Important: If you specify invalid values, an error is returned. You have up to four attempts to enter valid values.

Step 5. Sign in and configure XClarity One (see Configuring essential portal settings).

Configuring essential portal settings

When running XClarity One as a virtual machine and you access the portal for the first time, you need to configure essential settings through the setup wizard. You can launch the XClarity One portal from any computer that has network connectivity to the virtual-machine host.

About this task

XClarity One is only accessible through a secure connection. Always 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

Procedure

Complete the following steps to initially set up XClarity One.

1. Launch the setup wizard, by pointing your browser to the IP address of the 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`
2. Follow the steps in the setup wizard to create you organization and initial user (organization owner), configure the NTP server, and import licenses.
3. Sign in, and then configure the portal by completing the following steps.
   a. Configure the network, including IP address, DNS address, and host configuration. Ensure that all required ports and firewalls are open (see Portal network in the XClarity One online documentation).
   b. **Optional**: Configure an HTTP2 web proxy (see Portal network in the XClarity One online documentation).
   c. **Optional**: Configure security certificates (see Security certificates in the XClarity One online documentation).
   d. **Optional**: Configure an external authentication server (see External identity provider in the XClarity One online documentation).

Organization and owner

Your view of Lenovo XClarity One is based on the organization that you are part of. When XClarity One is installed as a virtual machine, you can set up only a single organization during initial setup. You cannot request additional organizations.

Follow the steps in the wizard to create the organization and an initial user, which will be the 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.

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.

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.

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.

Licenses

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

If you skip this step in the setup wizard, 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. To import and apply licenses later, click **Licenses** from the context menu on the **Settings** view, and then following the instructions in the wizard to complete the import process.

Important:

- Ensure that you purchased the correct licenses for using XClarity One as a local virtual machine. For more information, see Acquiring licenses.
- Ensure that the customer number used to purchase the licenses matches the customer number for your organization.
- Ensure that the license filename does not contain parentheses.

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**

     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 **Request activation key**.

     c. Select **Input a Single Authorization Code**.

     d. Enter the 22-character authorization code, and click **Continue**.

     e. 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. Follow the steps in the XClarity One setup wizard to import the licenses.

Signing in to the XClarity One 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.

Uninstalling XClarity One

Complete these steps to uninstall a Lenovo XClarity One virtual appliance.

To uninstall a XClarity One virtual appliance, complete the following steps.

Step 1. Unmanage all management hubs that are currently managed by the XClarity One portal (see Device discovery and management in the XClarity One online documentation).

Step 2. Uninstall XClarity One, depending on the operating system.

- **ESXi using VMware vCenter Server**

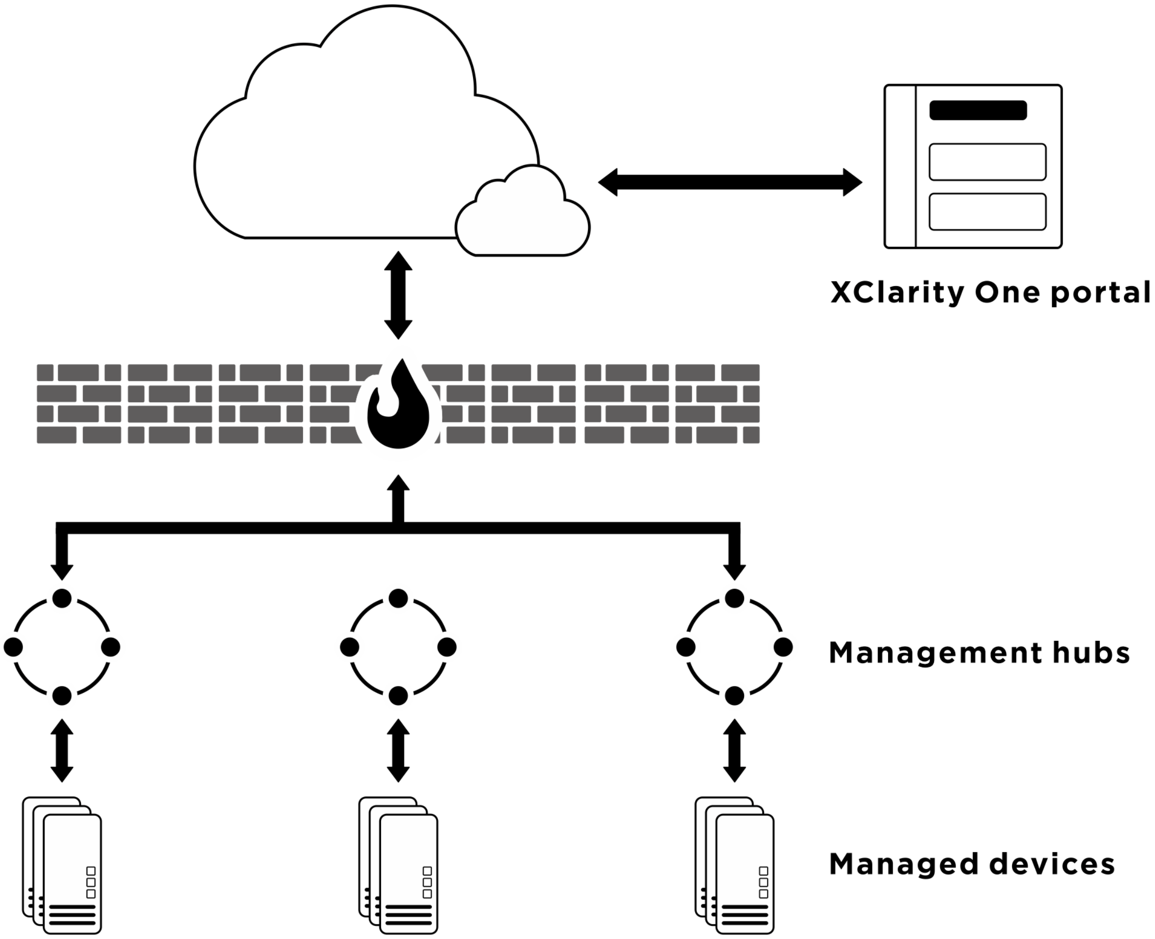
1. Connect to the host through VMware vCenter Server.
2. Right-click the XClarity One virtual machine, and click **Power → Power Off / Shut Down Guest OS**.
3. Right-click the XClarity One virtual machine again, and click **Delete from Disk**.

- **ESXi using VMware ESXi Host Client**
  1. Connect to the host through the VMware ESXi Host Client.
  2. Right-click the XClarity One virtual machine, and click **Power → Power Off**.
  3. Right-click the XClarity One virtual machine again, and click **Delete**.

Chapter 5. Setting up a management hub

Lenovo XClarity One monitors and manages devices through one or more light-weight device managers, called *management hubs*. The management hubs run as a virtual appliance *on premises* in the data centers, across multiple sites, where your devices are located, to provide in fast response times, low latency, and data security.

Lenovo XClarity Management Hub 2.0 is the supported management hub for management and provisioning of supported Lenovo devices in a secure environment.



Before installing and configuring XClarity Management Hub 2.0:

- Ensure that you have reviewed the prerequisites, including hardware requirements and recommendations, for XClarity Management Hub 2.0 (see Hardware and software requirements for XClarity Management Hub 2.0).
- Ensure that the resources that you intend to manage are supported and are at the required version levels (see Hardware and software requirements for XClarity Management Hub 2.0).

Hardware and software requirements for XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 runs as a virtual appliance on a host system that is installed locally in your datacenter. The following requirements must be met.

Host requirements

Host environment

The following hypervisors are supported for running XClarity Management Hub 2.0 as a virtual appliance.

- Microsoft Windows Server 2019 or 2022 with Hyper-V (.vhdx)
- Proxmox 8.1 (.qcow2)
- Nutanix Stack 6.5 (.qcow2)
- Ubuntu 22.04 (.qcow2)
- VMware ESXi 7.0 or 8.0 (.ova)

Hardware requirements

The following table lists the *minimum recommended* configurations for XClarity Management Hub 2.0 based on the number of managed devices. Depending on your environment(such as firmware updates, and server configuration), additional resources might be needed for optimal performance.

Number of managed devices	Processors	Memory (GB)	Storage (GB)
1 – 100	1	4 GB	320 GB
101 – 2,000	3	8 GB	320 GB
2,001 – 5,000	6	16 GB	320 GB

Software requirements

XClarity Management Hub 2.0 requires the following software.

- **Lenovo XClarity One** XClarity Management Hub 2.0 is used in conjunction with an orchestrator server, such as XClarity One, for centralized monitoring, management, provisioning, and analytics.
- **NTP server** A Network Time Protocol (NTP) server is required to ensure that timestamps for all events and alerts that are received from managed devices are synchronized with XClarity Management Hub 2.0. Ensure that the NTP server is accessible over the management network (typically the Eth0 interface).

  Consider using the host system on which XClarity Management Hub 2.0 is installed as the NTP server. If you do, ensure that the host system is accessible over the management network.

Management hubs and devices

When used in conjunction with XClarity One in the cloud, a single instance of XClarity Management Hub 2.0 supports a maximum of 5,000 devices.

When used in conjunction with XClarity One as a local VM, a single instance of XClarity Management Hub 2.0 supports a maximum of 1,000 devices.

Ensure that devices are running the latest level of firmware. Devices must be running firmware that was released January 2023 or later.

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 considerations from the XClarity Management Hub 2.0 Support for Servers webpage.

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

Web browsers

The XClarity Management Hub 2.0 web interface works with the following web browsers.

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

Installing XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 is set up as virtual appliance on a host system on premises in your local datacenter.

Before you begin

Ensure that you have reviewed the prerequisites, including hardware requirements and recommendations, for XClarity Management Hub 2.0 (see Hardware and software requirements for XClarity Management Hub 2.0).

Ensure that the devices that you intend to manage are supported and are at the required version levels (see XClarity Management Hub 2.0 Support for Servers webpage).

For optimal performance, consider installing the management hub instance in the same location as the devices that you intend to manage. If you have devices in multiple locations, you can install a management hub in each location.

You can set up XClarity Management Hub 2.0 on any device that meets the requirements, including a managed server. If you use a managed server for the management-hub host:

- Ensure that the host server is set to automatically power on.
- Do not use the XClarity One portal to apply firmware updates to the host server. Even when only some firmware is applied with immediate activation, XClarity One forces the host server to restart, which would restart the XClarity Management Hub 2.0 and make the management-hub unavailable to complete the updates on the host system. When applied with deferred activation, only some firmware is applied when the host server is restarted.

About this task

You can assign the virtual-appliance IP address using a static IP address on the eth0 port during configuration.

If you do not assign the IP address during configuration, IP settings are assigned using Dynamic Host Configuration Protocol (DHCP) by default when you initially start the virtual appliance. You can configure the XClarity Management Hub 2.0 IP settings when you initially start the virtual appliance. Ensure that you have the required IP information before starting. You have a maximum of 60 seconds to enter settings at each prompt.

Attention: Changing the IP address of the XClarity Management Hub 2.0 virtual-appliance after the management hub is up and running will cause connectivity issues with the XClarity One portal and all managed devices. If you need to change the IP address, disconnect management hub from the portal, and unmanage all managed devices before changing the IP address. After the IP address change is complete, reconnect management hub to the portal and re-manage the devices. For more information about setting IP addresses, see Configuring the management hub network.

Procedure

To install the XClarity Management Hub 2.0 virtual appliance, complete the following steps.

Step 1. Download the XClarity Management Hub 2.0 image to a client workstation from the XClarity Management Hub 2.0 downloads webpage.

1. From the XClarity One portal, click the **Organization management** view to display the **Overview** page.
2. Click the **Add** icon (⊕) on the **Management Hub** panel to display the **Add hub** dialog.
3. Click **Download XClarity Management Hub** to download the hub image to your local system.
4. Copy the image to the host system where you want to install the management hub.

You can also download the file directly from the XClarity Management Hub 2.0 downloads webpage.

Step 2. Install and configure the virtual appliance on the host system.

- **For ESXi using VMware vSphere**
  1. Connect to the host through VMware vSphere Client.
  2. Right-click **Virtual Machines → Create/Register VM → Deploy a virtual machine from an OVF or OVA file**.
  3. Complete each step in the VM creation wizard. Keep the following considerations in mind as you progress through the wizard.
     - **Appliance Name**. Choose a name that is unique to this host.
     - **Storage**. Choose a datastore that has at least 320 GB storage available.
     - **Disk Format**. Choose the disk format that meets the needs of your organization. If you are not sure which format to choose, select **Thin Provision**.
     - **Additional Settings**. Optionally update the network configuration for the virtual-appliance to set the static IP address for the eth0 interface.
- **For ESXi using VMware vCenter**
  1. Connect to the host through VMware vCenter.
  2. Under "Hosts and groups" or "VMs and Templates," right-click the host, and click **File → Deploy OVF Template**.
  3. Complete each step in the VM creation wizard. Keep the following considerations in mind as you progress through the wizard.
     - **Appliance Name**. Choose a name that is unique to this host.
     - **Storage**. Choose a datastore that has at least 320 GB storage available.
     - **Disk Format**. Choose the disk format that meets the needs of your organization. If you are not sure which format to choose, select **Thin Provision**.
     - **Customize template**. Optionally update the network configuration for the virtual-appliance to set the static IP address for the eth0 interface.
  4. If you chose to set the static IP address for the virtual appliance, complete the following steps.
     a. Select the VM in the Inventory.
     b. Click **Configure → vApp**, and then select **Enable vApp Options**.
     c. After it is enabled, select **OVF environment** for the IP allocation scheme.
     d. On the **OVF Details** tab, select “VMware Tools” for the **OVF environment transport**.
- **For Hyper-V**
  1. From the Server Manager Dashboard, click **Hyper-V**.
  2. Right-click the server, and click **Hyper-V Manager**.
  3. Under **Actions**, click **New → Virtual Machine** to start the VM creation wizard.

4. Complete each step in the virtual-appliance deployment wizard. Keep the following considerations in mind as you progress through the wizard.
   - **Specify Name and Location**. Enter a name for the new virtual machine (for example, `xc1h-v<`*version*`>`).
   - **Specify Generation**. Select **Generation 1**.
   - **Assign Memory**. Select at least **8 GB** of memory to use for this virtual machine.
   - **Configure Networking**. Choose the virtual switch that you created when you installed and configured the host.
   - **Connect Virtual Hard Disk**. Click **Use an existing virtual hard disk**, browse to the location where you downloaded the XClarity Management Hub 2.0 VHDX disk and select it (for example, `lnvgy_sw_lxmh_<`*version*`>-1.0.0_winsrvr_x86_64.vhdx`).
5. Right-click on the virtual machine that you just created, and click **Settings**.
6. Configure the number of processors to assign to the virtual machine. Select **Processor**, and specify at least 1 virtual processors to use for this virtual machine (see Hardware and software requirements for XClarity Management Hub 2.0). Click **Apply**, and then click **OK**.
7. (Optional) You can optionally set a static MAC address for each network adapter by expanding **Network Adapter** for the virtual switch, clicking **Advanced Features**, clicking **Static** under **MAC address**, and then specifying the MAC address.

- **For Proxmox Virtual Environment**
  1. Download or copy the `qcow2` image to a storage location that is attached to the Proxmox VE node using your favorite utility. The following example uses the `scp` command to copy the image from a Linux machine to the Proxmox node.
     ```
     scp lnvgy_sw_lxmh_1886-1.0.2_kvm_x86_64.qcow2 root@192.0.2.10:/var/lib/vz/template/qemu
     ```

     Note: Ensure that you are singed in using an account with administrative privileges. If not, ask your system administrator to help.
  2. From the **Server View** panel on the Proxmox VE host, select and expand the cluster, and then select the node where you want to deploy the virtual appliance.
  3. Right-click the node, and click **Create VM** to start the VM creation wizard.
  4. Complete each step in the VM creation wizard. Keep the following considerations in mind as you progress through the wizard.
     - **General**. Enter a name for the new virtual machine (for example, xchub-v<*VERSION*>), and then choose the resource pool if applicable.

       Proxmox VE allocates the VM automatically to a default resource pool that is associated with your user account.

       Node and **VM ID** are filled in automatically. You can leave them unchanged.
     - **OS**. Choose **Other** for the **Guest OS Type**, and select **Do not use any media.**
     - **System**. Choose **VirtIO SCSI** for the **SCSI Controller**, and select the **Qemu Agent**.
     - **Disk.** Choose the storage location and disk size (in GB). You can select any size as the disk is deleted in the next steps.
     - **CPU**. Choose **host** for the processor **Type**, and specify at least 1 virtual processor cores to use for this virtual machine.
     - **Memory**. Choose at least **8 GB** of memory to use for this virtual appliance
     - **Network**. Clear **Firewall**, choose **VirtIO (paravirtualized)** for the **Model**, and leave the remaining values unchanged.
  5. Click the newly created VM.

6. Click **Hardware**, click **Hard Disk**, and then click **Detach**. The disk will show as **Unused**.
7. Select the unused **Hard Disk** and **CD/DVD Drive**, and then remove them.
8. From the node console, go to the location where you downloaded the .qcow2 image, and run the following command to import the image to the VM.
   `qm importdisk` *<VM-ID> <QCOW2-DISK-NAME> <NODE-STORAGE-LOCATION>*

   Confirm that the disk was imported successfully by checking the storage location.
9. Attach the imported disk to the VM.
   - Click the newly created VM, click **Hardware**, click **Unused Disk**, and then click **Edit**.
   - Select **SCSI** for the **Bus/Device.**
   - Click **Add**.
10. Make the attached disk bootable.
    - Click **Options**, click **Boot Order**, and then click **Edit**.
    - Drag the imported disk on the 1st position.
    - Select the **Enabled** checkbox for the imported disk.
    - Click **OK**.

- **For KVM (Ubuntu and Nutanix)**
  1. Copy the qcow2 image to the host server.
  2. From the Virtual Machine Manager window, click **File → New Virtual Machine** start the VM creation wizard.
  3. Complete each step in the VM creation wizard. Keep the following considerations in mind as you progress through the wizard.
     - **Installation Method**. Select **Import existing disk image.**
     - **Disk Image**. Click **Browse Local**, find the location where you copied the cqow2 image, and select that image.
     - **OS type**. Select **Generic** for the OS type.

       If you receive a warning that the emulator might not have search permissions, click **Yes** to correct the issue.
     - **Memory**. Select at least **8 GB** of memory to use for this virtual machine
     - **CPUs**. Select at least 1 virtual processor core to use for this virtual machine.
     - **Name.** Enter a name for the new virtual machine (for example, `xc1h-v`*<VERSION>*).
     - **Network**. Configure the network settings as appropriate.

Step 3. Power on the virtual appliance.

When the virtual appliance is started, the IPv4 address that was assigned by DHCP is listed for the eth0 network interface, as shown in the example below.

The eth0 management port uses a DHCP IP address by default. At the end of the management-hub boot process, you can choose to set a static IP address for the eth0 management port by entering `1` when prompted. The prompt is available for 150 seconds, until the login prompt is displayed. To proceed to the login prompt without delay using the default settings, enter `x` at the prompt.

Important:

- If you specify invalid values when changing an option, an error is returned. You have up to four attempts to enter valid values.

- When changing the static IP address settings, you have a maximum of 60 seconds to enter the new settings. Ensure that you have the required IP information before continuing (IPv4 address, subnet mask, and gateway IP address).
- If you change the IP address settings from the console, XClarity Management Hub 2.0 is restarted to apply the new settings.
- By default, XClarity Management Hub 2.0 uses subnet **192.168.255.0/24** for its internal network (CNI). If this subnet overlaps with the host network, change the subnet to one of the following choices to avoid networking issues.
  - 10.255.252.0/24
  - 172.16.255.0/24
- XClarity Management Hub 2.0 uses gateway **192.168.255.1**.

```
        Welcome to Lenovo XClarity Management Hub 2.0  Version x.x.x

VM Information:
---------------
-                IPV4: 192.0.2.151
-             Netmask: 255.255.255.0
-             Gateway: 192.168.255.1
-        Internal CNI: 192.168.255.0/24
-                UUID: E9D28B3B901A4E399E9D7D8876F787C1

System Information:
-------------------
-         CPU # Cores: 2
-     CPU Utilization: 18.48 %
-  Memory Utilization: 33.91 % (1331 MB of 3925 MB)
- Storage Utilization: 10.36 % (24.86 GB of 240 GB)


===========================================================================
===========================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To select subnet for Lenovo XClarity virtual appliance internal network
  x. To continue without changing IP settings
  … …
```

Step 4. Log in and configure XClarity Management Hub 2.0 (see Configuring XClarity Management Hub 2.0).

Configuring XClarity Management Hub 2.0

When you access the Lenovo XClarity Management Hub 2.0 for the first time, you are prompted to create the first user, to accept the privacy statement and license agreement, and configure the management hub through the setup wizard. You can launch the XClarity Management Hub 2.0 from any computer that has network connectivity to the virtual-machine host.

About this task

XClarity Management Hub 2.0 is only accessible through a secure connection. Always 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

Important: For XClarity Management Hub 2.0 v1.0, sign in for the first time using the default username **USERID** and password **PASSW0RD** (using a zero), and then immediately change the password. After signing in, manually configure the essential settings outlined in step 4 below. There is no setup wizard in v1.0.

Procedure

Complete the following steps to initially set up XClarity Management Hub 2.0.

Step 1. 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**.

Step 2. Create the initial user account by completing the fields in the **User settings** dialog.

1. Provide your account settings, including your email address and full name.
2. Create the initial username and password.

   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.

Step 3. Read and accept the End User License Agreement.

Step 4. Complete the setup wizard to configure essential settings.

- Configure the date and time.
- Configure the network settings, including IP addresses and DNS settings.
- Create more user accounts.
- Configure the service-recovery password and password-expiration interval.
- Connect the XClarity Management Hub 2.0 instance to XClarity One.

Step 5. Optional: Set up multi-factor authentication by clicking **User settings** from the user-account drop-down menu in the upper-right corner, clicking **Set up authenticator application** , and then completing the dialog.

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

Configuring the management hub date and time

Review these considerations to help you configure the date and time for Lenovo XClarity Management Hub 2.0.

To configure network settings, click **Date and time** from the context menu on the **Administration** view.

Time zone

Choose the time zone where the management-hub host is located.

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

NTP server

You must set up at least one and up to four Network Time Protocol (NTP) servers to synchronize the timestamps between the management hub, the XClarity One portal, and all managed devices.

Attention: The management hub 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 management hub is set to synchronize to a different source than its host, you must disable the host time synchronization between the management hub 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 management hub to synchronize with the new time.

Configuring the management hub network

Review these network considerations to help you set up the network in your datacenter to use XClarity Management Hub 2.0.

To configure network settings, click **Network** on the context menu from the **Administration** view.

Network interface (eth0)

XClarity Management Hub 2.0 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 Management Hub 2.0 must be able to communicate with all devices that you intend to manage.
- The network interface must be connected to the Internet, preferably through a firewall.

IPv4 address settings

XClarity Management Hub 2.0 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:

- Network address translation (NAT), which remaps one IP address space into another, is not supported.
- Changing the IP address of the XClarity Management Hub 2.0 virtual-appliance after the management hub is up and running will cause connectivity issues with the XClarity One portal and all managed devices. If you need to change the IP address, disconnect management hub from the portal, and unmanage all managed devices before changing the IP address. After the IP address change is complete, reconnect management hub to the portal and re-manage the devices.
- 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 Management Hub 2.0 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.

Web proxy settings

You can optionally configure Lenovo XClarity Management Hub 2.0 use an HTTP2 web proxy for outbound communication between the management hub and the portal, Lenovo support websites, and other external services when direct access to the Internet is not available.

Important:

- Ensure that you use HTTP2
- Ensure that the proxy server is set up as a non-terminating proxy.
- Ensure that the proxy server is set up as a forwarding proxy.
- Ensure that load balancers are configured to keep sessions with one proxy server and not switch between them.

Firewalls

No *inbound* firewall rules needed.

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

DNS name	Ports	Proto-cols	Description
xclarityone.lenovo.com	443	HTTPS	Used by the management hub to connect to the XClarity One portal. This is used for both the WebSocket (continuous) and the REST API (on demand) connections.
xclarityone.lenovo.com	443	HTTPS	Used by the management hub connect to the identity provider in the XClarity One portal
support.lenovo.com	443	HTTPS	Used by the management hub to firmware updates on the managed devices

Open ports

You can optionally configure Lenovo XClarity Management Hub 2.0 use a web proxy for communication between the portal, Lenovo support websites, and other external services instead of direct access through the Internet.

If devices are behind a firewall and if you intend to manage those devices from a management hub that is outside of that firewall, you must ensure that all ports involved with communications between the management hub and the baseboard management controller in each device are open.

Service or component	Outbound (ports open to external systems)	Inbound (ports open on target devices)
XClarity Management Hub 2.0	• 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**	• HTTPS - TCP on port **443** • SSDP - UDP on ports **32768-65535**
ThinkSystem and ThinkAgile servers	• SFTP - TCP on port **115** • HTTPS – TCP on port **443** • SSDP discovery – UDP on port **1900** • Firmware updates - TCP on port **6990**	• HTTPS – TCP on port **443**

Adding management hub users

It is recommended that you create at least two user accounts for XClarity Management Hub 2.0.

To add users, click **Users** from the context menu on the **Security** view, and then click the **Add** icon (+) on the **Users** panel.

Usernames

You can specify 2 – 32 characters, including alphanumeric + . - _ characters.

The name is case insensitive and is saved in lowercase.

Passwords

Passwords expire after 90 days.

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.

Setting the service-recovery password

If Lenovo XClarity Management Hub 2.0 becomes unresponsive and cannot be recovered, you can collect service data for that management-hub instance. The service-recovery password is used to collect service data.

The service-recovery password and the password-expiration interval are set during initial configuration through the setup wizard. By default, the password must be reset every 90 days.

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.

Connecting the management hub to XClarity One

After you connect (register) Lenovo XClarity Management Hub 2.0 to the Lenovo XClarity One portal, you can begin managing and monitoring your devices.

▶ XClarity One: Connecting a hub

Ensure that the XClarity Management Hub 2.0 is reachable on the network from XClarity One and that XClarity One is reachable on the network from XClarity Management Hub 2.0.

Connecting a management hub

To connect the management hub to a portal, complete the following steps.

1. Create the management-hub registration key.
   a. From XClarity Management Hub 2.0, click the **Connections** view. Click **Connect to a portal** to open a wizard.
   b. Click **Copy to Clipboard** to copy the management-hub registration key.
   c. Click **Next** to display the **Portal registration key** page. *Do not close the wizard.*
2. Add the management-hub registration key to the XClarity One.
   a. From the XClarity One portal, click the **Organization management** view.
   b. Click the **Add** icon (⊕) on the **Management Hub** page to display the **Add hub** dialog.
   c. Provide a custom name and location, and paste the hub registration key.
   d. Click **Add hub**. The **Token** dialog is displayed.
   e. Click **Copy to Clipboard** to copy the portal registration key, and then close the dialog.
3. Add the portal registration key to the management hub.
   a. From XClarity Management Hub 2.0, paste the portal registration key in the **Portal registration key** page.
   b. Click **Connect** to complete the connection process.

Disconnecting a management hub

If you disconnect this management hub, all data for the hub is removed from the XClarity One portal; however, device and system data is retained in the management hub. The management hub continues to manage devices and receive data from those devices. If you reconnect this management hub to the XClarity One portal, these devices show up as managed devices.

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 6. Discovering and managing devices

Lenovo XClarity One discovers and manages supported devices through 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 unmanaged 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.

Chapter 7. 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 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.