



Lenovo XClarity Management Hub Planning and Installation Guide



Version 2.0.0

Note

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

First Edition (March 2023)

© Copyright Lenovo 2022.

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

Contents

Contents	i	Configuring the XClarity Management Hub date and time	13
Chapter 1. Planning for Lenovo XClarity Management Hub	1	Managing Lenovo XClarity Management Hub security certificates	15
Supported hardware and software	1	Regenerating the self-signed XClarity Management Hub server certificate	16
Firewalls and proxy servers	2	Installing a trusted, externally-signed XClarity Management Hub server certificate	18
Port availability	2	Importing the server certificate into a web browser	20
Network considerations.	3	Collecting service data for XClarity Management Hub	21
High-Availability considerations	4	Chapter 3. Updating XClarity Orchestrator	23
Chapter 2. Configuring the XClarity Management Hub	7	Chapter 4. Uninstalling the XClarity Management Hub	29
Logging in to the XClarity Management Hub web interface.	7		
Connecting Lenovo XClarity Management Hub to XClarity Orchestrator.	9		
Creating Lenovo XClarity Management Hub user accounts	11		
Configuring XClarity Management Hub network settings	12		

Chapter 1. Planning for Lenovo XClarity Management Hub

Review the following considerations and prerequisites to help you plan for the installation of Lenovo XClarity Management Hub.

Supported hardware and software

Ensure that your environment meets the hardware and software requirements for Lenovo XClarity Management Hub.

Host systems

Hypervisor requirements

The following hypervisors are supported for installing XClarity Management Hub.

- VMware ESXi 7.0, U1, U2, and U3
- VMware ESXi 6.7, U1, U2¹, and U3

For VMware ESXi, the virtual appliance is an OVF template.

Important:

- For VMware ESXi 6.7 U2, you must use the ISO image VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso or later.

Hardware requirements

The following table lists the *minimum recommended* configurations for XClarity Management Hub based on the number of managed edge-client devices. Depending on your environment, additional resources might be needed for optimal performance.

Number of managed edge-client devices	Processors	Memory	Storage
0 - 100 devices	6	32GB	340 GB
100 - 200 devices	8	34 GB	340 GB
200 - 400 devices	10	36 GB	340 GB
400 - 600 devices	12	40 GB	340 GB
600 - 800 devices	14	44 GB	340 GB
800 – 1,000 devices	16	48 GB	340 GB

1. This is the minimum amount of storage for use by the XClarity Management Hub virtual appliance, as an SSD datastore.

Software requirements

XClarity Management Hub requires the following software.

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

Manageable devices

XClarity Management Hub can manage, monitor, and provision a maximum of 10,000 ThinkEdge Client devices (without baseboard management controllers).

You can find a complete list of supported ThinkEdge Client devices and options (such as I/O, DIMM, and storage adapters), minimum required firmware levels, and limitations considerations from the [Lenovo XClarity Support for ThinkAgile, ThinkEdge, ThinkSystem, System x, Converged HX, and NeXtScale rack and tower 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 web interface works with the following web browsers.

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

Firewalls and proxy servers

Several ports must be available, depending on how the firewalls are implemented in your environment. Ensure that the firewalls are configured to allow Internet access or use a proxy server.

Port availability

When using Lenovo XClarity Management Hub to manage devices through Lenovo XClarity Orchestrator, certain ports must be open to facilitate communication. If the required ports are blocked or used by another process, some XClarity Orchestrator functions might not perform correctly.

Note: *Inbound* traffic flows from managed devices and external systems to XClarity Management Hub, so ports must be open on the XClarity Management Hub appliance. *Outbound* traffic flows from XClarity Management Hub to managed devices.

- [“Access to the XClarity Management Hub server” on page 2](#)
- [“Access between the Lenovo XClarity Management Hub and managed devices” on page 3](#)

Access to the XClarity Management Hub server

If XClarity Management Hub and all manageable devices are behind a firewall, and you intend to access those devices from a browser that is outside of the firewall, you must ensure that XClarity Management Hub ports are open.

XClarity Management Hub server listens on and responds through the ports that are listed in the following table.

Notes:

- XClarity Management Hub is a RESTful application that communicates securely over TCP on port 443.
- Lenovo XClarity Management Hub can be optionally configured to make outbound connections to external services. These connections might also require access to a domain name service (DNS) server on TCP or UDP port 53 to resolve external server names.

Communication	Lenovo XClarity Management Hub appliance
Outbound (ports open on external systems)	<ul style="list-style-type: none"> DNS – TCP/UDP on port 53
Inbound (ports open on the Lenovo XClarity Management Hub appliance)	<ul style="list-style-type: none"> HTTPS – TCP on port 443 MQTT – TCP on port 8883

Access between the Lenovo XClarity Management Hub and managed devices

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

- **Devices**

Communication	ThinkEdge Client devices
Outbound (ports open on external systems)	Not applicable
Inbound (ports open on the Lenovo XClarity Management Hub appliance)	<ul style="list-style-type: none"> – MQTT – TCP on port 8883

Network considerations

You can configure Lenovo XClarity Management Hub to use a single network interface (eth0) or two separate network interfaces (eth0 and eth1) for communication.

Lenovo XClarity Management Hub communicates over the following networks.

- The *management network* is used for communications between Lenovo XClarity Management Hub and managed devices.
- The *data network* is used for communications between the operating systems that are installed on the servers and the company intranet, the Internet, or both.

Single interface (eth0)

When using a single network interface (eth0), management communications, data communications, and operating-system deployment occur over the same network.

When you set up Lenovo XClarity Management Hub, define the eth0 network interface using the following considerations.

- The network interface must be configured to support device discovery and management (including firmware updates). Lenovo XClarity Management Hub must be able to communicate with all devices that it will manage from the management network. Lenovo XClarity Management Hub must be able to communicate with all devices that it will manage from the network.
- To deploy OS images, the eth0 interface must have IP network connectivity to the server network interface that is used to access the host operating system.
- **Important:** Implementing a shared data and management network can cause disruptions in traffic, such as packets being dropped or management-network connectivity issues, depending on your network configuration (for example, if traffic from servers have a high priority and traffic from the management controllers have a low priority). The management network uses UDP traffic in addition TCP. UDP traffic can have a lower priority when the network traffic is high.

Two separate interfaces (eth0 and eth1)

When using two network interfaces (eth0 and eth1), you can setup the networks in as physically-separate or virtually-separate networks.

Review the following considerations when defining the eth0 and eth1 network interfaces.

- The eth0 network interface must be connected to the management network and must be configured to support device discovery and management. Lenovo XClarity Management Hub must be able to communicate with all devices that it will manage from the management network.
- The eth1 network interface can be configured to communicate with an internal data network, a public data network, or both.
- To deploy operating-system images, the eth1 network interface must have IP network connectivity to the server network interface that is used to access the host operating system.
- Functions can be performed on either network.
- For virtually-separate networks, packets from the management network and packets from the data network are sent over the same physical connection. Use VLAN tagging on all management-network data packets to keep the traffic between the two networks separated.

IP address considerations

Review the following IP address considerations before configuring the network.

- Changing the virtual-appliance IP address after XClarity Management Hub is up and running will cause connectivity issues with XClarity Orchestrator and all managed devices. If you need to change the IP address, disconnect XClarity Management Hub from XClarity Orchestrator and unmanage all managed devices before changing the IP address, and then remanage the devices and reconnect XClarity Management Hub to XClarity Orchestrator after the IP address change is complete
- Configure the devices and components in ways that minimize IP address changes. Consider using static IP addresses instead of Dynamic Host Configuration Protocol (DHCP). If DHCP is used, ensure that IP address changes are minimized, such as basing the DHCP address on a MAC address or configuring DHCP so that the lease does not expire. If the IP address of a managed device (other than a ThinkEdge Client device) changes, you must unmanage the device, and then manage it again.
- Network address translation (NAT), which remaps one IP address space into another, is not supported.
- The network interfaces must be configured with an IPv4 address to manage the following devices. IPv6 addresses are not supported.
 - ThinkServer servers
 - Lenovo Storage devices
- Managing RackSwitch devices using IPv6 link local through a data port or management port is not supported.

High-Availability considerations

To set up high availability for Lenovo XClarity Orchestrator, use the high availability features that are part of the host operating system.

VMware ESXi

In a VMware high-availability environment, multiple hosts are configured as a cluster. Shared storage is used to make the disk image of a virtual machine (VM) available to the hosts in the cluster. The VM runs on only one host at a time. When there is an issue with the VM, another instance of that VM is started on a backup host.

VMware high availability requires the following components.

- A minimum of two hosts on which ESXi is installed. These hosts become part of the VMware cluster.

- A third host on which VMware vCenter is installed.

Tip: Ensure that you install a version of VMware vCenter that is compatible with the versions of ESXi that are installed on the hosts to be used in the cluster.

VMware vCenter can be installed on one of the hosts that is used in the cluster. However, if that host is powered off or not usable, you lose access to the VMware vCenter interface as well.

- Shared storage (datastores) that can be accessed by all hosts in the cluster. You can use any type of shared storage that VMware supports. The datastore is used by VMware to determine whether a VM should fail over to a different host (heartbeating).

For details about setting up a VMware high-availability cluster, see .

Chapter 2. Configuring the XClarity Management Hub

When you access the Lenovo XClarity Management Hub for the first time, there are several steps that you must complete to initially set up the XClarity Management Hub.

Procedure

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

- Step 1. Log in to the XClarity Management Hub web interface.
- Step 2. Read and accept the license agreement.
- Step 3. Create additional user accounts.
- Step 4. Configure network access, including IP addresses for the data and management networks.
- Step 5. Configure the date and time.
- Step 6. Register the XClarity Management Hub with the orchestrator server.

Logging in to the XClarity Management Hub web interface

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

Before you begin

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

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

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

If you are configuring XClarity Management Hub remotely, you must have connectivity to the same layer 2 network. It must be accessed from a non-routed address until the initial setup is complete. Therefore, consider accessing XClarity Management Hub from another VM that has connectivity to XClarity Management Hub. For example, you can access XClarity Management Hub from another VM on the host where XClarity Management Hub is installed.

XClarity Management Hub automatically logs out user sessions after 60 minutes, regardless of activity.

Procedure

Complete the following steps to log in to the XClarity Management Hub web interface.

- Step 1. Point your browser to the XClarity Management Hub IP address.
`https://<IPv4_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 an IPv4 address in `eth0_config`, use that IPv4 address to access the XClarity Management Hub.

- If a DHCP server is set up in the same broadcast domain as XClarity Management Hub, use the IPv4 address that is displayed in the XClarity Management Hub virtual-machine console to access the XClarity Management Hub.
- If you have eth0 and eth1 networks on separate subnets, and if DHCP is used on both subnets, use the *eth1* IP address when accessing the web interface for initial setup. When the XClarity Management Hub starts for the first time, both eth0 and eth1 get a DHCP-assigned IP address, and the XClarity Management Hub default gateway is set to the DHCP-assigned gateway for *eth1*.

The XClarity Management Hub initial login page is displayed:



Step 2. Select the desired language from the **Language** drop-down list.

Note: The configuration settings and values that are provided by the managed devices might be available only in English.

Step 3. Enter your user credentials, and click **Log In**.

If you are logging in to XClarity Management Hub for the first time, enter the default credentials **USERID** and **PASSWORD** (where 0 is zero).

Step 4. Read and accept the license agreement.

Step 5. If you logged in for the first time using default credentials, you are prompted to change the password. By default, passwords must contain **8 – 256** characters and must meet the following criteria.

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

- (1) Must contain at least one uppercase alphabetic character
- (2) Must contain at least one lowercase alphabetic character
- (3) Must contain at least one number

- (4) Must contain at least one special character
- (5) Must not be the same as the user name

Step 6. If you logged in for the first time, you are prompted to choose whether to use the current self-signed certificate or to use an externally CA-signed certificate. If you choose to use an externally-signed certificate, the Server Certificate page is displayed.

Attention: The self-signed certificate is not secure. You are advised to generate and install your own externally-signed certificate.

For information about using an externally-signed certificate, see [Installing a trusted, externally-signed XClarity Management Hub server certificate](#).

After you finish

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

- Log out of the current session by clicking **Log out**. The XClarity Management Hub log in page is displayed.
- Submit ideas or provide feedback about XClarity Management Hub by clicking **Submit ideas** or **Submit feedback**.
- View the online documentation clicking **User's Guide**.
- View information about the XClarity Management Hub release by clicking **About**.
- Change the language of the user interface by clicking **Change language**. The following languages are supported.
 - English (en)
 - Simplified Chinese (zh_CN)
 - Traditional Chinese (zh_TW)
 - French (fr)
 - German (de)
 - Italian (it)
 - Japanese (ja)
 - Korean (ko)
 - Brazilian Portuguese (pt_BR)
 - Russian (ru)
 - Spanish (es)
 - Thai (th)

Connecting Lenovo XClarity Management Hub to XClarity Orchestrator

After you register (connect) Lenovo XClarity Management Hub with Lenovo XClarity Orchestrator, you can begin managing your devices.

Before you begin

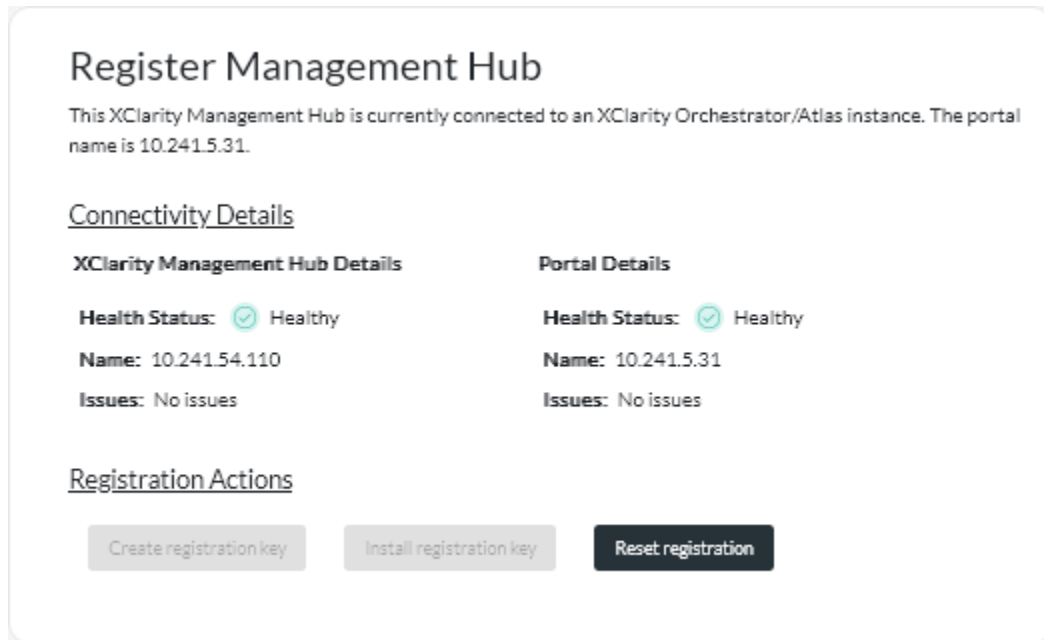
Ensure that the XClarity Management Hub is reachable on the network from XClarity Orchestrator and that XClarity Orchestrator is reachable on the network from XClarity Management Hub.

Procedure

To register XClarity Management Hub, complete the following steps.

Step 1. Create a XClarity Management Hub registration key.

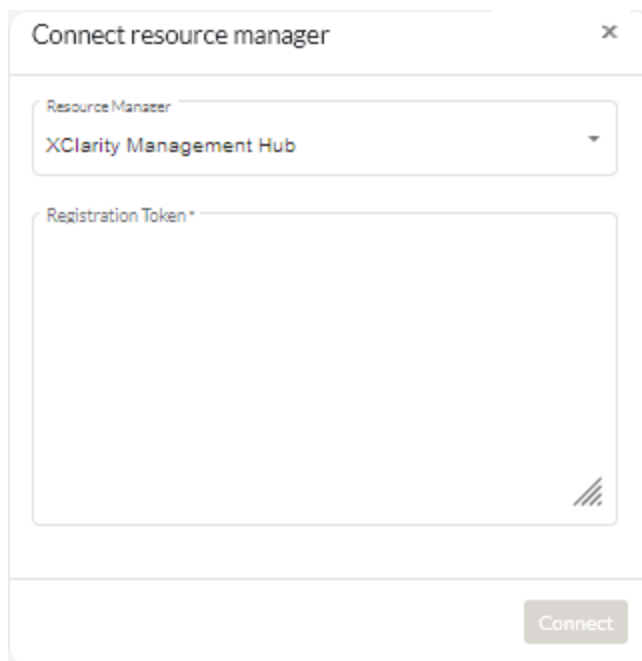
1. From the Management Hub menu bar, click **Registration** to display the Registration page.



2. Click **Create registration key**.
3. Click **Copy to Clipboard** to copy the registration key, and then close the dialog.

Step 2. Add the XClarity Management Hub registration key to XClarity Orchestrator.

1. From the XClarity Orchestrator menu bar, click **Resources** (⊕) → **Resource Managers** to display the Resource Managers card.
2. Click the **Connect** icon (⊕) to display the resource manager. The Connect resource manager dialog.



3. Select **XClarity Management Hub** as the resource manager.

4. Copy the registration key into the **Registration Token** field.
5. Click **Connect** to display the Connect Resource Manager dialog that contains the XClarity Orchestrator registration key.
6. Click **Copy to Clipboard** to copy the registration key, and then close the dialog.

- Step 3. Add the XClarity Orchestrator registration key to XClarity Management Hub.
1. From the Management Hub menu bar, click **Registration** to display the Registration page.
 2. Click **Install registration key**.
 3. Copy the registration key into the **Registration Token** field.
 4. Click **Connect**.

After you finish

- Manage devices using XClarity Management Hub (see in the XClarity Orchestrator online documentation).
- Delete the current XClarity Management Hub registration key by clicking **Reset registration**.

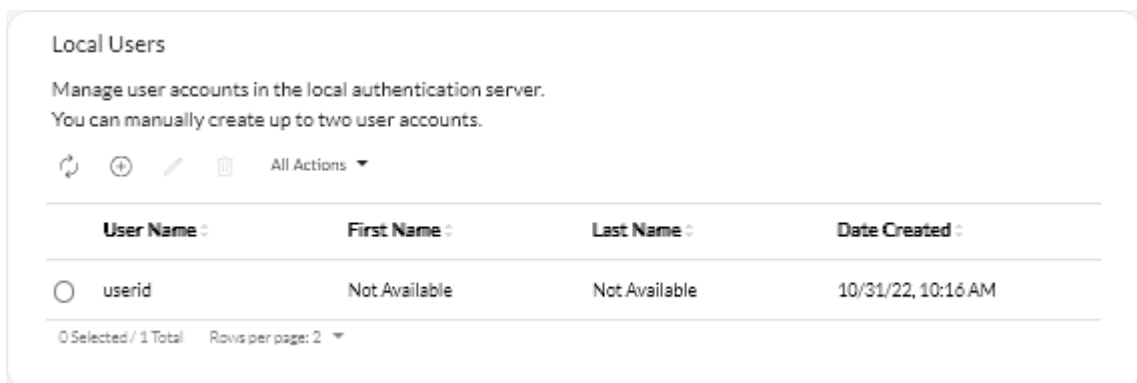
Creating Lenovo XClarity Management Hub user accounts

You can create up to 10 user accounts for Lenovo XClarity Management Hub.

Procedure

To create a user account, complete the following steps.

- Step 1. From the Lenovo XClarity Management Hub menu bar, click **Security** (⚙️) → **Local Users** to display the Local Users card.



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

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

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

Note: User names are not case sensitive.

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

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

- (1) Must contain at least one uppercase alphabetic character
- (2) Must contain at least one lowercase alphabetic character
- (3) Must contain at least one number
- (4) Must contain at least one special character
- (5) Must not be the same as the user name

Step 4. Click **Create**.

The user account is added to the table.

After you finish

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

- Modify password and properties for your user account by clicking the **Edit** icon (✎). Note that passwords do not expire.
- Delete a selected user by clicking the **Delete** icon (🗑).

Configuring XClarity Management Hub network settings

You can configure a single IPv4 network interface and Internet routing settings.

Before you begin

Review the network considerations before configuring the network (see [Network considerations](#)).

Procedure

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

- **Configure IP settings** For the eth0 interface, click the **Eth0 Interface** tab, configure applicable IPv4 address settings, and then click **Apply**.

Attention:

- Changing the virtual-appliance IP address after XClarity Management Hub is up and running will cause connectivity issues with XClarity Orchestrator and all managed devices. If you need to change the IP address, disconnect XClarity Management Hub from XClarity Orchestrator and unmanage all managed devices before changing the IP address, and then remanage the devices and reconnect XClarity Management Hub to XClarity Orchestrator after the IP address change is complete

Currently, only IPv4 addresses are supported.

- **IPv4 settings.** You can configure the IP assignment method, IPv4 address, network mask, and default gateway. For the IP assignment method, you can choose to use a statically-assigned IP address or obtain an IP address from a DHCP server. When using a static IP address, you must provide an IP address, network mask, and default gateway.

The default gateway must be a valid IP address and must use the same network mask (the same subnet) as the enabled interface (eth0).

If either interface uses DHCP to obtain an IP address, the default gateway also uses DHCP.

Eth0 interface

IPv4 Configuration

Method: Obtain IP from DHCP (dropdown)

IPv4 Network Mask: [text input]

IPv4 Address: [text input]

IPv4 Default Gateway: [text input]

Apply [button] Reset [button]

IPv6 Configuration

Method: Use stateless address... (dropdown)

IPv6 Prefix Length: [text input]

IPv6 Address: [text input]

IPv6 Default Gateway: [text input]

Apply [button] Reset [button]

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

Currently, only IPv4 addresses are supported.

You can change the IP address for the DNS server.

The fully-qualified domain name (FQDN) and hostname for the DNS server are the same as the XClarity Management Hub server and cannot be changed.

DNS Configuration

Preferred DNS address type: IPv4 IPv6

DNS Address*: 10.241.54.233

FQDN: node-63851f87.lenovo.com

Hostname: lmh

Apply [button] Reset [button]

Configuring the XClarity Management Hub date and time

You must set up at least one (and up to four) Network Time Protocol (NTP) server to synchronize the timestamps between XClarity Management Hub and all managed devices.

Before you begin

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

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

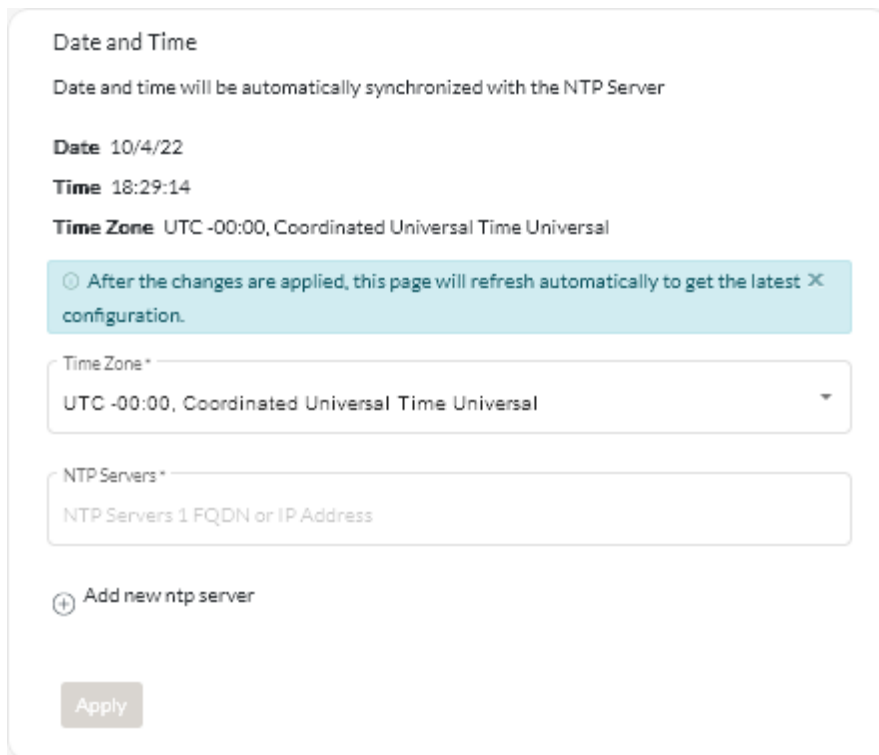
Attention: The XClarity Management Hub virtual appliance and its host must be set to synchronize to the same time source to prevent inadvertent time mis-synchronization between XClarity Management Hub and its host. Typically, the host is configured to have its virtual appliances time-sync to it. If XClarity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

- For ESXi, following instructions on the [VMware – Disabling Time Synchronization webpage](#).

Procedure

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

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



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

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

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

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

- Step 4. Click **Apply**.

Managing Lenovo XClarity Management Hub security certificates

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

Before you begin

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

About this task

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

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

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

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

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

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

Lenovo XClarity Management Hub server certificate. It automatically regenerated each time Lenovo XClarity Management Hub detects that its networking addresses (IP or DNS addresses) have changed to ensure that the certificate contains the correct addresses for the server. It can be customized and generated on demand (see).

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

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

- **OS Deploy Certificate.** A separate certificate is used by the operating-system deployment service to ensure that the operating-system installer can connect securely to deployment service during the deployment process. If the key has been compromised, you can regenerate it by restarting Lenovo XClarity Management Hub.

Regenerating the self-signed XClarity Management Hub server certificate

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

Before you begin

Attention: If you regenerate the XClarity Management Hub server certificate using a new root CA, XClarity Management Hub loses its connection to the managed devices, and you must re-manage the devices. If you regenerate the XClarity Management Hub server certificate without changing the root CA (for example, when the certificate is expired), there is no need to re-manage the devices.

About this task

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

Important: When the server certificate is modified, the management hub is restarted, and all user sessions are ended. Users must log back in to continue working in the web interface.

Procedure

To generate a self-signed XClarity Management Hub server certificate, complete the following steps.

- Step 1. From the XClarity Management Hub menu bar, click **Security** (⚙️) → **Server Certificate** to display the **Regenerate Self-Signed Server Certificate** card.

Regenerate Server Certificate

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

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

Regenerate Certificate
Save Certificate
Reset Certificate

Step 2. From the **Regenerate Self-Signed Server Certificate** card, fill in the fields for the request.

- Two-letter ISO 3166 code for the country or region of origin to associate with the certificate organization (for example, US for the United States).
- Full name of the state or province to associate with the certificate (for example, California or New Brunswick).
- Full name of the city to associate with the certificate (for example, San Jose). The length of the value cannot exceed 50 characters.
- Organization (company) to own the certificate. Typically, this is the legally incorporated name of a company. It should include any suffixes, such as Ltd., Inc., or Corp (for example, ACME International Ltd.). The length of this value cannot exceed 60 characters.
- (Optional) Organization unit to own the certificate (for example, ABC Division). The length of this value cannot exceed 60 characters.
- Common name of the certificate owner. Typically, this is the fully-qualified domain name (FQDN) or IP address of the server that uses the certificate (for example, www.domainname.com or 192.0.2.0). The length of this value cannot exceed 63 characters.

Note: Currently, this attribute has no affect the certificate.

- Date and time when the server certificate is no longer valid.

Note: Currently, these attributes have no affect the certificate.

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

Step 3. Click **Regenerate Self-Signed Server Certificate** to regenerate the self-signed certificate, and then click **Regenerate Certificate** to confirm. The management hub is restarted, and all established user sessions are ended.

Step 4. Log back in to the web browser.

After you finish

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

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

Installing a trusted, externally-signed XClarity Management Hub server certificate

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

Before you begin

Attention:

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

About this task

As a best practice, always use v3 signed certificates.

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

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

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

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

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

Procedure

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

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

1. From the XClarity Management Hub menu bar, click **Security** (🔒) → **Server Certificate** to display the Generate Certificate Signing Request card.

Generate Certificate Signing Request (CSR)

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

Country/Region* UNITED STATES	Organization* Lenovo
State/Province* NC	Organization Unit* DCG
City* Raleigh	Common Name* Generated by Lenovo Management Ecosystem

Subject Alternative Names ?

To add a new Subject Alternative Name, click +

Generate CSR File
Import Certificate

2. From the Generate Certificate Signing Request (CSR) card, fill in the fields for the request.

- Two-letter ISO 3166 code for the country or region of origin associated with the certificate organization (for example, US for the United States).
- Full name of the state or province to be associated with the certificate (for example, California or New Brunswick).
- Full name of the city to be associated with the certificate (for example, San Jose). The length of the value cannot exceed 50 characters.
- Organization (company) that is to own the certificate. Typically, this is the legal incorporate name of a company. It should include any suffixes, such as Ltd., Inc., or Corp (for example, ACME International Ltd.). The length of this value cannot exceed 60 characters.
- (Optional) Organization unit that is to own the certificate (for example, ABC Division). The length of this value cannot exceed 60 characters.
- Common name of the certificate owner. This must be the hostname of the server that is using the certificate. The length of this value cannot exceed 63 characters.

Note: Currently, this attribute has no affect the certificate.

- (Optional) Subject alternative names that are added to the X.509 "subjectAltName" extension when the CSR is generated. By default, XClarity Management Hub automatically defines subject alternative names for the CSR based on the IP address and hostname that are discovered by the network interfaces for the XClarity Management Hub guest operating system. You can customize, delete, or add to these subject alternative name values. However, the subject alternative names must have the fully-qualified domain name (FQDN) or IP address of the server, and the subject name be set to the FQDN.

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

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

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

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

Importing the server certificate into a web browser

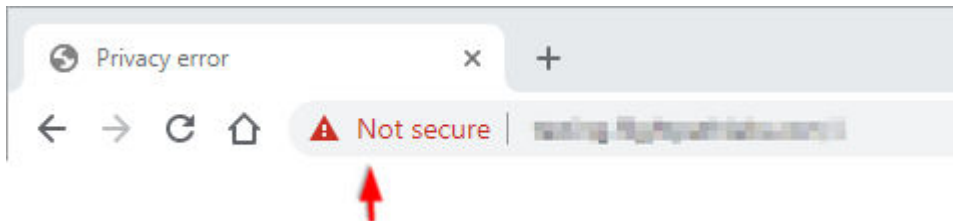
You can save a copy of the current server certificate, in PEM format, to your local system. You can then import the certificate into your web browser's list of trusted certificates or to other applications to avoid security warning messages from your web browser when you access Lenovo XClarity Management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

Procedure

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

- **Chrome**

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

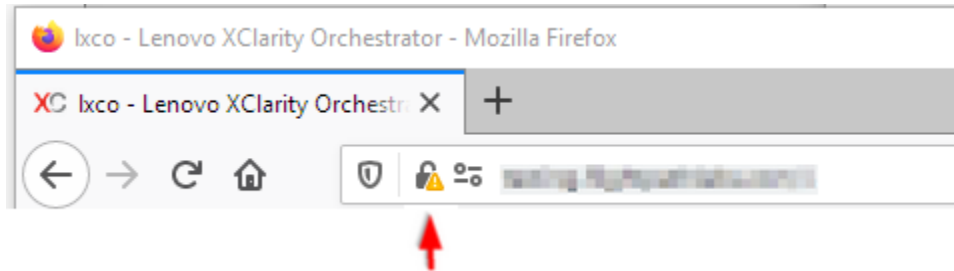


- b. Click **Certificate (invalid)** to display the Certificate dialog.
 - c. Click the **Details** tab.
 - d. Click **Copy to File** to display the Certificate Export Wizard.
 - e. Select Cryptographic Message Syntax Standard, and click **Next**.
 - f. Specify the name and location of the certificate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

- e. Click **Finish**.
- f. Close and reopen the Chrome browser, and then open XClarity Orchestrator.

- **Firefox**

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



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

Collecting service data for XClarity Management Hub

You can manually collect service data for Lenovo XClarity Management Hub and then save the information as an archive in tar.gz format to the local system. You can then send the service files to your preferred service provider to get assistance in resolving issues as they arise.

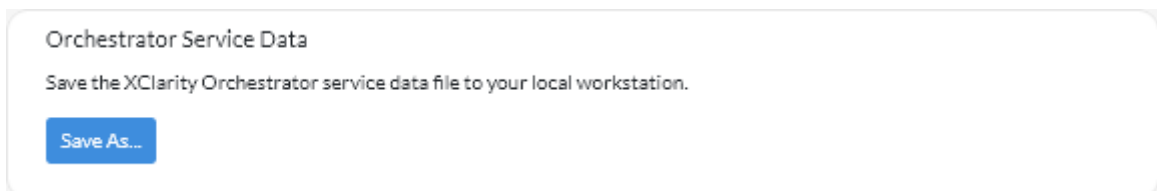
Before you begin

Ensure that web browser does not block pop-ups for the XClarity Management Hub website when downloading service data.

Procedure

To collect service data for XClarity Management Hub, complete the following steps.

- Step 1. From the XClarity Management Hub menu bar, click the **Administration (⚙️) → Service and Support**, and then click **Service Data** in the left navigation to display the Management Service Data card.



Step 2. Click **Save As** to collect service data and save the archive to the local system.

After you finish

You can also perform these related actions.

- Save one or more selected service-data archives to the local system from the Management Service Data card by clicking the **Save** icon (↓). If multiple files are selected, the files are compressed into a single .tar.gz file before downloading.
- Delete one or more selected service-data archives that are no longer needed from the Management Service Data card by clicking the **Delete** icon (🗑️), or delete all archives by clicking the **Delete All** icon (⊖).

Chapter 3. Updating XClarity Orchestrator

You can update Lenovo XClarity Orchestrator to use the latest orchestrator software.

Learn more:  [How to update XClarity Orchestrator](#)

Before you begin

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

An XClarity Orchestrator fix bundle (such as v1.4.2) can be applied only to a version of the same release (such as v1.4.0 or v1.4.1). A fix bundle contains all previous fixes (for example, v1.4.2 contains the same fixes as v1.4.1 plus additional fixes); however, a fix bundle does not contain the entire code base.

Attention: Review the following considerations before updating XClarity Orchestrator.

- **To XClarity Orchestrator v2.0** Updating to XClarity Orchestrator v2.0 requires XClarity Orchestrator v1.6. If you are not running XClarity Orchestrator v1.6, you must update to XClarity Orchestrator v1.6 before updating to XClarity Orchestrator v2.0.

The minimum storage required for the virtual appliance is a **total of 551 GB** across three attached disks. You must also attach a third disk (disk 2) with a minimum of 200 GB.

The XClarity Orchestrator virtual appliance must be powered off before adding a new hard disk.

To add a new hard disk to the virtual appliance, complete the following steps.

– **For ESXi using VMware vSphere**

1. Connect to the host through VMware vSphere Client.
2. Power off the XClarity Orchestrator virtual machine.
3. Right-click the virtual machine, and click **Edit Settings**.
4. Select **Add a new Device → Hard Disk**.
5. Change the size to 200 GB.
6. Click **OK**.
7. Power on the XClarity Orchestrator virtual machine.

– **For ESXi using VMware vCenter**

1. Connect to the host through VMware vCenter.
2. Power off the virtual machine.
3. Open the virtual machine's settings, and click **Add**.
4. Click **Hard Disk → Create a new Virtual Disk**.
5. Select **SCSI** for the disk format.
6. Configure the HDD capacity to 200 GB.
7. Click **OK**.
8. Power on the virtual machine.

– **For Microsoft Hyper-V**

1. From the Server Manager Dashboard, click **Hyper-V**.
2. Right-click the server, and click **Hyper-V Manager**.
3. Select the XClarity Orchestrator virtual machine, and click **Shut Down** in the Actions pane.
4. Click **Settings** to display the Settings dialog.
5. Select **IDE Controller 1**.
6. From the right pane, select **Hard Drive**, and then click **Add** to add a new hard disk.

7. From the right pane, select **Virtual hard disk (.vhd) file**, and then click **New** to display the New Virtual Hard Disk Wizard.
 8. Complete the wizard as prompted. Ensure that you specify a disk-drive name using .vhd format (for example, LXC0-disk3.vhd) and set the size to 200 GB.
 9. Select the XClarity Orchestrator virtual machine, and click **Start** in the Actions pane.
- **To XClarity Orchestrator v1.6.** Updating to XClarity Orchestrator v1.6 requires XClarity Orchestrator v1.5. If you are not running XClarity Orchestrator v1.5, you must update to XClarity Orchestrator v1.5 before updating to XClarity Orchestrator v1.6.
 - **To XClarity Orchestrator v1.5.** Updating to XClarity Orchestrator v1.5 requires XClarity Orchestrator v1.4. If you are not running XClarity Orchestrator v1.4, you must update to XClarity Orchestrator v1.4 before updating to XClarity Orchestrator v1.5.
 - **To XClarity Orchestrator v1.4.** Updating to XClarity Orchestrator v1.4 requires XClarity Orchestrator v1.3. If you are not running XClarity Orchestrator v1.3, you must update to XClarity Orchestrator v1.3 before updating to XClarity Orchestrator v1.4.
 - **To XClarity Orchestrator v1.3**
 - Updating to XClarity Orchestrator v1.3 might take two hours or more to complete. To determine whether the update is complete, click **Maintenance → Orchestrator Server Updates**, and verify that the new release is listed and that the Applied Status is no longer “Applying”.
 - **Attention:** Before updating XClarity Orchestrator to v1.3, ensure that the XClarity Orchestrator virtual appliance hostname is **lxco** and no domain name set on the DNS Configuration card on the **Administration (⚙️) → Networking** page.
 - Users that are assigned the **Supervisor** role are added to the **SupervisorGroup** user group during the update (see).
 - Users that are assigned the **Operator** role are added to the **OperatorLegacyGroup** user group during the update. The **OperatorLegacyGroup** user group is associated with the **Operator Legacy** role, which gives users the same privileges as the **Operator** role in the previous releases. The **Operator Legacy** role and **OperatorLegacyGroup** user group will be deprecated in a future release (see). Existing user groups are assigned to the **Operator** role during the update (see).
 - Creating rules for raising custom analytics alerts is simplified in XClarity Orchestrator v1.3. Existing custom alert rules are not migrated to the new format and will be lost after the update completes.
 - **From XClarity Orchestrator v1.1**
 - Users that are assigned the **Supervisor** role are added to the **SupervisorGroup** user group during the update (see).
 - Users that are assigned the **Operator** role are added to the **OperatorLegacyGroup** user group during the update. The **OperatorLegacyGroup** user group is associated with the **Operator Legacy** role, which gives users the same privileges as the **Operator** role in the previous releases. The **Operator Legacy** role and **OperatorLegacyGroup** user group will be deprecated in a future release (see). Existing user groups are assigned to the **Operator** role during the update (see).
 - Creating rules for raising custom analytics alerts is simplified in XClarity Orchestrator v1.3. Existing custom alert rules are not migrated to the new format and will be lost after the update completes.
 - The minimum storage required for the virtual appliance is a **total of 301 GB** across two attached disks. You must increase the storage for the disk 0 to a minimum of 251 GB. You must also attach a second disk (disk 1) with a minimum of 100 GB. The XClarity Orchestrator virtual appliance must be powered off before adding a new hard disk.

To add a new hard disk to the virtual appliance, complete the following steps.

- **For ESXi using VMware vSphere**
 1. Connect to the host through VMware vSphere Client.
 2. Power off the XClarity Orchestrator virtual machine.

3. Right-click the virtual machine, and click **Edit Settings**.
 4. Select **Add a new Device → Hard Disk**.
 5. Change the size to 100 GB.
 6. Click **OK**.
 7. Power on the XClarity Orchestrator virtual machine.
- **For ESXi using VMware vCenter**
 1. Connect to the host through VMware vCenter.
 2. Power off the virtual machine.
 3. Open the virtual machine's settings, and click **Add**.
 4. Click **Hard Disk → Create a new Virtual Disk**.
 5. Select **SCSI** for the disk format.
 6. Configure the HDD capacity to 100 GB.
 7. Click **OK**.
 8. Power on the virtual machine.
 - **For Microsoft Hyper-V**
 1. From the Server Manager Dashboard, click **Hyper-V**.
 2. Right-click the server, and click **Hyper-V Manager**.
 3. Select the XClarity Orchestrator virtual machine, and click **Shut Down** in the Actions pane.
 4. Click **Settings** to display the Settings dialog.
 5. Select **IDE Controller 0**.
 6. From the right pane, select **Hard Drive**, and then click **Add** to add a new hard disk.
 7. From the right pane, select **Virtual hard disk (.vhd) file**, and then click **New** to display the New Virtual Hard Disk Wizard.
 8. Complete the wizard as prompted. Ensure that you specify a disk-drive name using .vhd format (for example, LXC0-disk2.vhd) and set the size to 100 GB.
 9. Select the XClarity Orchestrator virtual machine, and click **Start** in the Actions pane.
- **To XClarity Orchestrator v1.1**
 - All users are automatically added to the **SupervisorGroup** user group. All users have supervisor privileges by default after the update completes. A supervisor user can remove supervisor privileges for other users that should not have those privileges (see).
 - Existing external LDAP configurations are removed. You must reconfigure external LDAP authentication servers after the update completes (see).

During the update process, all users are logged off when the orchestrator server restarts. You must wait several minutes until the restart completes. After the update completes and restarts, clear the web browser cache and refresh the web browser before logging back in.

Ensure that you back up the XClarity Orchestrator virtual appliance before installing an update (see [Backing up and restoring management-server data](#) in the XClarity Orchestrator online documentation).

Ensure that all required ports and Internet addresses are available before you attempt to update XClarity Orchestrator. For more information and .

Procedure

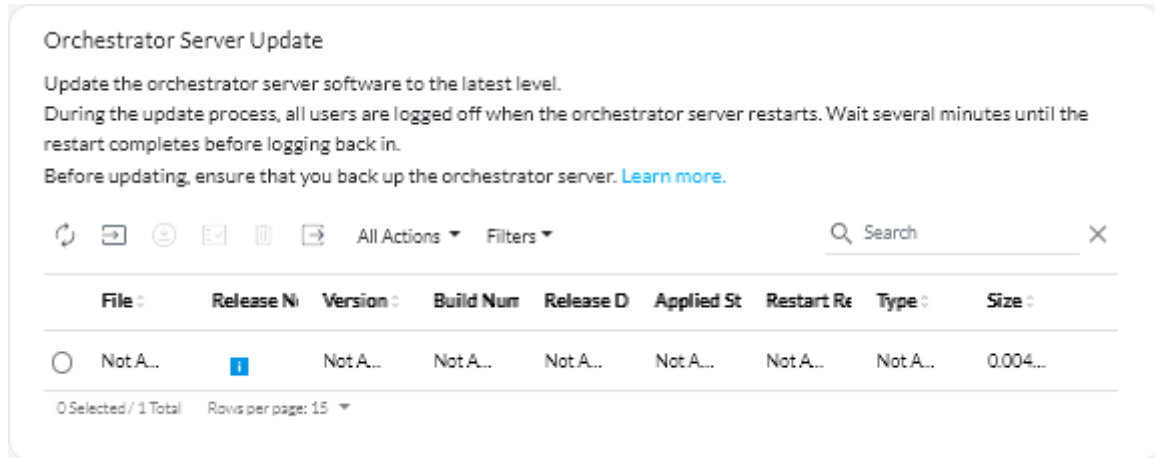
To update XClarity Orchestrator, complete the following steps.

- Step 1. Download the orchestrator-server update-package file (.tgz) from the [XClarity Orchestrator download webpage](#) to a workstation that has a network connection to the XClarity Orchestrator host.

The update-package file contains all required files: payload file (.tar.gz), metadata (.xml), change history (.chg), and readme (.txt).

Step 2. From the XClarity Orchestrator main menu, click **Maintenance** (🔧), and then click **Orchestrator Server Updates** to display the Orchestrator Server Updates card.

Orchestrator-server updates that are earlier than the currently installed version are listed in the table with an applied status of “Not applicable” and cannot be applied to the orchestrator server.



Step 3. Click the **Import** icon (📁) to display the Import dialog.

Step 4. Drag and drop the entire update-package file (.tgz) to the Import dialog, or click **Browse** to locate the file.

Step 5. Click **Import**.

Attention: Importing the update files might take a while. You must remain on the Orchestrator Server Updates card until the import process completes. Navigating away from the Orchestrator Server Updates card aborts the import process.

When the import is complete, the orchestrator-server update is listed in the table on the Orchestrator Server Files card.

You can monitor the import progress by clicking **Monitoring** (📊) → **Jobs** from the XClarity Orchestrator menu bar.

Step 6. From the Orchestrator Server Files card, select the update package that you want to install.

Step 7. Click the **Apply Update** icon (📄).

You can monitor the update progress by clicking **Monitoring** (📊) → **Jobs** from the XClarity Orchestrator menu bar.

Step 8. Wait for the update to complete and XClarity Orchestrator to restart. The update process might take a while.

If you have access to the virtual appliance host, you can monitor the progress from the virtual-appliance console, for example:

```
Lenovo XClarity Orchestrator Version x.x.x
-----

eth0  Link encap:Ethernet HWaddr 2001:db8:65:12:34:56
      inet addr: 192.0.2.10 Bcast 192.0.2.55 Mask 255.255.255.0
      inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link

=====
=====
```

You have 118 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 use a DHCP address for Lenovo XClarity virtual appliance eth0 port
3. To select subnet for Lenovo XClarity virtual appliance internal network
- x. To continue without changing IP settings

... ..

Step 9. Clear the web browser cache, and refresh the web browser.

When completed, the **Applied Status** column changes to “Applied.”

After you finish

You can perform the following actions from the Orchestrator Server Files card.

- View the current version and build number for the XClarity Orchestrator instance by clicking the **User-Account** menu (👤) on the XClarity Orchestrator title bar, and then clicking **About**.
- View the update history for a specific update that is applied to XClarity Orchestrator by clicking the update-status link in the **Applied Status** column.
- Save a selected orchestrator-server update to the local system by clicking the **Save As** icon (📄).
- Delete a selected orchestrator-server update by clicking the **Delete** icon (🗑️).

Chapter 4. Uninstalling the XClarity Management Hub

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

Procedure

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

Step 1. Unmanage all devices that are currently managed by XClarity Management Hub.

Step 2. Uninstall XClarity Management Hub, depending on the operating system.

- **ESXi**

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

Lenovo