



# Lenovo XClarity Orchestrator 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 2020, 2023.

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

---

# Contents

<b>Contents</b> . . . . .	<b>i</b>	Implementing high availability (ESXi) . . . . .	14
<b>Summary of changes</b> . . . . .	<b>.iii</b>	<b>Chapter 4. Configuring XClarity Orchestrator for the first time</b> . . . . .	<b>17</b>
<b>Chapter 1. Planning for XClarity Orchestrator</b> . . . . .	<b>1</b>	Accessing the XClarity Orchestrator web interface for the first time . . . . .	17
Licensing . . . . .	1	Creating a local user . . . . .	19
Supported hardware and software . . . . .	2	Configuring the network . . . . .	21
Firewalls and proxy servers . . . . .	4	Configuring the date and time . . . . .	23
Port availability . . . . .	4	Setting up the authentication server . . . . .	25
Network considerations. . . . .	5	Configuring additional security settings . . . . .	28
Security considerations. . . . .	5	Configuring and enabling automatic problem notification (Call Home) . . . . .	28
Secure-environment considerations . . . . .	5	Setting up event-data forwarding . . . . .	31
Cryptography considerations. . . . .	6	Connecting resource managers . . . . .	32
Security-certificate considerations. . . . .	6	<b>Chapter 5. Applying XClarity Orchestrator licenses</b> . . . . .	<b>37</b>
Authentication-server considerations . . . . .	7	<b>Chapter 6. Updating XClarity Orchestrator</b> . . . . .	<b>43</b>
Access-control considerations . . . . .	7	<b>Chapter 7. Uninstalling XClarity Orchestrator</b> . . . . .	<b>49</b>
High-Availability considerations . . . . .	8		
<b>Chapter 2. Setting up XClarity Orchestrator on a local system</b> . . . . .	<b>9</b>		
<b>Chapter 3. Implementing high availability</b> . . . . .	<b>13</b>		
Implementing high availability (Hyper-V) . . . . .	13		



---

## Summary of changes

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

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

This version supports the following enhancements for planning and installation. For information about changes in earlier releases, see [What's new](#) in the XClarity Orchestrator online documentation.

Function	Description
Planning and installation	A minimum of 551 GB of total storage space is required for the virtual appliance. The OS deployment feature requires a dedicated disk with a minimum of 200 GB storage. (See <a href="#">Supported hardware and software</a> and <a href="#">Setting up XClarity Orchestrator on a local system</a> ).



---

# Chapter 1. Planning for XClarity Orchestrator

---

## Licensing

Lenovo XClarity Orchestrator is a for-fee application. You can use XClarity Orchestrator for free for up to 90 days using the free-trial license; however, after the free trial expires, you must purchase and install appropriate licenses to continue using applicable XClarity Orchestrator functions and to get XClarity Orchestrator service and support.

XClarity Orchestrator supports the following licenses.

- **XClarity Orchestrator.** Enables orchestrator and base management functions and entitlement for XClarity Orchestrator service and support. For orchestrator functions, a license is required in XClarity Orchestrator for every device that supports server configuration and OS deployment. For XClarity Orchestrator service and support, a license is required for *every managed device*.

License compliance is determined based on the number of managed devices. The number of managed devices must not exceed the total number of licenses in all active XClarity Orchestrator license keys. When the number of XClarity Orchestrator licenses is not compliant (for example, if licenses expire or if managing additional devices exceeds the total number of active licenses), you have a grace period of 90 days to install appropriate licenses. If the grace period (including the free trial) licenses ends before the required number of licenses is installed, XClarity Orchestrator functions (including analytics) are disabled for *all devices*. When you log in, you are redirected to License Information page where you can apply additional licenses.

For example, if you manage an additional 100 ThinkSystem servers and 20 rack switches using an existing XClarity Administrator instance that you are managing through XClarity Orchestrator, you have 90 days to purchase and install 100 additional XClarity Orchestrator licenses before all functions are disabled in the user interface. Licenses for the 20 rack switches are not needed to use the XClarity Orchestrator functions; however, they are needed if you want service and support for XClarity Orchestrator. If XClarity Orchestrator functions are disabled, the functions are re-enabled after you install enough licenses to be back in compliance.

**Important:** The base XClarity Orchestrator license is a prerequisite for the XClarity Pro and XClarity Orchestrator Analytics licenses. If the number of XClarity Pro or XClarity Orchestrator licenses *is* compliant, but the number of active base licenses *is not* compliant, all XClarity Orchestrator functions (including analytics functions) are disabled for all devices.

- **Lenovo XClarity Pro.** Enables advanced management functions (server configuration and OS deployment). A license is required in XClarity Orchestrator for each device that supports advanced-management functions.

License compliance is determined based on the number of managed devices. The number of managed devices must not exceed the total number of licenses in all active XClarity Pro license keys. When the number of XClarity Pro licenses is not compliant, you have a grace period of 90 days to install appropriate licenses. If the grace period (including the free trial) ends before the required number of licenses is installed, the server configuration and OS deployment functions are disabled for *all devices*.

For more information about XClarity Pro licenses, see [Licenses and the free 90-day trial](#) in the Lenovo XClarity Administrator online documentation.

- **XClarity Orchestrator Analytics.** Enables analytics functions. A license is required in XClarity Orchestrator for each device that supports advanced-management functions.

License compliance is determined based on the number of managed devices. The number of managed devices must not exceed the total number of licenses in all active XClarity Orchestrator Analytics license keys. When the number of XClarity Orchestrator Analytics licenses is not compliant (for example, if

licenses expire or if managing additional devices exceeds the total number of active licenses), you have a grace period of 90 days to install appropriate licenses. If the grace period (including the free trial) ends before the required number of licenses is installed, the **Monitoring** → **Analytics** menus are disabled and you cannot view analytics reports or create custom alert rules and queries for *all devices*.

A license *is not* tied to specific devices.

The activation period starts when the licenses are redeemed.

Licenses are installed using a license *activation key*. After you redeem licenses, you can create an activation key for all or a subset of your available licenses, and then download and install the activation key in XClarity Orchestrator.

Each time XClarity Orchestrator becomes non-compliant, the grace period resets to 90 days.

If licenses are already installed, new licenses are *not* required when upgrading to a new release of XClarity Orchestrator.

If you are using a free trial license or if you have a grace period to become compliant, and you upgrade to a later version of XClarity Orchestrator, the trial license or grace period resets to 90 days.

When upgrading XClarity Orchestrator or if an error condition occurs that requires you to restore the activation keys, you can either use exported keys or download all activation keys (for each customer ID) from the [Features on Demand web portal](#), and then import the activation keys (either as individual activation keys or collectively as a key ZIP file) into XClarity Orchestrator.

For information about purchasing licenses, contact your Lenovo representative or authorized business partner.

---

## Supported hardware and software

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

### Host systems

XClarity Orchestrator runs in a virtual appliance on a host system.

### Hypervisor requirements

The following hypervisors are supported for installing XClarity Orchestrator.

- Microsoft Windows Server 2019 with Hyper-V installed
- Microsoft Windows Server 2022 with Hyper-V installed
- VMware ESXi 7.0
- VMware ESXi 6.7, U1, U2, and U3
- VMware ESXi 6.5, U1 and U2

For Hyper-V, the virtual appliance is a virtual-disk image (VHD). For VMware ESXi, the virtual appliance is an OVF template.

### Hardware requirements

The following *minimum requirements* must be met for the virtual appliance. Depending on the size of your environment, additional resources might be required for optimal performance.

- 4 virtual processor cores
- 16 GB memory



- 551 GB storage, across two attached disks.
  - 251 GB minimum for the virtual appliance (disk 0)
  - 100 GB for the updates repository (disk 1)
  - 200 GB for the OS-images repository (disk 2)

**Important:** You cannot increase or decrease the size of the disk that is used for the updates repository and OS-images repository.

## Software requirements

XClarity Orchestrator requires the following software.

- **Authentication server.** XClarity Orchestrator uses an internal Lightweight Directory Access Protocol (LDAP) server, by default, for authentication. If you choose to use an external authentication server, the following LDAP servers are supported:
  - Microsoft Active Directory running on Windows Server 2008 or later
- **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 Orchestrator. Ensure that the NTP server is accessible over the management network (typically the Eth0 interface). Consider using the local system on which XClarity Orchestrator is installed as the NTP server. If you do, ensure that the local system is accessible over the management network.

## Manageable resources

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

XClarity Orchestrator supports the following resource managers.

- **Lenovo XClarity Management Hub** XClarity Orchestrator manages, monitors, and provisions devices that are under management by XClarity Management Hub. Each XClarity Management Hub instance can manage up to **10,000** ThinkEdge Client devices.

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](#).

- **Lenovo XClarity Administrator v2.6 or later** XClarity Orchestrator manages, monitors, and provisions physical devices that are under management by XClarity Administrator. Each XClarity Administrator instance can manage up to **1,000** devices (servers, chassis, switches, and storage).

XClarity Orchestrator supports all devices that are supported by XClarity Administrator and Lenovo XClarity Management Hub except where noted. 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 following Lenovo XClarity Support webpages.

- [ThinkAgile, ThinkEdge, ThinkSystem, System x, Converged HX, and NeXtScale rack and tower servers](#)
- [Flex System devices and ThinkSystem compute nodes](#)
- [ThinkServer rack and tower servers](#)
- [RackSwitch devices](#)
- [Storage devices](#)

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

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

- Schneider Electric EcoStruxure IT ExpertXClarity Orchestrator manages and monitors infrastructure resources, such as PDUs and UPSs, that are managed by EcoStruxure IT Expert
- VMware vRealize Operations ManagerXClarity Orchestrator monitors virtual workload metrics from vRealize Operations Manager.

**Note:** vRealize Operations Manager is not included in the list of resource managers, as it does not manage devices in XClarity Orchestrator.

### Web browsers

The XClarity Orchestrator 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 later
- Safari 13.0.4 or later (running on macOS 10.13 or later)

### Third-party software

XClarity Orchestrator integrates with the following software.

- Splunk v7.0.3 and later (see [XClarity Orchestrator app for Splunk User's Guide](#))

---

## 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

Lenovo XClarity Orchestrator requires certain ports to be open to facilitate communication. If the required ports are blocked or used by another process, some XClarity Orchestrator functions might not perform correctly.

If XClarity Orchestrator and all managed resources are behind a firewall, and you intend to access those resources from a browser that is *outside* of the firewall, ensure that the required ports are open. XClarity Orchestrator listens on and responds through the ports that are listed in the following table.

### Notes:

- XClarity Orchestrator is a RESTful application that communicates securely over TCP on port 443.
- *Inbound* traffic flows from managed resources and external systems to XClarity Orchestrator, so ports must be open on the XClarity Orchestrator appliance. *Outbound* traffic flows from XClarity Orchestrator to managed resources.
- XClarity Orchestrator can be optionally configured to make outbound connections to external services, such as LDAP, SMTP, or syslog. These connections might require additional ports that are generally user configurable and not included in this list. These connections might also require access to a domain name service (DNS) server on TCP or UDP port 53 to resolve external server names.

Commu- nication	XClarity Orchestrator appliance	External authentication servers	Event forwarding services	Lenovo services (including Call Home)
<b>Outbound</b> (ports open on external systems)	<ul style="list-style-type: none"> <li>DNS – TCP/UDP on port <b>53</b></li> </ul>	<ul style="list-style-type: none"> <li>LDAP– TCP on port <b>389</b><sup>1</sup></li> </ul>	<ul style="list-style-type: none"> <li>Email server (SMTP) – UDP on port <b>25</b><sup>1</sup></li> <li>REST Web Service (HTTP) – UPD on port <b>80</b><sup>1</sup></li> <li>Splunk – UDP on port <b>8088</b><sup>1</sup>, <b>8089</b><sup>1</sup></li> <li>Syslog – UDP on port <b>514</b><sup>1</sup></li> </ul>	<ul style="list-style-type: none"> <li>HTTPS (Call Home) – TCP on port <b>443</b></li> </ul>
<b>Inbound</b> (ports open on XClarity Orchestra- tor appliance)	<ul style="list-style-type: none"> <li>HTTPS – TCP on port <b>443</b></li> </ul>	Not applicable	Not applicable	Not applicable

1. This is the default port. You can configure this port from the XClarity Orchestrator user interface.

---

## Network considerations

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

- The network interface is used for discovery and management. It must be able to communicate with all devices that you intend to manage.
- If you intend to manually send collected service data to Lenovo Support or use automatic problem notification (Call Home), the interfaces must be connected to the Internet, preferably through a firewall.
- If you change the XClarity Orchestrator virtual-appliance IP address after connecting resource managers, XClarity Orchestrator will lose communication with the managers, and the managers will appear offline. If you need to change the virtual-appliance IP address after XClarity Orchestrator is up and running, ensure that all resource managers are disconnected (deleted) before changing the IP address.
- 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 changes, you must disconnect (delete) the managed devices, and then connect them again.
- Network address translation (NAT), which remaps one IP address space into another, is not supported.

---

## Security considerations

Review the following considerations to help you plan for the security of Lenovo XClarity Orchestrator and all managed resources.

### Secure-environment considerations

It is important that you evaluate the security requirements in your environment, understand all security risks, and minimize those risks. Lenovo XClarity Orchestrator includes several features that can help you secure your environment. Use the following information to help you implement the security plan for your environment.

**Important:** You are responsible for the evaluation, selection, and implementation of security features, configuration procedures, and appropriate controls for your environment. Implementing the security features that are described in this section does not secure your environment completely.

Consider the following information when you are evaluating the security requirements for your environment.

- The physical security of your environment is important. Limit access to rooms and racks where systems-management hardware is kept.
- Use a software-based firewall to protect your network hardware and data from known and emerging security threats, such as viruses and unauthorized access.
- Do not change the default security settings for the network switches and pass-thru modules. The manufacturing default settings for these components disable the use of unsecure protocols and enable the requirement for signed firmware updates.
- At a minimum, ensure that critical firmware updates are installed. After making any changes, always back up the configuration.
- Ensure that all security-related updates for DNS servers are installed promptly and kept up to date.
- Instruct your users to not accept any untrusted certificates. For more information, see [Working with security certificates](#) in the XClarity Orchestrator online documentation.
- Where possible and practical, place the systems-management hardware in a separate subnet. Typically, only supervisors should have access to the systems-management hardware, and no basic users should be given access.
- When you choose passwords, do not use expressions that are easy to guess, such as "password" or the name of your company. Keep the passwords in a secure place, and ensure that access to the passwords is restricted. Implement a password policy for your company.

**Important:** Strong password rules should be required for all users.

- Establish power-on passwords for users as a way to control who has access to the data and setup programs on the servers. See the documentation that comes with your hardware for more information about power-on passwords.

## Cryptography considerations

Lenovo XClarity Orchestrator supports TLS 1.2 and stronger cryptographic algorithms for secure network connections.

For increased security, only high-strength ciphers are supported. The client operating system and web browsers must support one of the following cipher suites.

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

## Security-certificate considerations

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

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

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

For more information about certificates, see .

## Authentication-server considerations

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

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

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

For more information about setting up external LDAP servers, see .

## Access-control considerations

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

### About this task

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

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

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

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

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

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

For more information about access-control lists, see [Controlling access to resources](#) in the XClarity Orchestrator online documentation.

---

## 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 [Implementing high availability \(ESXi\)](#).

---

## Chapter 2. Setting up XClarity Orchestrator on a local system

Install and configure the Lenovo XClarity Orchestrator virtual appliance on a system in your local environment.

### Before you begin

Ensure that you have reviewed the prerequisites, including hardware requirements and recommendations, for XClarity Orchestrator (see [Supported hardware and software](#)).

Ensure that all appropriate ports are enabled, including ports that XClarity Orchestrator requires (see [Port availability](#)).

Ensure that the resource managers that you intend to manage are supported and are at the required version levels (see [Supported hardware and software](#)).

For information about updating an XClarity Orchestrator virtual appliance that is already installed, see [Updating XClarity Orchestrator](#).

For information about setting up a high-available environment, see [Implementing high availability](#).

Lenovo XClarity Orchestrator is a for-fee application. You can use XClarity Orchestrator for free for up to 90 days using the free-trial license; however, after the free trial expires, you must purchase and install appropriate licenses to continue using applicable XClarity Orchestrator functions and to get XClarity Orchestrator service and support. For information about purchasing licenses, contact your Lenovo representative or authorized business partner. For information about installing the license, see [Applying XClarity Orchestrator licenses](#).

### 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 Orchestrator 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, and DNS 1 IP address (optional), and DNS 2 IP address (optional).
- For static IPv6 settings, you can change the IP address, prefix length, and 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:** If you change the XClarity Orchestrator virtual-appliance IP address after connecting resource managers, XClarity Orchestrator will lose communication with the managers, and the managers will appear offline. If you need to change the virtual-appliance IP address after XClarity Orchestrator is up and running, ensure that all resource managers are disconnected (deleted) before changing the IP address. For more information about setting IP addresses, see [Configuring the network](#).

### Procedure

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

Step 1. Download the XClarity Orchestrator image from the [XClarity Orchestrator download webpage](#) to the local system. Log in to the website, and use the access key that was given to you to download the image.

For Hyper-V, the virtual appliance is a virtual-disk image (VHD). For VMware ESXi, the virtual appliance is an OVF template.

Step 2. Install and configure the virtual appliance on the local 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 virtual-appliance deployment 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 a minimum of 551 GB of 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 static IP address for the eth0 interface.

- **For ESXi using VMware vCenter**

1. Connect to the host through VMware vCenter.
2. Under "Hosts and Clusters" or "VMs and Templates," right-click the host, and click **File** → **Deploy OVF Template**.
3. Complete each step in the virtual-appliance deployment 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 a minimum of 551 GB of 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 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 on **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 Microsoft 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 begin the New Virtual Machine Wizard, and click **Next**.
4. On the Specify Name and Location page, enter a name for the new virtual machine (for example, LXCO-*{version}*).
5. On the Specify Generation page, select **Generation 1**.



6. On the Assign Memory page, select at least 16 GB of memory to use for this virtual machine (see [Supported hardware and software](#)).
7. On the Configure Networking page, choose the virtual switch that you created when you installed and configured the host.
8. On the Connect Virtual Hard Disk page, click **Use an existing virtual hard disk**, browse to the location where you copied the XClarity Orchestrator VHD images, and select the **\*disk001\*.vhd** image.
9. Click **Finish**.
10. Right-click on the virtual machine that you just created, and click **Settings**.
11. Configure the number of processors to assign to the virtual machine.
  - a. Select **Processor**, and specify at least 4 virtual processors to use for this virtual machine (see [Supported hardware and software](#)).
  - b. Click **Apply**, and then click **OK**.
12. Add the second hard drive to the virtual appliance.
  - a. Expand **IDE Controller 0**, and then select **Hard Drive**.
  - b. From the **Virtual hard disk** field, browse to the location where you copied the XClarity Orchestrator VHD images, and select the **\*disk002\*.vhd** image.
  - c. Click **Apply**, and then click **OK**.
13. Add the third hard drive to the virtual appliance.
  - a. Expand **IDE Controller 1**, and then select **Hard Drive**.
  - b. From the **Virtual hard disk** field, browse to the location where you copied the XClarity Orchestrator VHD images, and select the **\*disk003\*.vhd** image.
  - c. Click **Apply**, and then click **OK**.
14. (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.

Step 3. Power on the virtual appliance.

When the virtual appliance is started, the IPv4 and IPv6 addresses that were assigned by DHCP are listed for each interface, as shown in the following 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 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. By default, XClarity Orchestrator uses subnet **192.168.252.0/24** for its internal network. If this subnet overlaps with the host network, change the subnet to one of the other available choices to avoid networking issues.
  - 192.168.252.0/24
  - 172.31.252.0/24
  - 10.255.252.0/24

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

## After you finish

Log in and configure XClarity Orchestrator.

---

## Chapter 3. Implementing high availability

To implement high availability for Lenovo XClarity Orchestrator, use the high-availability function that is provided by the host environment.

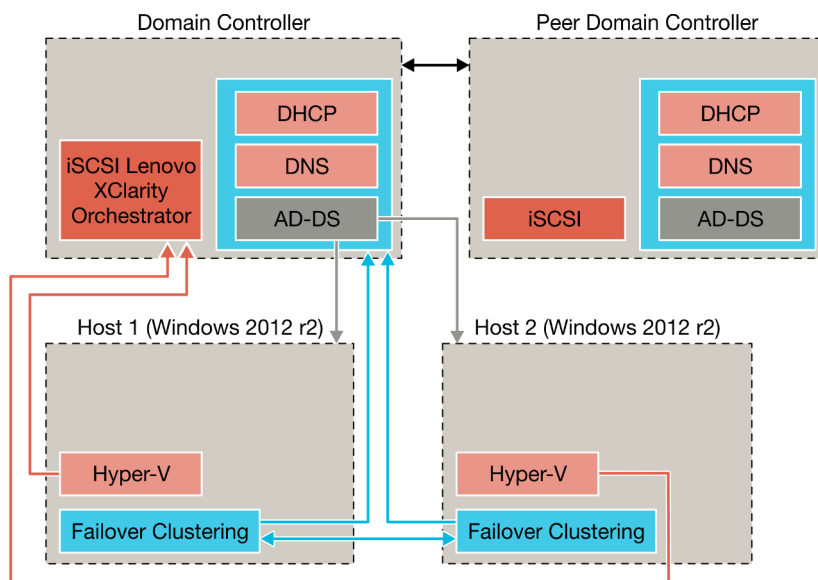
---

### Implementing high availability (Hyper-V)

To implement high availability for Lenovo XClarity Orchestrator in a Microsoft Hyper-V environment, use the high-availability function that is provided by Hyper-V.

#### About this task

The following illustration provides a high-level overview of one way to implement high availability for XClarity Orchestrator in a Hyper-V environment. In this example, the XClarity Orchestrator image is installed on the shared storage and accessed by the cluster.



#### Procedure

To set up a high-availability environment, complete the following steps.

Step 1. Set up the domain controller.

- a. Perform the initial DHCP setup.
- b. Set up DNS.
- c. Set up Active Directory - Domain Services (AD-DS).
- d. Complete the DHCP setup.

Step 2. Set up the first host.

- a. Install Microsoft Windows 2012 r2.
- b. Join the AD-DS domain.
- c. Add the following features.
  - Hyper-V
  - Failover clustering

- Step 3. Set up the second host.
- a. Install Microsoft Windows 2012 r2.
  - b. Join the AD-DS domain.
  - c. Add the following features.
    - Hyper-V
    - Failover clustering
- Step 4. Configure the shared storage (such as iSCSI) on the domain controller and both hosts.
- Step 5. Configure failover clustering.
- Step 6. Add the XClarity Orchestrator image.

---

## Implementing high availability (ESXi)

To implement high availability for Lenovo XClarity Orchestrator in a VMware ESXi environment, use the high-availability function that is provided by ESXi.

### About this task

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.

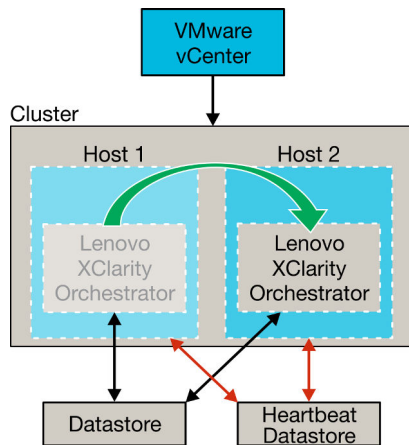
- A minimum of two hosts on which ESXi is installed. These hosts become part of the VMware cluster.
- A third host on which VMware vCenter is installed.

**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).

The following figure illustrates one way to implement high availability for XClarity Orchestrator in an ESXi environment. In this scenario, the XClarity Orchestrator virtual appliance is installed on the shared storage and accessed by the cluster.



For details about setting up a VMware high availability cluster (VMware 5.0), see the [Setting up HA for VMware webpage](#).

## Procedure

To set up a high-availability environment, complete the following steps.

- Step 1. Set up shared storage that is to be accessible from all hosts in the cluster.
- Step 2. Install ESXi on two servers, each with static IP addresses. Ensure that VMware vCenter is configured on a separate server.
- Step 3. Start VMware vCenter.
- Step 4. Configure the other two hosts to work with VMware vCenter.
  - a. Create the cluster.
  - b. Add the hosts to the cluster.
  - c. Add both datastores to the hosts in the cluster.

**Note:** You need the second datastore for heartbeat.

- Step 5. Deploy XClarity Orchestrator to the cluster.



---

## Chapter 4. Configuring XClarity Orchestrator for the first time

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

### Procedure

To set up XClarity Orchestrator for the first time, complete the following steps.

- Step 1. Access the XClarity Orchestrator web interface.
- Step 2. Change the initial password.
- Step 3. Read and accept the license agreement.
- Step 4. Create additional user accounts.
- Step 5. Configure the date and time.
- Step 6. Configure network access, including IP addresses for the data and management network.
- Step 7. Choose to use the default authentication server or configure an external LDAP client.
- Step 8. Configure additional security settings, including importing trusted certificates for internal and external services.
- Step 9. Configure and enable automatic problem notification, if applicable.
- Step 10. Configure XClarity Orchestrator to forward events to specific services and applications, if applicable.
- Step 11. Connect your resource managers.

---

### Accessing the XClarity Orchestrator web interface for the first time

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

### Before you begin

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

- 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**.

XClarity Orchestrator uses a single subnet, typically eth0.

If you are configuring XClarity Orchestrator 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 Orchestrator from another VM that has connectivity to XClarity Orchestrator. For example, you can access XClarity Orchestrator from another VM on the host where XClarity Orchestrator is installed.

### Procedure

To access the XClarity Orchestrator web interface for the first time, complete the following steps.

1. Point your browser to the IP address of the XClarity Orchestrator virtual appliance.

- **Using static an IPv4 address** If you specified an IPv4 address during installation, use that IPv4 address to access the web interface using the following URL.

`https://{IPv4_address}/#/login.html`

For example:

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

- **Using a DHCP server in the same broadcast domain as XClarity Orchestrator** If a DHCP server is set up in the same broadcast domain as XClarity Orchestrator, use the IPv4 address that is displayed in the XClarity Orchestrator virtual-appliance console to access the web interface using the following URL.

`https://{IPv4_address}/#/login.html`

For example:

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

The initial login page is displayed.



We provide centralized monitoring, management, provisioning, and analytics for environments with large numbers of devices.

Username \*

Password \*

→ Log In

[Submit Idea](#) [Users Forum](#) [Users Guide](#) [License Entitlement](#) [Toolkits](#)

© 2022 Lenovo. All rights reserved.

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

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



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

3. Enter the default credentials `USERID` and `PASSWORD` (where 0 is zero), and click **Log In**. The first time that a specific user account is used to log in to XClarity Orchestrator, you are required to change the password. By default, passwords must contain **8 – 256** characters and must meet the following criteria.

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

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

## After you finish

**Important:** You might receive security or certificate warnings the first time that you access XClarity Orchestrator. You can ignore the warnings.

Continue initial setup by going to [Creating a local user](#).

---

## Creating a local user

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

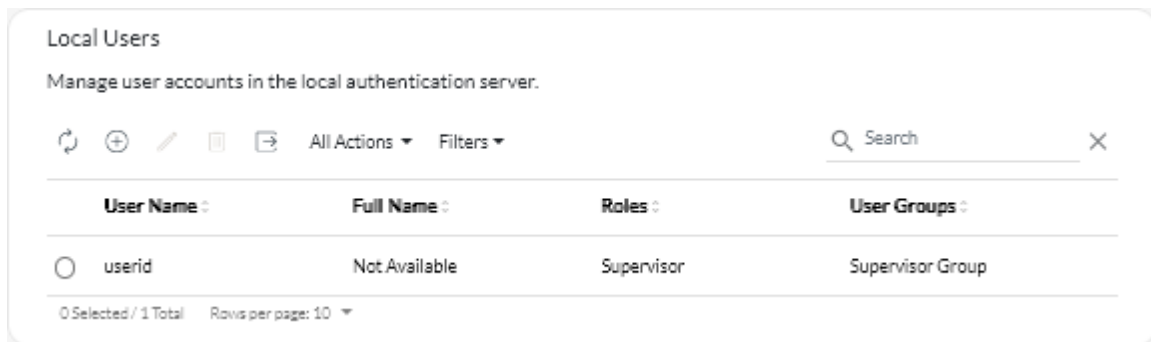
### About this task

As an added measure of security, create at least two user accounts.

### Procedure

To create a local user, complete the following steps.

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



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

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

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

**Note:** User names are not case sensitive.

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

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

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

- (Optional) Specify contact information for the user account, including the full name, email address, and phone number.

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

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

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

Step 5. Click **Create**.

The user account is added to the table.

## After you finish

Continue initial setup by going to [Configuring the network](#).

---

## Configuring the network

When you initially set up Lenovo XClarity Orchestrator, you must configure a single network interface (using IPv4 and IPv6 settings). You can also configure Internet routing settings.

### Before you begin

Review the following considerations when choosing the interface.

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

### Attention:

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

### Procedure

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

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

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

### IPv4 Configuration

Enabled

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

### IPv6 Configuration

Enabled

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

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

Currently, only IPv4 addresses are supported.

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

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

#### Notes:

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

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

**Notes:**

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

**After you finish**

Continue initial setup by going to [Configuring the date and time](#).

---

**Configuring the date and time**

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

**Before you begin**

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

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

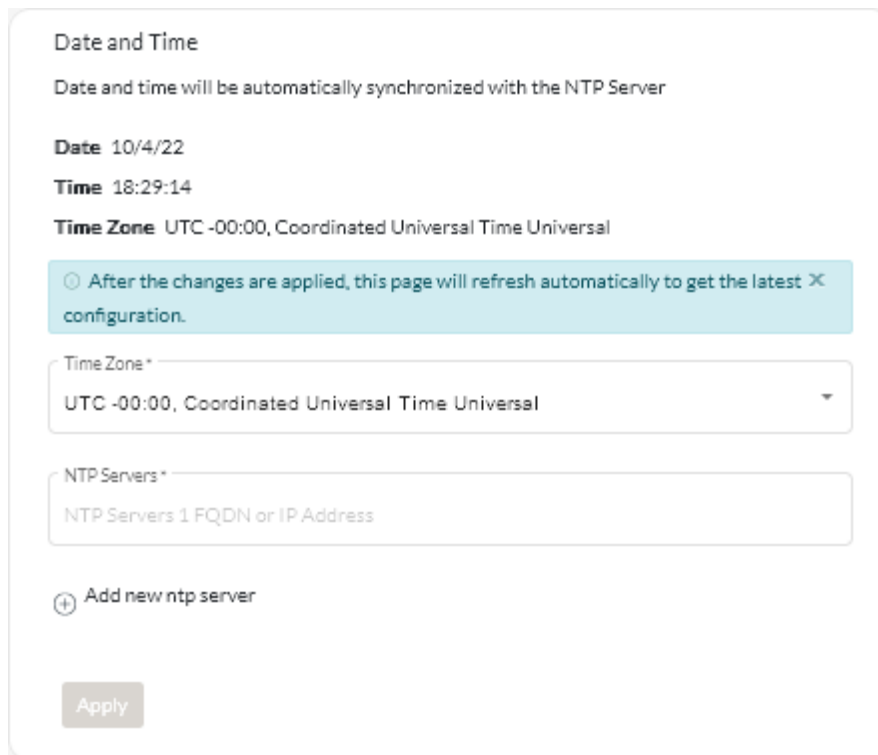
**Attention:** The XClarity Orchestrator virtual appliance and its host must be set to synchronize to the same time source to prevent inadvertent time mis-synchronization between XClarity Orchestrator and its host. Typically, the host is configured to have its virtual appliances time-sync to it. If XClarity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

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

## Procedure

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

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



The screenshot shows the 'Date and Time' configuration page. At the top, it states 'Date and time will be automatically synchronized with the NTP Server'. Below this, the current 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' text input field with the placeholder 'NTP Servers 1 FQDN or IP Address'. A plus icon and the text 'Add new ntp server' are located below the input field. At the bottom left of the card is an 'Apply' button.

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

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

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

Step 4. Click **Apply**.

## After you finish

Continue initial setup by going to [Setting up the authentication server](#).

---

## Setting up the authentication server

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

### Before you begin

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

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

### About this task

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

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

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

### Procedure

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

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

### LDAP Client ↻

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

**Server Information**

Domain\*

Server Address\*

Port\*  
636

🗑️ ⊕ ↑ ↓

Active Directory     Custom LDAP

**Configuration** LDAP over SSL

Base distinguished name for users\*

Base distinguished name for groups\*

**Binding credentials** ⓘ

Binding Method  
Configured Credentials

Binding username\*

Binding password\* 👁️

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

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

Fetch

Reset
Apply changes

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

1. Click the **Add** icon (⊕) to add an LDAP server.

2. Specify the domain name, IP address, and port for the external LDAP server.

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

When the port number is set to 3268 or 3269, the entry is assumed to identify a global catalog. The LDAP client attempts to authenticate using the domain controller for the first configured server IP address. If this fails, the LDAP client attempts to authenticate using the domain controller for the next server IP address.

3. Optionally choose to enable customizing advanced configuration settings. When you choose to use a custom configuration, you can specify the user search filter. If you do not specify a user search filter, (&&(objectClass=user)(|(userPrincipalName={0})(sAMAccountName={0}))) is used by default.

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## After you finish

Continue initial setup by going to [Configuring additional security settings](#).

---

## Configuring additional security settings

You can configure additional security settings, including certificates and user-account security settings.

### Procedure

To configure additional security, complete one or more of the following steps.

- Lenovo XClarity Orchestrator uses SSL certificates to establish secure, trusted communications between XClarity Orchestrator and the resource managers (such as Lenovo XClarity Administrator), as well as communications with XClarity Orchestrator by users. By default, XClarity Orchestrator and the resource managers use XClarity Orchestrator-generated certificates that are self-signed and issued by an internal certificate authority (CA). You can choose to generate a certificate signing request (CSR) for signing by an external certificate authority, such as your organization's certificate authority or a third-party certificate authority (see [Installing an externally-signed XClarity Orchestrator server certificate](#) in the XClarity Orchestrator online documentation).
- You can import trusted certificates for external services into the XClarity Orchestrator truststore to establish a secure connection to resource managers and event forwarders, such as Splunk (see [Setting up an external LDAP authentication server](#) in the XClarity Orchestrator online documentation).
- You can import trusted certificates for internal services into the XClarity Orchestrator truststore to establish a secure connection to resource managers and trusted LDAP servers (see [Adding a trusted certificate for internal services](#) in the XClarity Orchestrator online documentation).
- Configure the security settings for password complexity, account lockout, and web session inactivity time-out settings. For more information about these settings, see [Configuring user security settings](#) in the XClarity Orchestrator online documentation.

## After you finish

Continue initial setup by going to [Configuring and enabling automatic problem notification \(Call Home\)](#).

---

## Configuring and enabling automatic problem notification (Call Home)

You can set up Lenovo XClarity Orchestrator to automatically open a service ticket and send collected service data to Lenovo Support using the Call Home function when a device generates certain serviceable events, such as an unrecoverable memory, so that the issue can be addressed.

## Before you begin

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

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

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

**Important:** If Call Home is enabled on both XClarity Orchestrator and Lenovo XClarity Administrator, ensure that Lenovo XClarity Administrator v2.7 or later is used to avoid duplicate service tickets. If Call Home is enabled on XClarity Orchestrator and disabled on Lenovo XClarity Administrator, then Lenovo XClarity Administrator v2.6 or later is supported.

## About this task

If Call Home is configured and enabled and a serviceable event occurs on a specific device, XClarity Orchestrator *automatically* opens a service ticket and transfers service data for that device to the Lenovo Support Center.

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

When Call Home is not enabled, you can manually open a service ticket and send service files to the Lenovo Support Center by following the instructions on the [How to open a support ticket webpage](#). For information about collecting service files, see [Manually opening a service ticket in the Lenovo Support Center](#) in the XClarity Orchestrator online documentation.

For information about viewing service tickets that were opened automatically by Call Home, see [Viewing service tickets and status](#) in the XClarity Orchestrator online documentation.

## Procedure

To setup Call Home for automatic problem notification, complete the following steps.

- Step 1. From the XClarity Orchestrator menu bar, click the **Administration** (⚙️) → **Service and Support**, and then click **Call Home Configuration** in the left navigation to display the Call Home Configuration card.

### Call Home Configuration

From this page, you can configure a Call Home that automatically sends service data for any managed endpoint to Lenovo Support when certain serviceable events occur on a managed endpoint.

[Lenovo Privacy Statement](#)

I agree with the Lenovo Privacy Statement

#### Customer Details

---

Customer Number

**Primary contact to use from multiple group assignments** ?

First group assignment

Last group assignment

#### Default Contact

---

Call Home State:

<input type="text" value="Contact Name"/>	<input type="text" value="Street Address"/>
<input type="text" value="Email"/>	<input type="text" value="City"/>
<input type="text" value="Phone Number"/>	<input type="text" value="State/Province"/>
<input type="text" value="Company Name"/>	<input type="text" value="Country/Region"/>
<input type="text" value="Method For Contact"/>	<input type="text" value="Zip Code/Postal Code"/>

**System Location** ?

---

Step 2. Review the [Lenovo Privacy Statement](#), and then click **I Agree with the Lenovo Privacy Statement**

Step 3. Optional: Specify the default Lenovo customer number to use when reporting problems.

You can find your customer number in the proof-of-entitlement email that you received when you purchased your XClarity Orchestrator license.

Step 4. Change the Call Home status to **Enable**.

Step 5. Select the primary contact to use from multiple group assignments.

You can assign a primary support contact to a group of devices. If a device is a member of multiple groups, it is possible that each group is assigned a different primary contact. You can choose to use the primary contact assignment for the first group or the last group that the device was assigned to.

Step 6. Fill in the contact information and preferred method of contact by Lenovo Support.

If a device is not a member of a group with an assigned primary contact, the default contact is used for Call Home.

Step 7. Optional: Fill in the system location information.

Step 8. Click **Call Home Connection Test** to verify that XClarity Orchestrator can communicate with the Lenovo Support Center.

Step 9. Click **Apply**.

## After you finish

Continue initial setup by going to [Setting up event-data forwarding](#).

---

## Setting up event-data forwarding

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

### About this task

#### Events data

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

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

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

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

#### Inventory and events data

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

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

## Metrics data

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

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

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

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

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

For more information about forwarding event data, see [Port availability](#) in the XClarity Orchestrator online documentation.

## After you finish

Continue initial setup by going to [Connecting resource managers](#).

---

## Connecting resource managers

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

### Before you begin

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

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

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

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

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

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

- Ensure that it is an X.509 v3 certificate. XClarity Orchestrator cannot connect to an XClarity Administrator that has an externally signed v1 certificate.
- Ensure that the certificate details include the following requirements.
  - KeyUsage must contain
    - Key Agreement
    - Digital Signature
    - Key Encipherment

- Enhanced Key Usage must contain
  - Server Authentication (1.3.6.1.5.5.7.3.1)
  - Client Authentication (1.3.6.1.5.5.7.3.2)

## About this task

XClarity Orchestrator supports the following resource and application managers.

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

**Important:** The registration process Lenovo XClarity Management Hub is different than other resource manager. For detailed instructions, see .

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

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

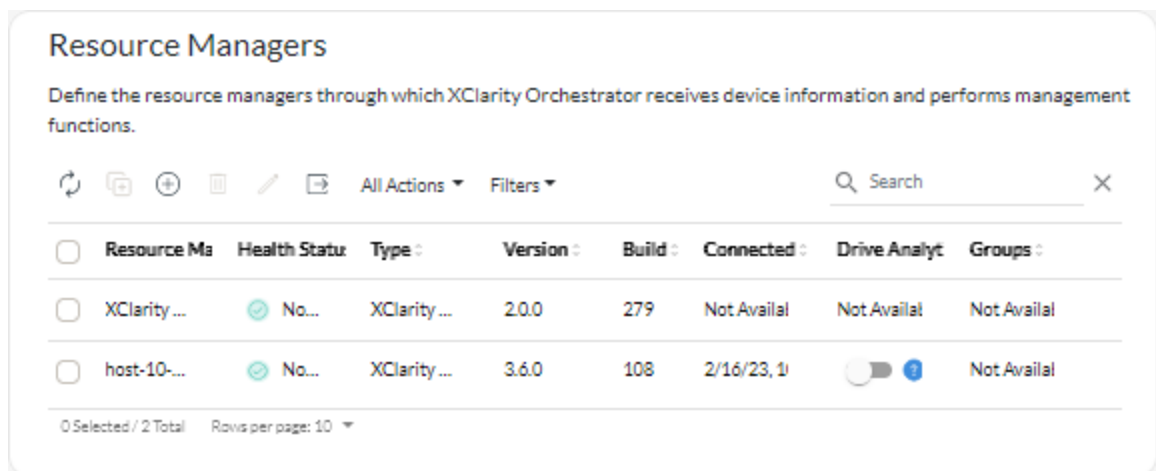
- Retrieves information about all devices that are managed by the resource manager.
- Creates and enables an event forwarder (for a REST web service) in the management server to monitor and forward events to XClarity Orchestrator.

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

## Procedure

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

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



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

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


- **XClarity Management Hub**
  - Enter the registration key that was generated by the XClarity Management Hub instance, and then click **Connect**. To get the registration request token, log in to the XClarity Management Hub, click **Registration**, and then click **Create registration key**.
  - Copy the generated XClarity Orchestrator registration key.
  - From the XClarity Management Hub web interface, click **Registration**, and click **Install registration key**, paste the XClarity Orchestrator registration token in the XClarity Management Hub instance, and then click **Connect**.
- **XClarity Administrator**
  - Specify the fully-qualified domain name or IP address (IPv4 or IPv6). Using the host name without the domain name is not supported.
  - Optionally change the port of the resource manager. The default is 443.
  - Specify the user account and password to use to log in to the resource manager.
  - Optionally enable **Drive Analytics Data Collection**. When enabled, drive analytics data is collected daily for ThinkSystem and ThinkAgile devices and is used for predictive analytics. Drive analytics data collection is supported only for XClarity Administrator v3.3.0 and later resource managers.

**Attention:** System performance might be affected when data is collected.
- **EcoStruxure IT Expert**. Specify the name, token key, and URL to use for the connection.
- **vRealize Operations Manager**
  - Specify the fully-qualified domain name or IP address (IPv4 or IPv6). Using the host name without the domain name is not supported.
  - Optionally change the port of the resource manager. The default is 443.
  - Optionally select the authorization source for the users and groups.



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

Step 4. Click **Connect**.

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

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

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

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

## After you finish

Initial setup is complete.



---

## Chapter 5. Applying XClarity Orchestrator licenses

Lenovo XClarity Orchestrator is a for-fee application. You can use XClarity Orchestrator for free for up to 90 days using the free-trial license; however, after the free trial expires, you must purchase and install appropriate licenses to continue using applicable XClarity Orchestrator functions and to get XClarity Orchestrator service and support.

### Before you begin

For information about purchasing licenses, contact your Lenovo representative or authorized business partner.

A license is needed for each managed device that supports advanced functions (server configuration and OS deployment).

- A chassis license provides licenses for 14 devices.
- For System x3850 X6 (6241) scalable complex servers, each server needs a separate license, regardless of partitions.
- For System x3950 X6 (6241) scalable complex servers, if not partitioned, each server needs a separate license. If partitioned, each partition needs a separate license.
- The following devices *do not support* advanced functions and therefore *do not require* licenses for these features; however, a license must be purchased for each of these devices to get XClarity Orchestrator service and support.
  - ThinkServer servers
  - System x M4 servers
  - System x X5 servers
  - System x3850 X6 and x3950 X6 (3837) servers
  - Storage devices
  - Switches

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

### About this task

XClarity Orchestrator supports the following licenses.

- **XClarity Orchestrator.** Enables orchestrator and base management functions and entitlement for XClarity Orchestrator service and support. For orchestrator functions, a license is required in XClarity Orchestrator for every device that supports server configuration and OS deployment. For XClarity Orchestrator service and support, a license is required for *every managed device*.

License compliance is determined based on the number of managed devices. The number of managed devices must not exceed the total number of licenses in all active XClarity Orchestrator license keys. When the number of XClarity Orchestrator licenses is not compliant (for example, if licenses expire or if managing additional devices exceeds the total number of active licenses), you have a grace period of 90 days to install appropriate licenses. If the grace period (including the free trial) licenses ends before the required number of licenses is installed, XClarity Orchestrator functions (including analytics) are disabled for *all devices*. When you log in, you are redirected to License Information page where you can apply additional licenses.

For example, if you manage an additional 100 ThinkSystem servers and 20 rack switches using an existing XClarity Administrator instance that you are managing through XClarity Orchestrator, you have 90 days to purchase and install 100 additional XClarity Orchestrator licenses before all functions are disabled in the

user interface. Licenses for the 20 rack switches are not needed to use the XClarity Orchestrator functions; however, they are needed if you want service and support for XClarity Orchestrator. If XClarity Orchestrator functions are disabled, the functions are re-enabled after you install enough licenses to be back in compliance.

**Important:** The base XClarity Orchestrator license is a prerequisite for the XClarity Pro and XClarity Orchestrator Analytics licenses. If the number of XClarity Pro or XClarity Orchestrator licenses *is* compliant, but the number of active base licenses *is not* compliant, all XClarity Orchestrator functions (including analytics functions) are disabled for all devices.

- **Lenovo XClarity Pro.** Enables advanced management functions (server configuration and OS deployment). A license is required in XClarity Orchestrator for each device that supports advanced-management functions.

License compliance is determined based on the number of managed devices. The number of managed devices must not exceed the total number of licenses in all active XClarity Pro license keys. When the number of XClarity Pro licenses is not compliant, you have a grace period of 90 days to install appropriate licenses. If the grace period (including the free trial) ends before the required number of licenses is installed, the server configuration and OS deployment functions are disabled for *all devices*.

For more information about XClarity Pro licenses, see [Licenses and the free 90-day trial](#) in the Lenovo XClarity Administrator online documentation.

- **XClarity Orchestrator Analytics.** Enables analytics functions. A license is required in XClarity Orchestrator for each device that supports advanced-management functions.

License compliance is determined based on the number of managed devices. The number of managed devices must not exceed the total number of licenses in all active XClarity Orchestrator Analytics license keys. When the number of XClarity Orchestrator Analytics licenses is not compliant (for example, if licenses expire or if managing additional devices exceeds the total number of active licenses), you have a grace period of 90 days to install appropriate licenses. If the grace period (including the free trial) ends before the required number of licenses is installed, the **Monitoring → Analytics** menus are disabled and you cannot view analytics reports or create custom alert rules and queries for *all devices*.

A license *is not* tied to specific devices.

The activation period starts when the licenses are redeemed.

Licenses are installed using a license *activation key*. After you redeem licenses, you can create an activation key for all or a subset of your available licenses, and then download and install the activation key in XClarity Orchestrator.

Each time XClarity Orchestrator becomes non-compliant, the grace period resets to 90 days.

If licenses are already installed, new licenses are *not* required when upgrading to a new release of XClarity Orchestrator.

If you are using a free trial license or if you have a grace period to become compliant, and you upgrade to a later version of XClarity Orchestrator, the trial license or grace period resets to 90 days.

When upgrading XClarity Orchestrator or if an error condition occurs that requires you to restore the activation keys, you can either use exported keys or download all activation keys (for each customer ID) from the [Features on Demand web portal](#), and then import the activation keys (either as individual activation keys or collectively as a key ZIP file) into XClarity Orchestrator.

You can view a list of your current software licenses from the [Features on Demand web portal](#).

## Procedure

To install XClarity Orchestrator licenses, complete the following steps.

- Step 1. Contact your Lenovo representative or authorized Business Partner to purchase licenses based on the number of devices that you want to manage.

After purchasing licenses, an authorization code is sent to you in an *electronic proof of entitlement* email. You can also retrieve the authorization code from the [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.

- Step 2. Retrieve the activation keys for the licenses.

- **Creating activation keys from an authorization code**

1. Open the [Features on Demand web portal](#) from a web browser, and log in to the portal using your email address as your user ID.
2. Click **Request activation key**.
3. Select **Input a Single Authorization Code**.
4. Enter the 22-character authorization code, and click **Continue**.
5. Enter your Lenovo customer number in the **Lenovo Customer Number** field.
6. 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.

7. Follow the prompts to enter product details and contact information, and click **Continue** to generate the activation key.
8. Optionally specify additional recipients to receive the activation keys.
9. 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 [Features on Demand web portal](#) by clicking **Download link**.

- **Downloading existing activation keys**

1. Open the [Features on Demand web portal](#) from a web browser, and log in to the portal using your email address as your user ID.
2. Click **Retrieve History**.
3. Select “Search history via Lenovo Customer Number” as the **Search type**.
4. Enter your Lenovo Customer number in the **Search Value** field. The customer number format is 121XXXXXXX.
5. Click **Select all** to download all activation keys or select individual activation keys from the list.
6. Click **Email** to email the keys to you, or click **Download** to download the keys to your local system.

- Step 3. Apply licenses in XClarity Orchestrator.

1. From the XClarity Orchestrator menu bar, click **Maintenance** (🔧), and then click the **Licenses** tab to display the License Information card.

Product	License Key Descript	Number of licenses	Expiration Date	Status
XClarity Orchestr...	Lenovo SYSTEM...	Unlimited	3/1/22	Expired
XClarity Orchestr...	Lenovo SYSTEM...	100000	3/1/20	Expired

2. Click the **Import and Apply** icon (📁) to apply the licenses.
3. Drag and drop the activation key file for the licenses that you want to apply to the Import dialog, or click **Browse** to locate the file.

To import multiple activation keys, compress the .KEY files into a ZIP file, and select the ZIP file for import.

4. Click **Import** to import and apply the licenses. When the installation is complete, the activation (license) key is listed in the table with the number of installed licenses and the activation period (start and expiration dates).

Step 4. If you applied the valid licenses after functions were disabled, log out and then log in again to enable the applicable functions.

## After you finish

You can perform the following actions from the License Information card.

- Save one or more selected activation keys to the local system by clicking the **Save** icon (↓).

When you export multiple activation keys, the files are downloaded as a single ZIP file.

- Delete a specific activation keys by clicking the **Delete** icon (🗑️).

## Getting help

- 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, authorization codes, or activation keys, or if they were sent to wrong person, contact one of the regional representatives, based on your geography.
  - [ESDNA@lenovo.com](mailto:ESDNA@lenovo.com) (North American countries)
  - [ESDAP@lenovo.com](mailto:ESDAP@lenovo.com) (Asia Pacific countries)
  - [ESDEMEA@lenovo.com](mailto:ESDEMEA@lenovo.com) (European, Middle Eastern, and Asian countries)
  - [ESDLA@lenovo.com](mailto:ESDLA@lenovo.com) (Latin American countries)
  - [ESDChina@Lenovo.com](mailto:ESDChina@Lenovo.com) (China)
- If information about my entitlement is not correct, contact Lenovo Support at [SW\\_override@lenovo.com](mailto: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

- If you have issues or questions about downloading the license, contact Lenovo Support at [LenovoSupport\\_Ops@lenovo.com](mailto:LenovoSupport_Ops@lenovo.com).





---

## Chapter 6. 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 [Port availability](#) and .

## Procedure

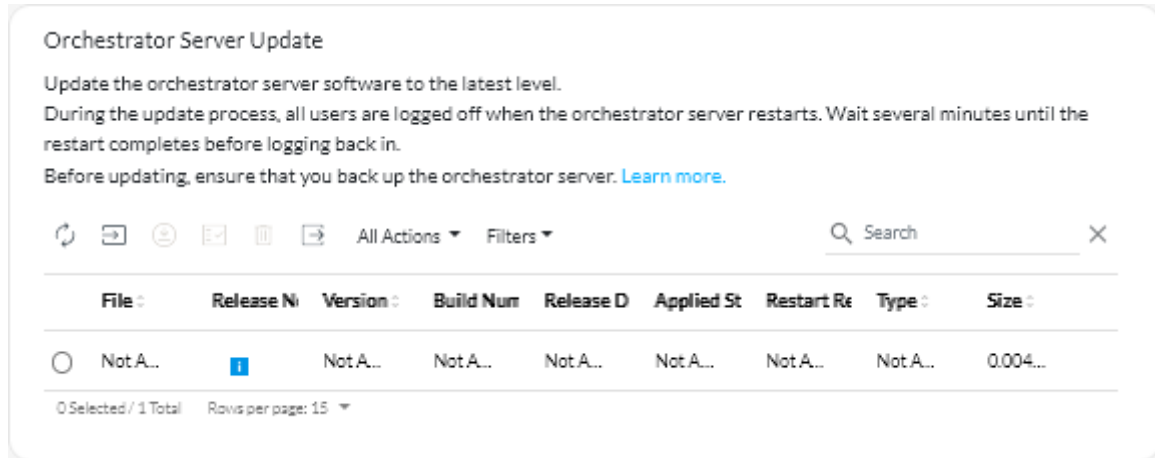
To update XClarity Orchestrator, complete the following steps.

- 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 7. Uninstalling XClarity Orchestrator

You can uninstall the Lenovo XClarity Orchestrator virtual appliance using the virtual-machine management tools.

### Procedure

To uninstall XClarity Orchestrator, complete the following steps.

Step 1. Disconnect and remove all resource managers.

- a. From the XClarity Orchestrator menu bar, click **Resources** (🔌) → **Resource Manager** to display the Resource Managers card.
- b. Select all resource managers.
- c. Click the **Delete** icon (🗑️).

Step 2. Uninstall XClarity Orchestrator using your virtual-machine management tools.

- **ESXi using VMware vCenter**

1. Connect to the host through VMware vCenter.
2. Right click the XClarity Orchestrator 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 XClarity Orchestrator 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 XClarity Orchestrator virtual machine, and click **Shut down**.
4. Right-click the virtual machine again, and click **Delete**.







**Lenovo**