Validated Profile: Cisco Catalyst Center on ESXi

Revised: January 30, 2024

Solution Overview

Catalyst Center on ESXi is a new form factor that supports the Catalyst Center application in a virtual environment. The virtual form factor helps customers rapidly deploy and operate Catalyst Center.

Catalyst Center on ESXi offers the same centralized and intuitive management as the Catalyst Center platform.

This guide provides technical guidance to design, deploy, and operate Catalyst Center on ESXi.

This guide contains the following main sections:

- *Solution Overview* presents a high-level overview of Catalyst Center on ESXi.
- *Design and Prerequisites* discusses the VMware ESXi prerequisites to deploy Catalyst Center on ESXi; requirements for creating the virtual appliance (VA); supported scale, latency, and bandwidth; launcher tool requirements; and how to set up network interfaces, NTP, and DNS servers for deployment of Catalyst Center on ESXi. The launcher tool is an internal Cisco utility used to deploy and configure the VA.
- *Deploy Catalyst Center on ESXi* discusses deployment of Catalyst Center on ESXi, different configuration methods, postdeployment configurations, configuration of authentication and policy servers, configuration of high availability (HA) using vSphere, backup and restore using local disk and NFS support, managing applications and software, and managing different user roles within Catalyst Center.
- *Operation: Monitoring and Troubleshooting* discusses how to monitor and troubleshoot the Catalyst Center VA deployed on ESXi.

The audience for this guide includes network design engineers and network operations personnel who don't have a Catalyst Center appliance but want to manage their networks with Catalyst Center.

Design and Prerequisites

This section explains the design and prerequisites for Catalyst Center on ESXi:

- Prerequisites for deployment

- Supported scale
- Certificate management for Catalyst Center on ESXi
- Launcher requirements for configuring Catalyst Center on ESXi
- Preparation of VMware vSphere; reservation of the enterprise interface; and preparation of DNS, NTP, and proxy servers
- Limitations and restrictions
- Feature support

Deployment Requirements

The following requirements must be met in order to successfully deploy a Catalyst Center on ESXi virtual appliance. For performance tips that cover the most performance-critical areas of VMware vSphere, see:

- VMware vSphere Client 7.0: *Performance Best Practices for VMware vSphere 7.0* (PDF)
- VMware vSphere Client 8.0: *Performance Best Practices for VMware vSphere 8.0* (PDF)

Virtual Machine Minimum Requirements

Table 1: Virtual Machine Minimum Requirements

Feature	Description
Virtualization platform and hypervisor	VMware vSphere (which includes ESXi and vCenter Server) 7.0.x or later, including all patches
Processors	Intel 2.1-GHz and later CPU 32 vCPUs with 64-GHz reservation must be dedicated to the VM
Memory	256-GB DRAM with 256-GB reservation must be dedicated to the VM
Storage	3-TB solid-state drive (SSD) If you plan to create backups of your virtual appliance, also reserve additional datastore space. For information, see "Backup Server Requirements" in the *Cisco Catalyst Center on ESXi Administrator Guide*.
I/O Bandwidth	180 MB/sec
Input/output operations per second (IOPS) rate	2000-2500, with less than 5 ms of I/O completion latency
Latency	Catalyst Center on ESXi to network device connectivity: 200 ms

Scale Numbers

The following tables list the number of devices and site elements that Catalyst Center on ESXi supports.

Table 2: Nonfabric Deployment Scale Numbers

Network Component	Maximum Number Supported
Access Points	4000
Devices	1000
Endpoints	25,000
Site Elements	2500

Table 3: Fabric Deployment Scale Numbers

Network Component	Maximum Number Supported
Endpoints	25,000
Devices	2000
Access Points	3000
Site Elements	2500
Per-Fabric Site Scale	
Fabric Nodes	500
VNs	64
IP Pools	100

For both nonfabric and fabric deployments, up to 10 concurrent user connections are supported for network admins to log in to Catalyst Center on ESXi.

Catalyst Center VA Launcher Requirements

If you plan to use the CC VA Launcher to deploy and configure a virtual appliance, the following requirements must be met by the machine on which you'll run the app:

Feature	Description
RAM	1 GB
Storage	• 40 GB for the virtual appliance's OVA file • 50 MB for the launcher bundle
Supported operating systems	• Linux: Ubuntu 20.04 and later • macOS (Intel and M1): macOS 14 and later • Microsoft Windows: Windows 10 and later
Sleep setting	Configure the machine to not go to sleep.

In addition to these requirements, do the following:

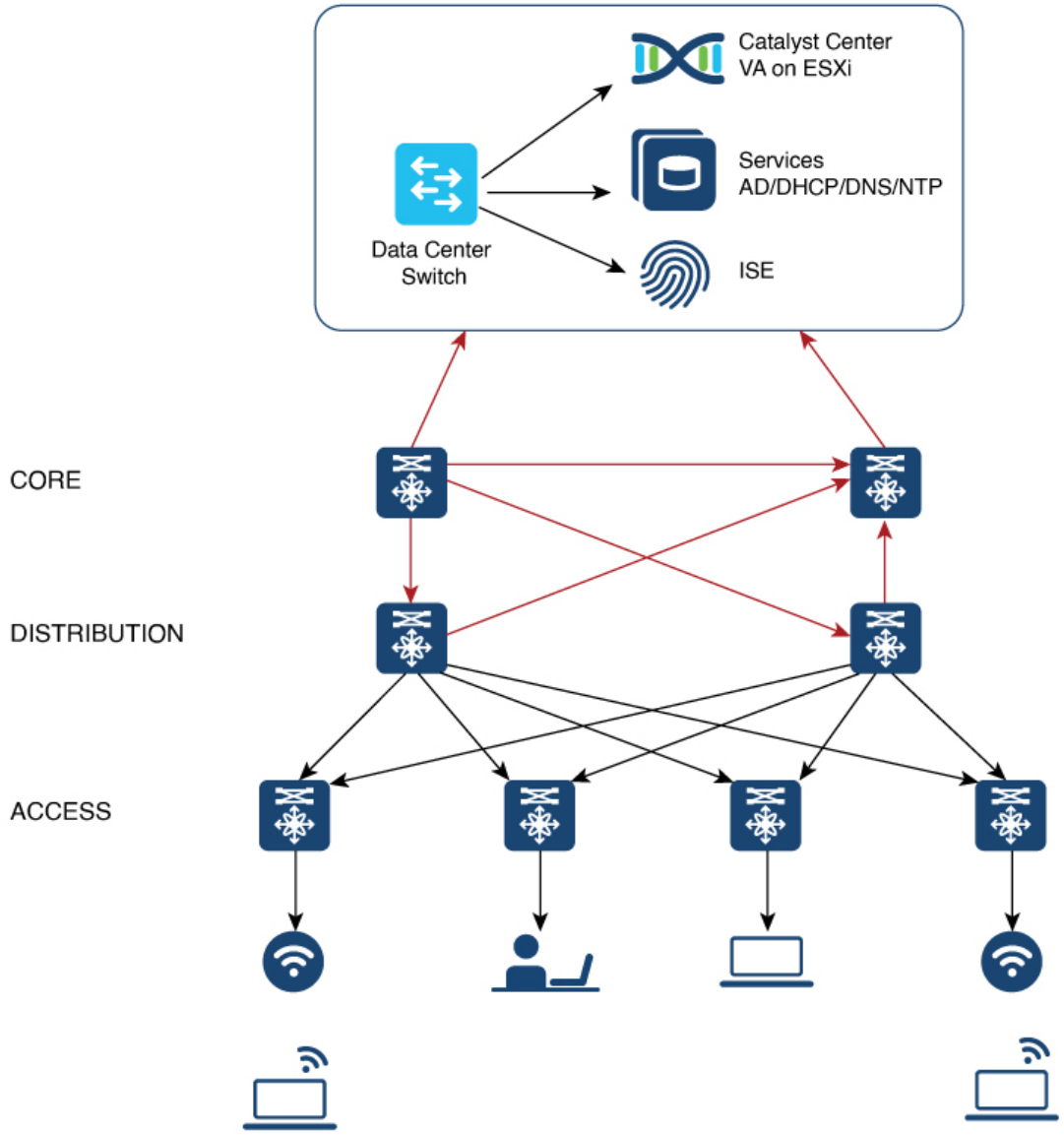
- Ensure that the user who will run the CC VA Launcher has the privileges necessary to deploy the virtual appliance's OVA file and modify the appliance's virtual machine settings.
- For the system you'll run the app on, configure its HTTP/network proxy settings (if applicable).

Supported Browsers

- Mozilla Firefox, version 65 or later
- Google Chrome, version 72 or later

Topology

Catalyst Center ESXi is located in the on-premises data center.



Prepare for Deployment

To prepare for the deployment of a Catalyst Center on ESXi virtual appliance, you'll need to complete the following tasks:

- Install VMware vSphere, on page 7.
- Reserve Enterprise Interface, on page 7.
- Prepare the DNS, NTP, and Proxy Servers, on page 8.
- Prepare for the Quick Start Workflow, on page 8.

Install VMware vSphere

To run, Catalyst Center on ESXi requires VMware vSphere (which includes ESXi and vCenter Server) 7.0.x or later, including all patches. Click here to access an overview of the VMware vSphere installation and setup process. After you have installed VMware vSphere, confirm that it can be reached from the computer that you will use to deploy the virtual appliance's OVA file.

Reserve Enterprise Interface

Before you set up the virtual appliance, ensure that you reserve one 1-Gbps/10-Gbps Enterprise interface to connect to and communicate with your enterprise network. Write down the IP address for this interface, because you'll need to enter it during appliance configuration.

Optionally, you can also reserve one 1-Gbps/10-Gbps Management network interface to access the Catalyst Center on ESXi GUI. Write down this interface's IP address as well if you plan to configure it.

Note the following points:

- The intracluster interface's IP address is predefined, so you won't need to enter it when you complete either the Maglev Configuration wizard with default mode selected or the browser-based Install Configuration wizard.
- Catalyst Center on ESXi supports the configuration of one additional interface for use by the virtual appliance. If you do so, make sure that you choose **VMXNET** from the **Adapter Type** drop-down list. Otherwise, appliance configuration will not complete successfully. For more information, see the Add a Network Adapter to a Virtual Machine topic in vSphere Virtual Machine Administration.

Import the IdenTrust Certificate Chain

The Catalyst Center on ESXi OVA file is signed with an IdenTrust CA certificate, which is not included in VMware's default truststore. As a result, the **Deploy OVF Template** wizard's **Review details** page will indicate that you are using an invalid certificate while completing the wizard. You can prevent this by importing the IdenTrust certificate chain to the host or cluster on which you want to deploy the OVA file.

Procedure

Step 1 On the VMware ESXi host or cluster where your virtual appliance will reside, download **trustidevcodesigning5.pem** from the same location that Cisco specified to download the Catalyst Center on ESXi OVA file.

Step 2 Unzip this file.

Step 3 Log in to the vSphere Web Client.

Step 4 Choose **Administration** > **Certificates** > **Certificate Management**.

Step 5 In the **Trusted Root Certificates** field, click **Add**.

Step 6 In the **Add Trusted Root** dialog box, click **Browse**.

Step 7 Navigate to and select the certificate chain that you downloaded in Step 1 (**trustidevcodesigning5.pem**), then click **Open**.

Step 8 Check the **Start Root certificate push to vCenter Hosts** check box, then click **Add**.

A message indicates that the certificate chain was imported successfully.

When you complete the **Deploy OVF Template** wizard, the **Review details** page's **Publisher** field should indicate that you are using a trusted certificate.

Prepare the DNS, NTP, and Proxy Servers

You'll be prompted to specify three items:

- The Domain Name System (DNS) server that Catalyst Center on ESXi will use to convert domain names to IP addresses.
- The Network Time Protocol (NTP) server that Catalyst Center on ESXi will use for clock synchronization.
- **(Optional)** The proxy server that Catalyst Center on ESXi will use to access internet-bound URLs.

Before you configure your virtual appliance, do the following:

- Ensure that the servers you want to use are available and running.
- For an NTP server, obtain its IP address or hostname. And for a proxy server, collect either its URL or hostname and its login credentials.

Prepare for the Quick Start Workflow

After you create a virtual machine on an ESXi host and configure a Catalyst Center on ESXi virtual appliance, you'll be prompted to complete the Quick Start workflow. By completing this workflow, you'll discover the devices that Catalyst Center on ESXi will manage and enable the collection of telemetry from those devices. To complete this workflow successfully, you'll need to perform the following tasks:

- Decide on the username and password for the new admin user you're going to create. The default admin username and password (**admin/maglev1@3**) should only be used the very first time you log in to Catalyst Center on ESXi.

  Important Changing this password is critical to network security, especially when the people who set up a Catalyst Center on ESXi virtual appliance are not the same people who will serve as its administrators.

- Obtain the credentials you use to log in to Cisco.com.
- Identify the users who need access to your system. For these users, define their roles as well as unique passwords and privilege settings.

You have the option to use an IPAM server and Cisco Identity Services Engine (ISE) with your virtual appliance. If you choose to use one or both of them, you'll also need to obtain the relevant URL and login credentials.

Enable Storage Input/Output Control

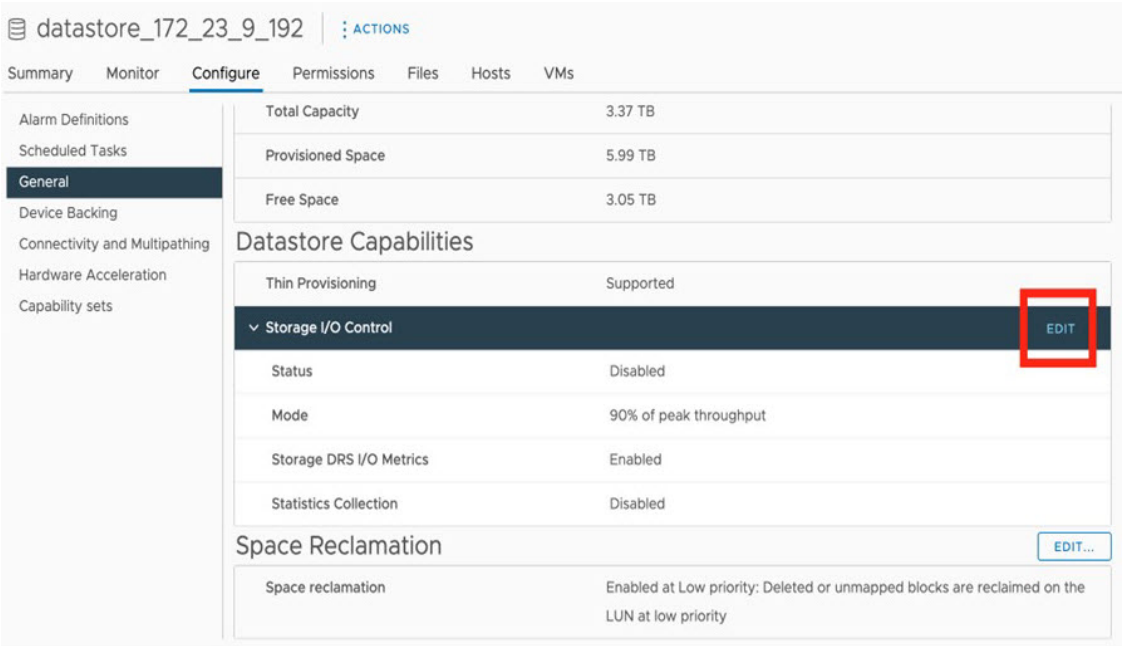
For the datastore in which you are planning to deploy a virtual appliance, complete the following procedure so the appliance's virtual machine input/out (I/O) is prioritized over other virtual machines when the network is experiencing I/O congestion.

Procedure

Step 1 In the vSphere Client, navigate to and click the datastore in which you plan to deploy a virtual appliance.

Step 2 Click the **Configure** tab, then click **General**.

Step 3 In the **Datastore Capabilities** area, click **Edit**.



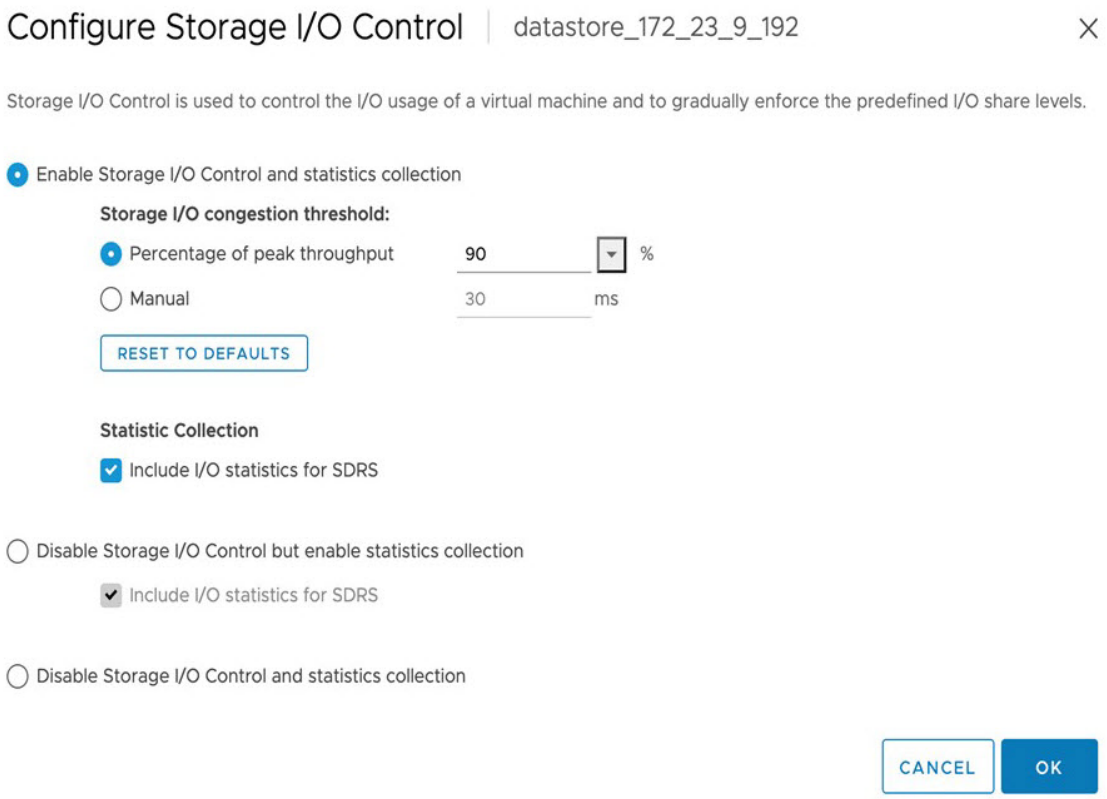
Step 4 In the **Configure Storage I/O Control** window, do the following:

a) Click the **Enable Storage I/O Control and statistics collection** radio button.

b) In the **Storage I/O congestion threshold** area, configure the congestion threshold you want to use.

You can either specify a peak throughput percentage or enter a value (in milliseconds).

c) (Optional) In the **Statistic Collection** area, check the **Include I/O statistics for SDRS** check box.



Step 5 Click **OK**.

Check HA Admission Control Setting

You cannot connect Catalyst Center on ESXi VMs to create three-node clusters. If you want to enable high availability (HA), you'll need to use VMware vSphere's HA functionality and enable strict admission control to ensure that:

- A virtual machine cannot be powered on if it will result in the violation of availability constraints.
- Configured failover capacity limits are enforced.
- HA operates as expected during a failover.

For more information, in the *Cisco Catalyst Center on ESXi Administrator Guide*, see the "High Availability" section in the "Configure System Settings" chapter.

Limitations and Restrictions

Catalyst Center on ESXi has the following limitations and restrictions:

- Unlike the Catalyst Center platform, you cannot connect VMs to create three-node clusters. To achieve high availability, you need to use VMware vSphere. For more information, in the *Cisco Catalyst Center on ESXi Administrator Guide*, see the "High Availability" section in the "Configure System Settings" chapter.
- Catalyst Center on ESXi does not support the following VMware vSphere features:
    - Fault tolerance

- Suspending and resuming VMs
- Cloning VMs
- Snapshot (as backup)
- NIC bonding

Features Support

Catalyst Center on ESXi supports all of the features that Catalyst Center supports, except for the following features:

- **Automation**: Cisco Wide Area Bonjour application, Cisco vManage for SD-WAN, Cisco DNA Traffic Telemetry Appliance, Cisco Secure Network Analytics.
- **Wireless**: Cisco User-Defined Network (UDN), Cisco Umbrella.
- **Assurance**: Sensor.
- **System Workflows**: Backup and Restore using VMware vSphere Client snapshot function, Backup and Restore from Catalyst Center hardware appliance to Catalyst Center on ESXi virtual appliance.
- **Diagnostics Center**: Validation Tool under **System** > **System Health** > **Tools**.
- **Setting Page**: Authentication API Encryption.
- **Security Policy Access (SPA)**: Security Sensor in Endpoint Analytics, Group-Based Policy Analytics (GBPA).

Deploy Catalyst Center on ESXi

The following sections explain how to deploy a VM on Catalyst Center on ESXi, power up the VM, configure the virtual appliance, and complete the Quick Start workflow.

The process to deploy Catalyst Center on ESXi and complete day-1 and day-*n* operations involves:

- Create a VM
- Configure the Catalyst Center on ESXi virtual appliance
- Complete the Quick Start workflow
- Postdeployment considerations
- Configure authentication and policy servers
- HA using vSphere
- Backup and restore
- Software management
- Manage user access

Create a Virtual Machine

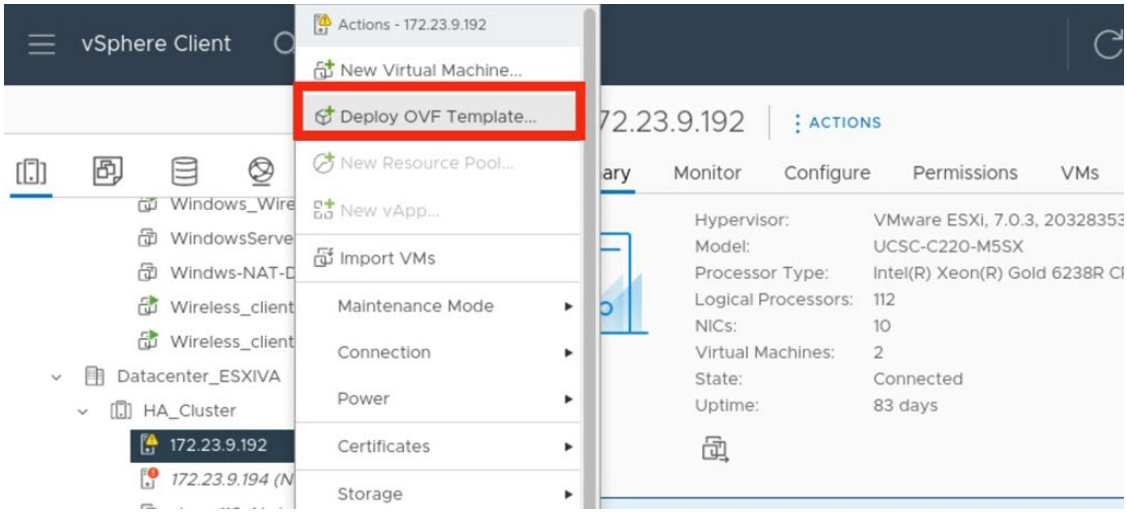
Complete the following procedure to create a virtual machine on the VMware ESXi host or cluster where your virtual appliance will reside.

Procedure

Step 1 Download the Catalyst Center on ESXi OVA file from the location specified by Cisco.

Step 2 Log in to the vSphere Web Client.

Step 3 In the navigation pane, right-click the IP address of host or cluster on which you want to deploy the OVA file and then click **Deploy OVF Template**.

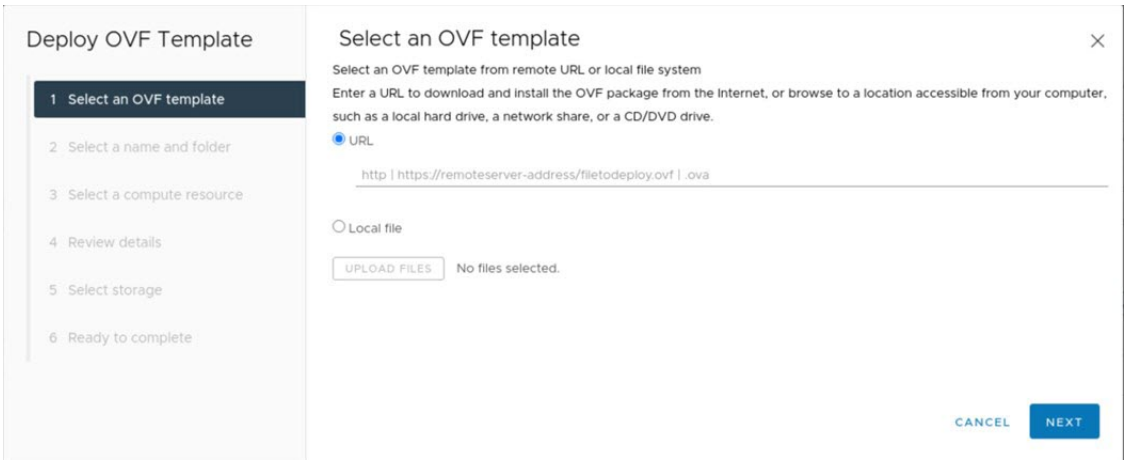


Step 4 Complete the **Deploy OVF Template** wizard:

a) In the **Select an OVF Template** wizard page, specify the OVA file you want to use for deployment and then click **Next**. You can either:

- Click the **URL** radio button and enter the appropriate path and OVA filename. If you choose this option, ensure that the OVA file is stored in and shared from a web-accessible location.
- Click the **Local file** radio button, click **Upload Files**, and then navigate to and select the appropriate OVA file.

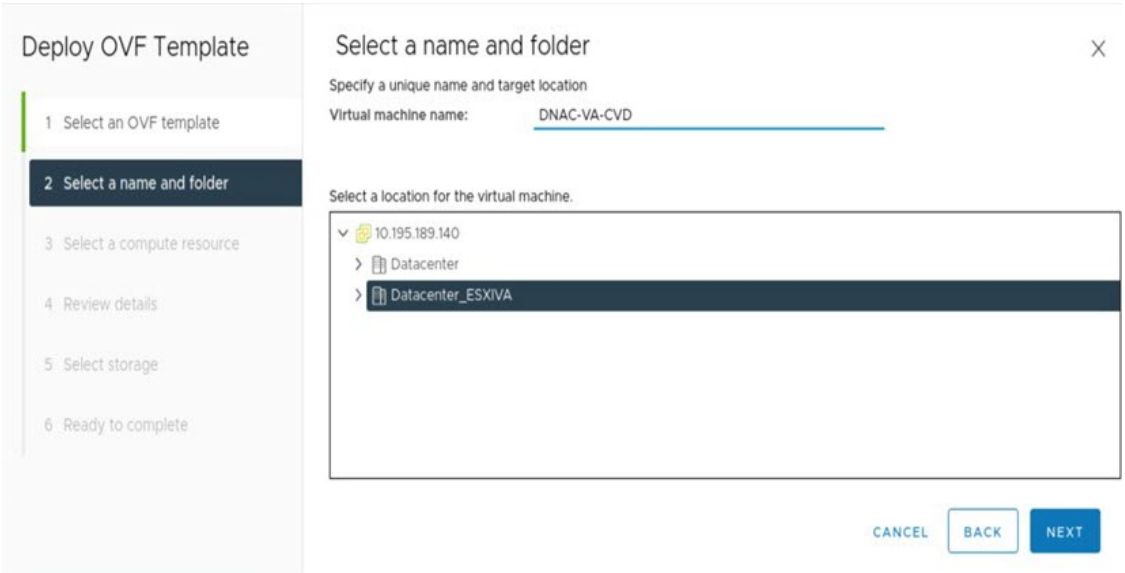
The wizard's **Select a name and folder** page opens. By default, the OVA's filename is set as the name of the virtual machine you're about to create. Also, the location where the ESXi host or cluster you selected in Step 3 resides is set as the deployment location.



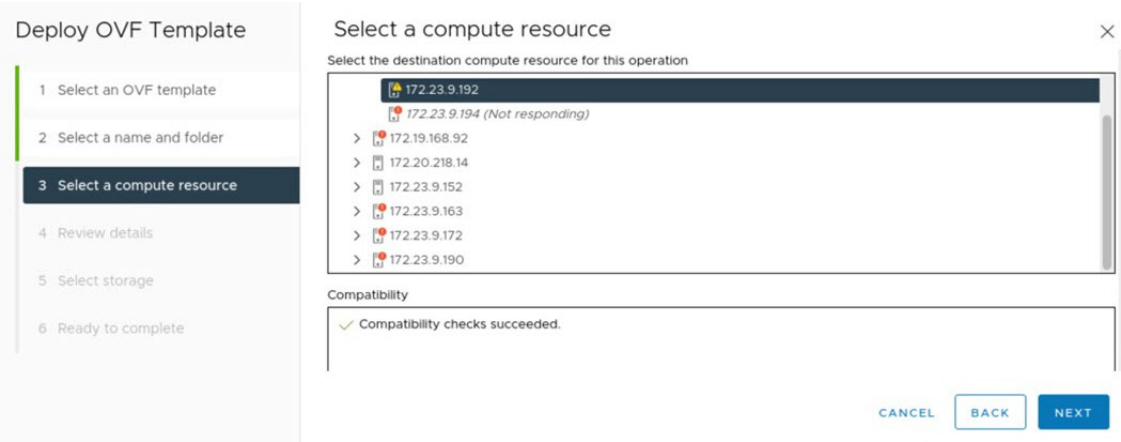
b) If you want to use the default values, click **Next** and proceed to Step 4c.

If you want to use different values, do the following:

1. Enter a name for the virtual machine you are creating.
2. Specify where the virtual machine will reside.
3. Click **Next**.

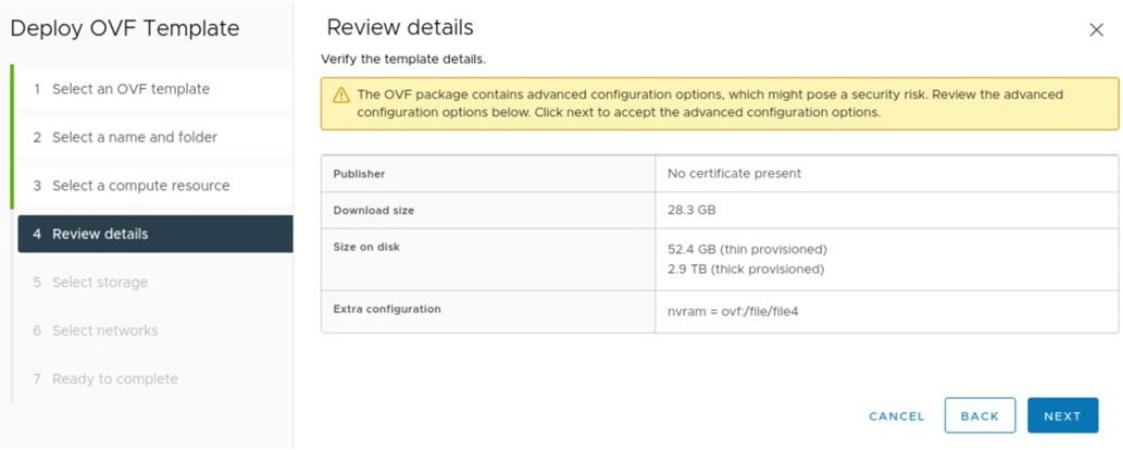


The wizard's **Select a compute resource** page opens.



c) Click the ESXi host or cluster on which you want to deploy the OVA file (the same one you right-clicked in Step 3), then click **Next**.

A page that lists deployment template details is displayed.

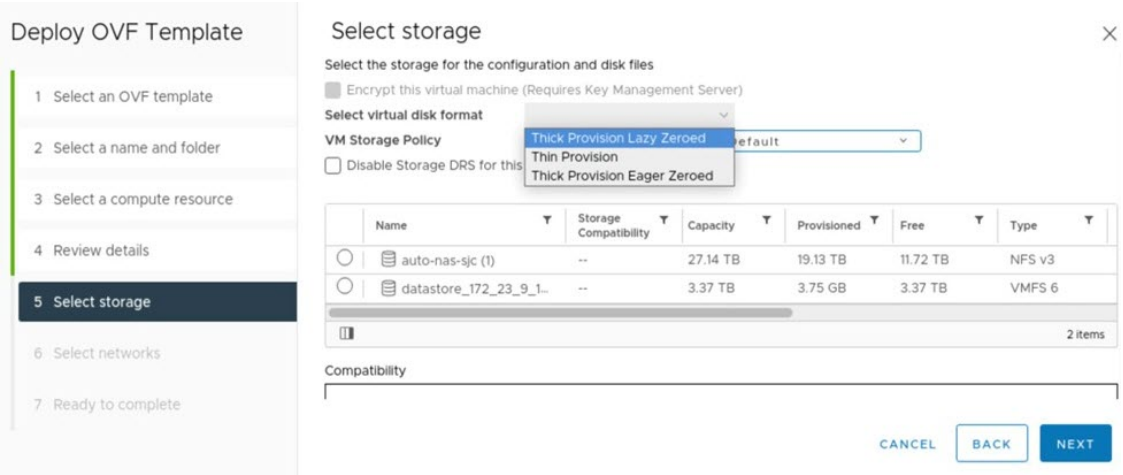


d) Review the template details and then do one of the following:

- If you need to make any changes, click **Back** as needed to return to the appropriate wizard page.
- If you want to proceed, click **Next**.

Note Ignore the information provided in the **Extra configuration** field. This refers to additional configurations that Cisco provides in the Catalyst Center on ESXi OVA file.

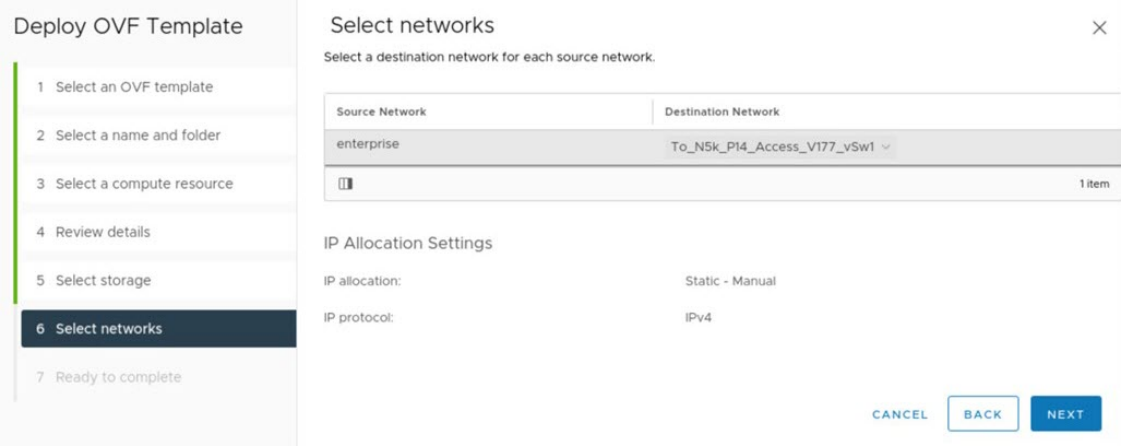
The wizard's **Select storage** page opens.



e) Do the following:

1. Click the radio button for the storage device you want to use.
2. In the **Select virtual disk format** field, choose either the **Thick Provision** or **Thin Provision** option.
3. Click **Next**.

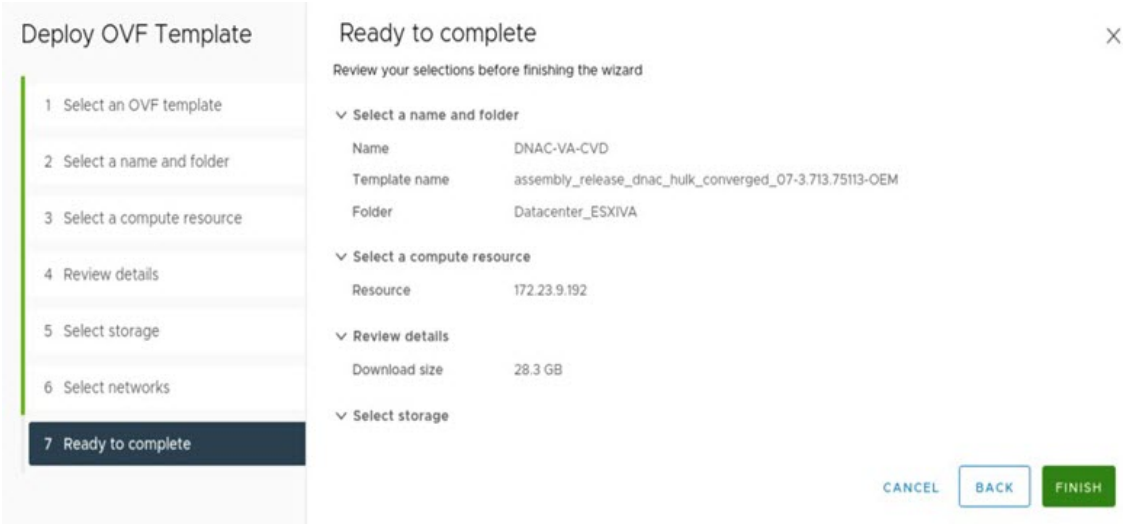
The wizard's **Select networks** page opens.



f) Do the following:

1. In the Enterprise Network's **Destination Network** drop-down list, choose the network that will connect to Catalyst Center on ESXi's Enterprise interface.
2. Click **Next**.

A summary of the deployment settings you've entered is displayed by the **Ready to complete** wizard page.



g) Review the settings, then do one of the following:

- If you need to make any changes, click **Back** as needed to return to the appropriate wizard page.
- If you want to proceed with deployment, click **Finish**.

Important In general, deployment takes around 45 minutes to complete. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.

Configure an Additional Network Adapter

Complete the following procedure in order to configure an additional network adapter for your virtual appliance, on which the Management interface will reside.

Procedure

Step 1 Log in to the vSphere Web Client.

Step 2 In the navigation pane, right-click the virtual machine you've created, then choose **Power** > **Power Off**.

Step 3 Right-click the virtual machine and then choose **Actions** > **Edit Settings**.

Step 4 With the **Virtual Hardware** tab selected, click **Add New Device** and then choose **Network Adapter**.

Step 5 In the **New Network** field's drop-down list, click **Browse**.

Step 6 In the **Select Network** dialog box, choose the network that will connect to the virtual appliance's Management interface and then click **OK**.

Step 7 In the **Adapter Type** field's drop-down list, choose **VMXNET3** and then click **OK**.

Step 8 In the navigation pane, right-click the virtual machine, then choose **Power** > **Power On**.

Step 9 Do one of the following:

- If you haven't done so already, Configure a Catalyst Center on ESXi Virtual Appliance using one of the available configuration wizards or the CC VA Launcher.

- If you've already configured the virtual appliance, proceed to Step 10.

Step 10 After Catalyst Center on ESXi comes up, run the Configuration wizard to configure the settings for the Management interface:

a) Open an terminal window to the virtual machine and run the **sudo maglev-config update** command.

The Configuration wizard opens, displaying the settings that have already been configured for the appliance's Enterprise interface.

b) Click **next>>**.

The settings that have already been configured for the appliance's Intracluster interface are now displayed.

c) Click **next>>**.

d) For the Management interface (NETWORK ADAPTER #3) you just created, enter the appropriate values for the following parameters and then click **next>>**:

- **Host IPv4/IPv6 Address** field: Enter the IP address for the Management interface.
- **IPv4 Netmask/IPv6 Prefix Length** field: Enter the netmask for the interface's IP address.
- **Default Gateway IPv4/IPv6 Address** field: Enter the default gateway IP address to use for the interface.
- **IPv4/IPv6 Static Routes** field: Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*.

Configure the Management Network (Day 0)

By default, the Catalyst Center OVA comes with only one interface, the Enterprise interface. To add the management network to the appliance, you can add the interface after creating the virtual machine as part of the day-0 operations. Alternately, you can add the interface after the deployment as part of day-*n* operations, and configure it using the Maglev Configuration wizard.

To add the additional network interface as part of day-0 operations, complete the following procedure.

Procedure

Step 1 If the Catalyst Center VM is running, do a graceful shutdown.

Step 2 Click the deployed Catalyst Center VM and choose **Actions** > **Edit Settings**.

Step 3 Click **ADD NEW DEVICE** and choose **Network Adapter**.

After you click **Network Adapter**, new network adapter is added to the VM.

Step 4 Select the network to use for the management network for the newly added adapter.

Step 5 For the adapter type, choose **VMXNET3** and click **OK**.
The new adapter is added and associated to the selected network.

Step 6 Power on the Catalyst Center VM.

Configure the Management Network (Day N)

By default, the Catalyst Center OVA comes with only one interface, the Enterprise interface. You can add the management interface after the deployment as part of day-*n* operations, and configure it using the Maglev Configuration wizard.

This procedure explains how to add the additional network interface as part of day-*n* operations.

After Catalyst Center is up, open the vSphere UI terminal of the VM and run the **sudo maglev-config update** command to start the network configuration wizard. The following steps apply to VMs that are already configured with a single NIC and a second NIC is added as part of day-*n* operations. If you add a second NIC for management before powering on the VM with the preceding method of **Actions** > **Edit Settings**, complete the following section to configure Catalyst Center using different configuration methods.

Procedure

Step 1	In the vSphere Client, click the deployed Catalyst Center VM and choose **Launch Console**. The Maglev wizard opens, where you configure the newly added management interface.
Step 2	At the initial screen, the wizard prompts you to configure the **enterprise** interface. If it's configured already, click **Next**.
Step 3	At the cluster interface configuration screen, click **Next**.
Step 4	The wizard prompts you to configure the newly added management interface. Enter the appropriate parameters (IP address, subnet mask, and so on) and click **Next**.
Step 5	The wizard prompts you to configure network parameters such as proxy, DNS, and NTP servers. Enter the appropriate parameters and click **Next**.
Step 6	Access the Catalyst Center UI by using the configured management network IP.

Configure a Catalyst Center on ESXi Virtual Appliance

After powering on the VM, complete one of the following procedures to configure a Catalyst Center on ESXi virtual appliance on a VMware ESXi host. All of the following configuration procedures occur *after* adding the management interface to the VM using the **Actions** > **Edit Settings** option.

- Configure a Virtual Appliance Using the Maglev Configuration Wizard: Default Mode, on page 18
- Configure a Virtual Appliance Using the Maglev Configuration Wizard: Advanced Mode for IPv4 Deployments, on page 31
- Configure a Virtual Appliance Using the Maglev Configuration Wizard: Advanced Mode for IPv6 Deployments, on page 48
- Configure a Virtual Appliance Using the Web UI Install Configuration Wizard, on page 65
- Configure a Virtual Appliance Using the Web UI Advanced Install Configuration Wizard for IPv4 Deployments, on page 77
- Configure a Virtual Appliance Using the Web UI Advanced Install Configuration Wizard for IPv6 Deployments, on page 87
- Configure a Virtual Appliance Using the Interactive CC VA Launcher, on page 99
- Configure a Virtual Appliance Using the CC VA Launcher in Silent Mode, on page 105

Configure a Virtual Appliance Using the Maglev Configuration Wizard: Default Mode

If you want to configure a virtual appliance as quickly as possible using the Maglev Configuration wizard and are okay with using preset appliance settings, complete the following procedure.

Note The Intracluster interface is preconfigured when using this wizard. If you don't want to use the default settings for this interface, you'll need to complete the Configure a Virtual Appliance Using the Maglev Configuration Wizard: Advanced Mode for IPv4 Deployments.

Before you begin

Gather the following information for the virtual appliance before you start this procedure:

- Static IP address
- Subnet mask
- Default gateway
- DNS address
- NTP server details
- Proxy server details

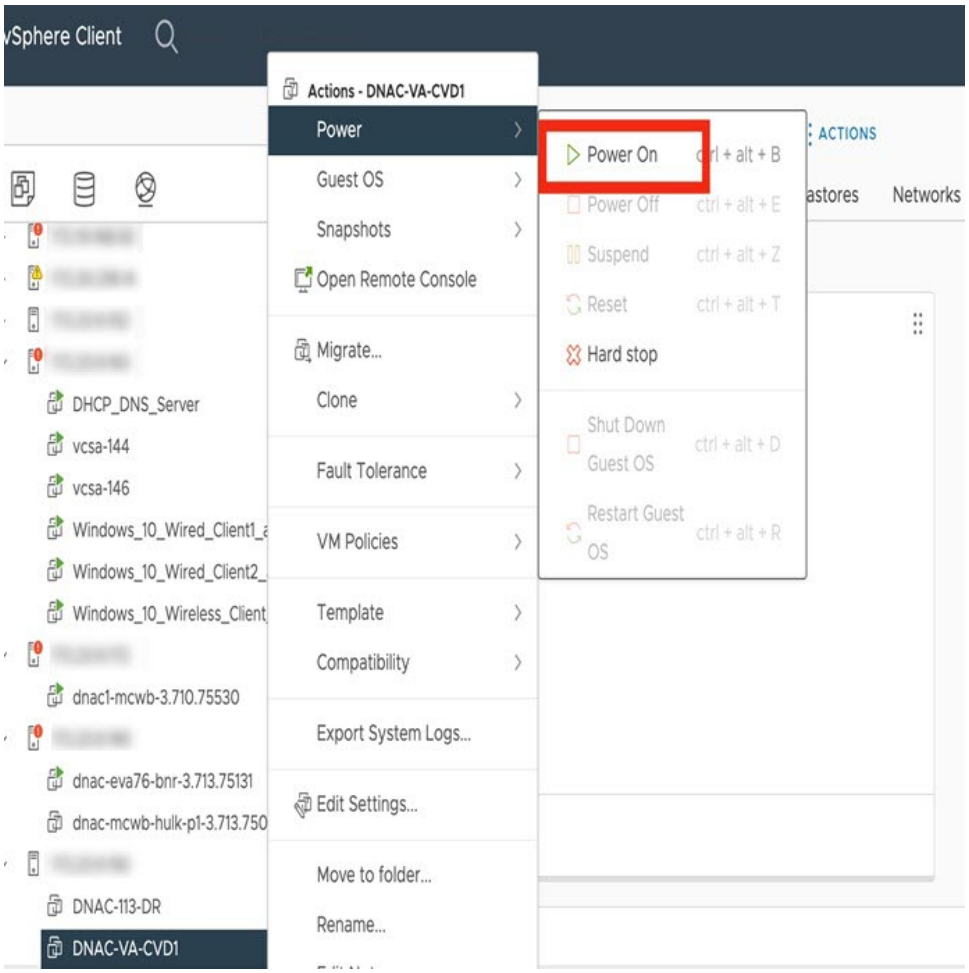
Important If you plan to configure the appliance's Management interface, also Configure an Additional Network Adapter for this interface to reside on before you start this wizard.

Procedure

Step 1 After deployment completes, power on the newly-created virtual machine:

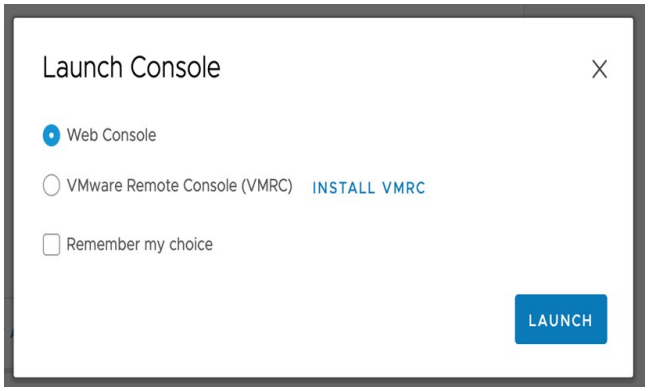
a) In the vSphere Client, right-click the virtual machine.

b) Choose **Power** > **Power On**.



It takes around 45 minutes for the virtual machine to become operational. The actual time will depend on things like available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the VMware VM Console.

Step 2 Launch either the remote console or web console by clicking the appropriate link.

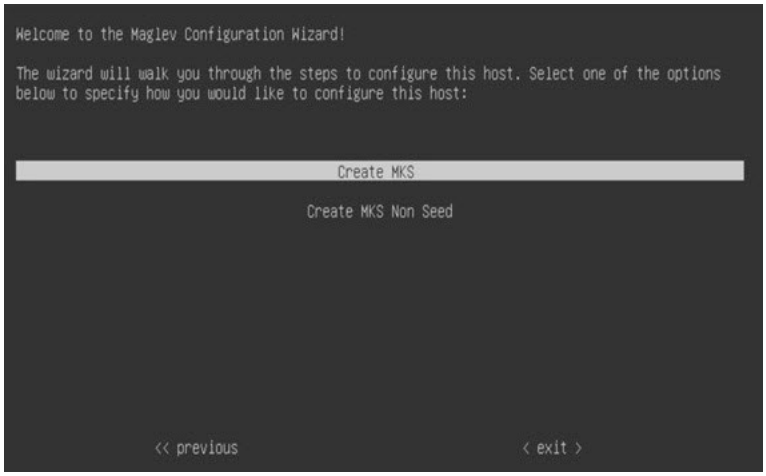


Step 3 Configure the virtual machine by completing the Maglev Configuration Wizard:

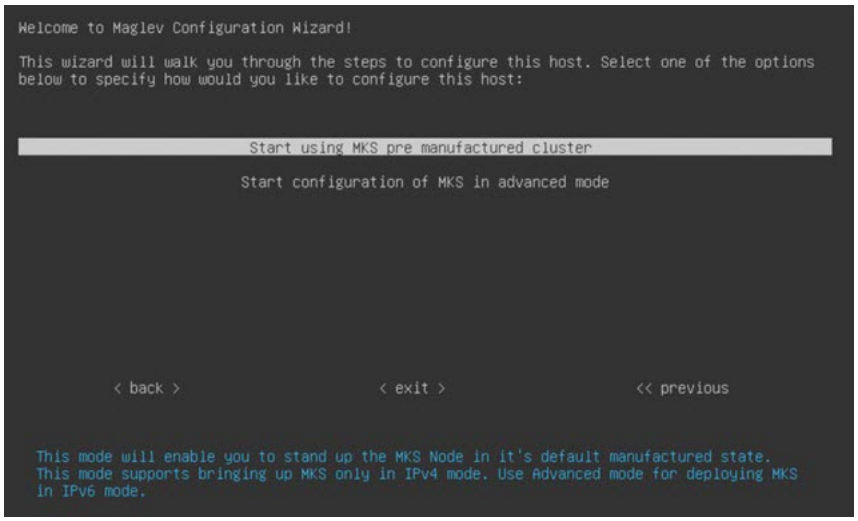
a) You don't need to enter any settings in the wizard's **STATIC IP CONFIGURATION** page, so click **skip>>**.

Static IP settings only need to entered when you configure a virtual appliance using a browser-based web UI mode of installation.

b) Click **Create MKS**.



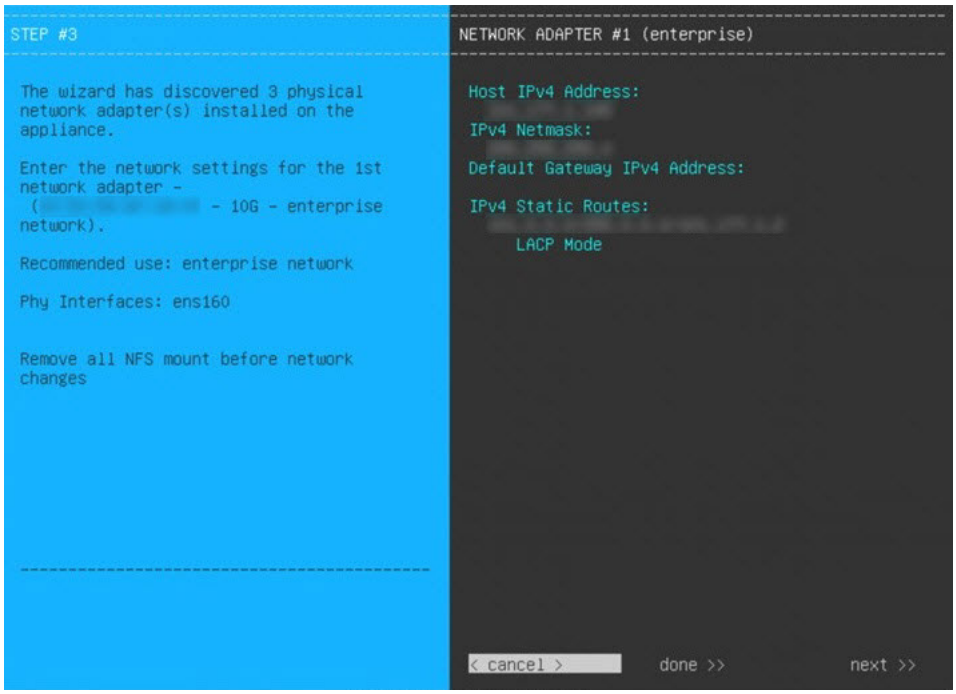
c) Click the **Start using MKS pre manufactured cluster** option.



d) Enter the configuration values for **NETWORK ADAPTER #1**, as shown in the following table, then click **next>>**.

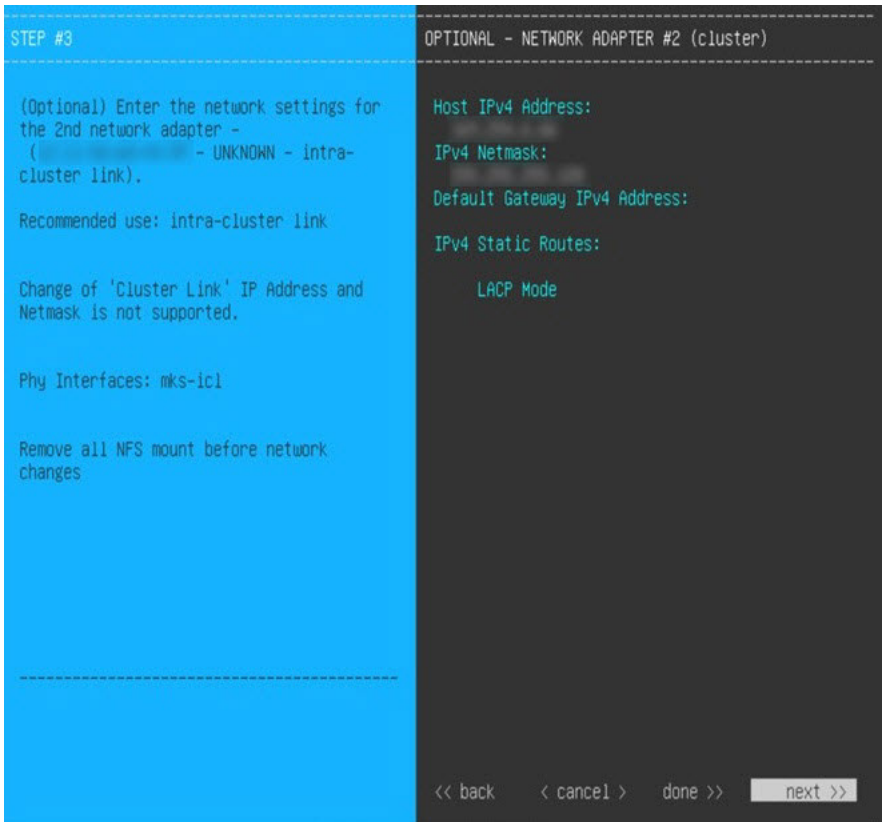
Catalyst Center on ESXi uses this interface to link the virtual appliance with your network.

Host IPv4 Address field	Enter the IP address for the Enterprise interface. This is required.
IPv4 Netmask field	Enter the netmask for the interface's IP address.
Default Gateway IPv4 Address field	Enter a default gateway IP address to use for the interface. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Catalyst Center on ESXi Management interface only.
LACP Mode field	Leave this field blank, as it's not applicable to virtual appliances.



The wizard validates the values you entered and issues an error message if any are incorrect. If you receive an error message, check that the value you entered is correct, then reenter it. If necessary, click **<<back** to reenter it.

e) You don't need to enter configuration values for **NETWORK ADAPTER #2**, as the **Host IPv4 Address** and **IPv4 Netmask** fields are prepopulated for the Intracluster interface. Click **next>>** to proceed.



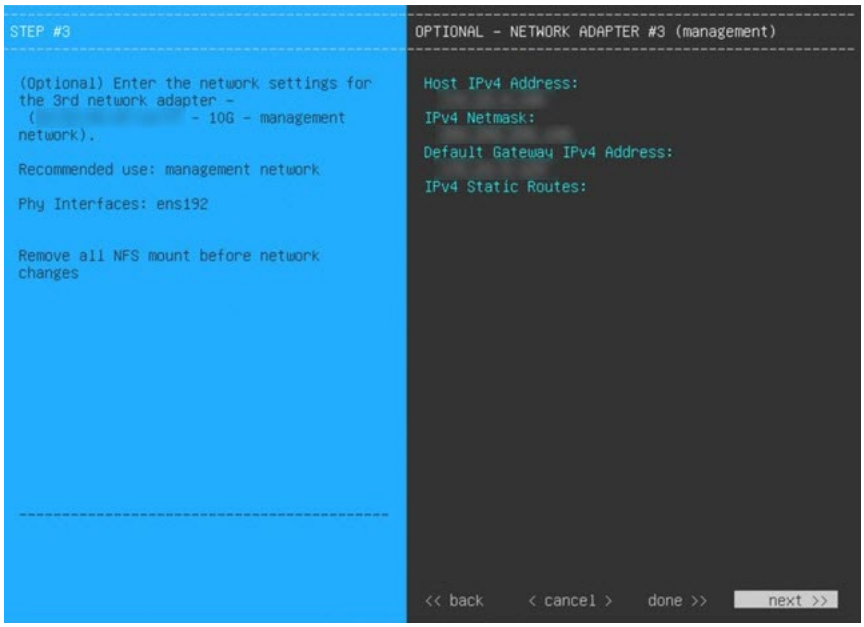
f) Enter the configuration values for **NETWORK ADAPTER #3**, as shown in the following table, then click **next>>**.

This interface allows you to access the Catalyst Center on ESXi GUI from the virtual appliance.

Note You will see this wizard page only if you have already Configure an Additional Network Adapter for the Management interface.

Host IPv4 address field	Enter the IP address for the Management interface. This is required only if you are using this interface to access the Catalyst Center on ESXi GUI from your management network; otherwise, you can leave it blank.
IPv4 Netmask field	Enter the netmask for the interface's IP address.
Default Gateway IPv4 Address field	Enter a default gateway IP address to use for the interface. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*.

Correct validation errors, if any, to proceed. The wizard validates and applies your network adapter configurations.

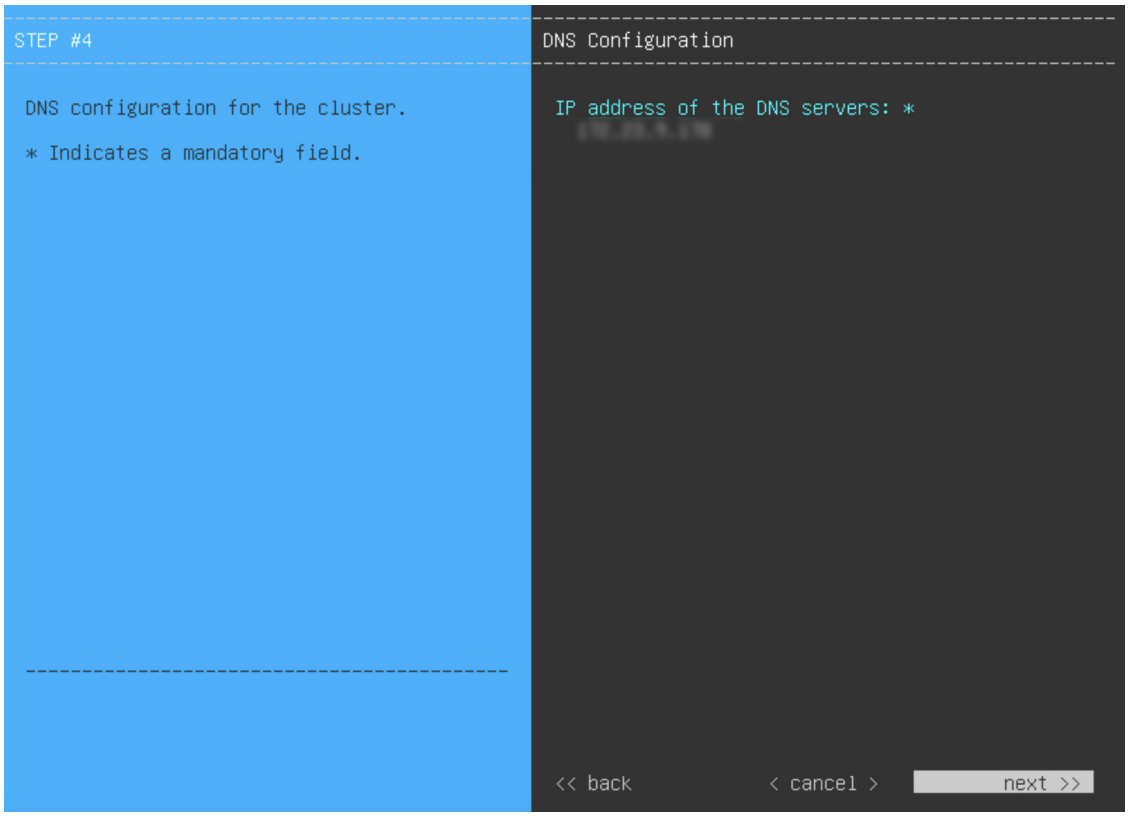


g) In the **DNS Configuration** page, enter the IP address of the preferred DNS server and then click **next>>**. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.

Important

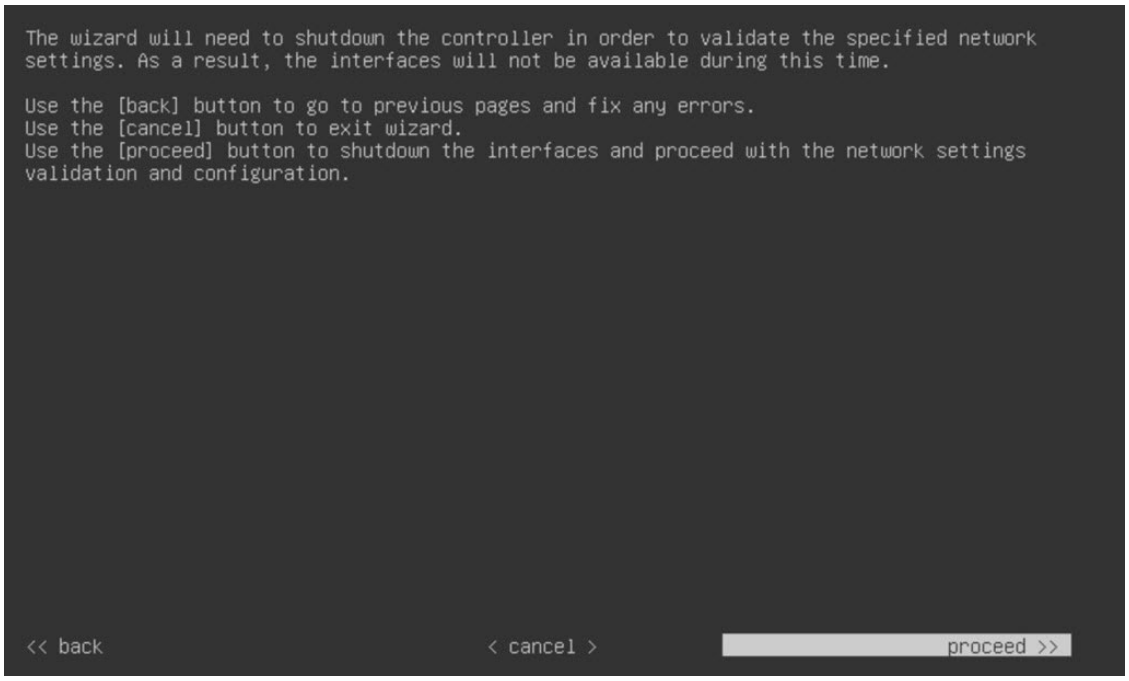
- For NTP, ensure port 123 (UDP) is open between Catalyst Center on ESXi and your NTP server.
- Configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for a virtual appliance.

The wizard updates, indicating that it needs to shut down the controller in order to validate the settings you've entered so far.



h) Do one of the following:

- If you need to change any settings, click **<<back** as needed, make the necessary changes, and then return to this wizard page.
- If you're happy with the settings you've entered, click **proceed**>>.

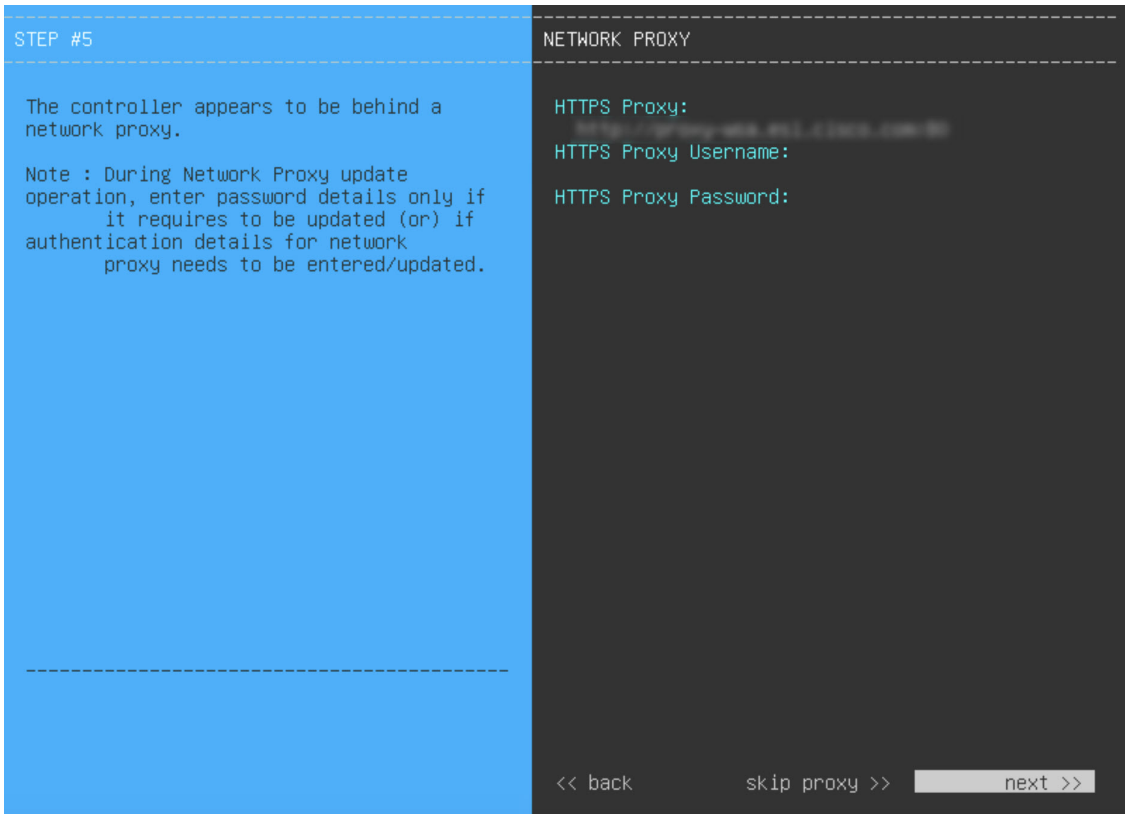


i) After validation successfully completes, do one of the following:

- If your network does *not* use a proxy server to access the internet, click **skip proxy>>** to proceed.
- If your network does use a proxy server, enter the configuration values in the **NETWORK PROXY** wizard page (as shown in the following table), then click **next>>**.

HTTPS Proxy field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** Connection from Catalyst Center on ESXi to the HTTPS proxy is supported only through HTTP in this release.
HTTPS Proxy Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
HTTPS Proxy Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

After you provide the necessary information, correct any validation errors to proceed (if necessary).

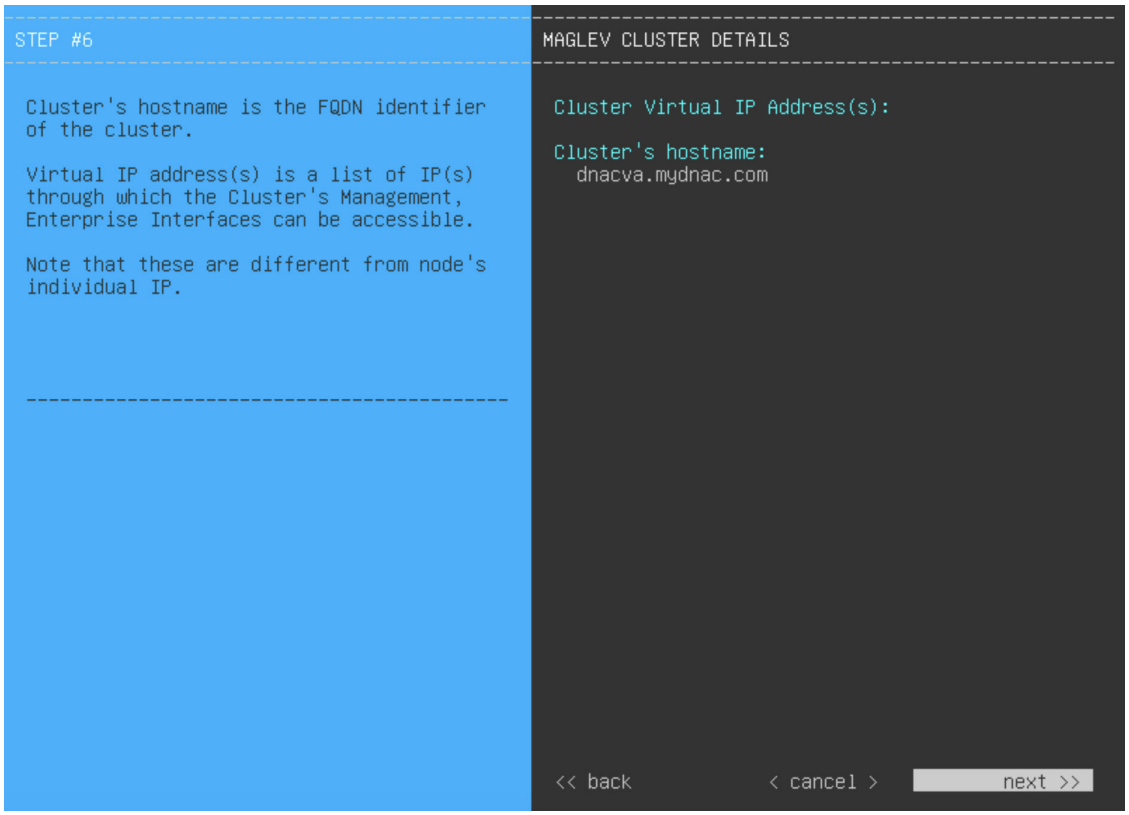


j) You are next prompted to enter the virtual appliance's virtual IP address in the **MAGLEV CLUSTER DETAILS** wizard page. Enter the virtual IP address configured for the Enterprise interface. If you configured a virtual IP address for the Management interface, enter this address as well (using a comma to separate the two IP addresses).

You can also specify the fully qualified domain name (FQDN) for your virtual appliance. Catalyst Center on ESXi uses this domain name to do the following:

- It uses this hostname to access your virtual appliance’s web interface and the Representational State Transfer (REST) APIs used by devices in the enterprise network that Catalyst Center on ESXi manages.
- In the Subject Alternative Name (SAN) field of Catalyst Center on ESXi certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.

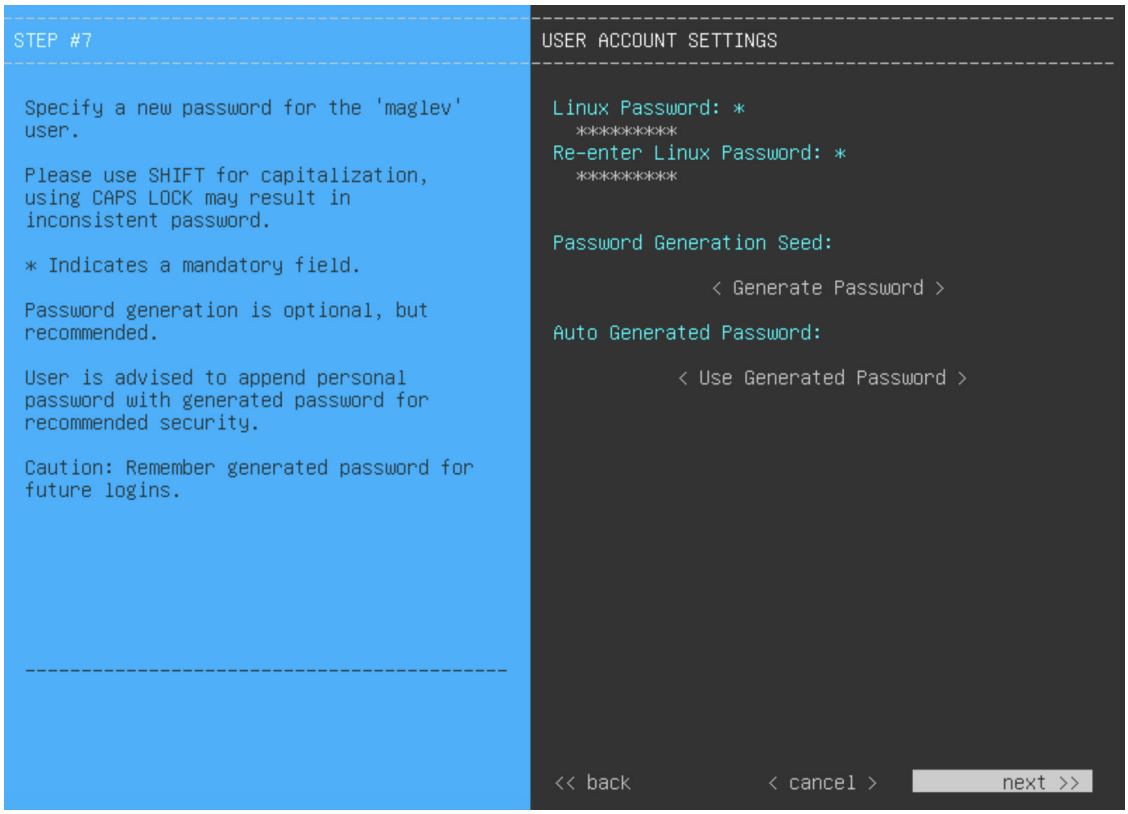
After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.



k) Enter the configuration values for the settings provided in the wizard's **USER ACCOUNT SETTINGS** page (as described in the following table), then click **next>>**.

Linux Password field	Enter and confirm the password for the `maglev` user.
Re-enter Linux Password field	Confirm the Linux password by entering it a second time.
Password Generation Seed field	If you do not want to create the Linux password yourself, enter a seed phrase in this field and then press <**Generate Password**> to generate the password.
Auto Generated Password field	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto-generated password. Press <**Use Generated Password**> to save the password.

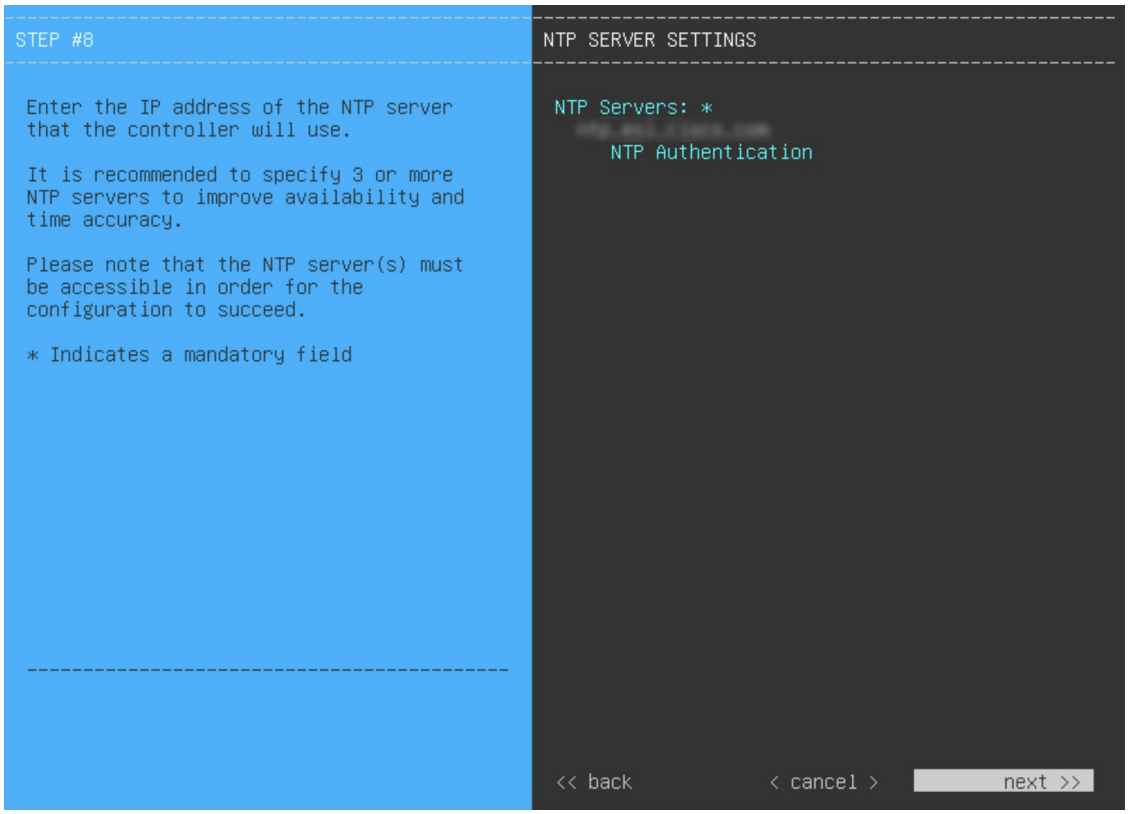
After you provide the necessary information, correct any validation errors to proceed (if necessary).



l) Enter the configuration values for the settings provided in the wizard's **NTP SERVER SETTINGS** page (as described in the following table), then click **next>>**.

NTP Servers field	Enter one or more NTP server addresses or hostnames, separated by spaces. At least one NTP address or hostname is required. For a production deployment, we recommend that you configure a minimum of three NTP servers.
NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center on ESXi, check this check box and then enter the following information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file. **Note** Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

After you provide the necessary information, correct any validation errors to proceed (if necessary).



A final message appears, stating that the wizard is ready to apply the configuration.

m) To apply the settings you've entered to the virtual appliance, click **proceed**>>.

After the configuration process completes, the virtual appliance powers on again and displays a **CONFIGURATION SUCCEEDED!** message. Then, it displays the Maglev login page.

Note It can take from 15-30 minutes for services to be stabilized so that you can login to the Catalyst Center UI.

Step 4 Complete the Quick Start Workflow, on page 106.

Configure a Virtual Appliance Using the Maglev Configuration Wizard: Advanced Mode for IPv4 Deployments

If you want to configure a virtual appliance using the Maglev Configuration wizard and need to specify settings that are different from the preset appliance settings, complete the following procedure.

Before you begin

Gather the following information for the virtual appliance before you start this procedure:

- Static IP address
- Subnet mask
- Default gateway

- DNS address
- NTP server details
- Proxy server details

Important If you plan to configure the appliance's Management interface, also Configure an Additional Network Adapter for this interface to reside on before you start this wizard.

Procedure

Step 1 After deployment completes, power on the newly-created virtual machine:

a) In the vSphere Client, right-click the virtual machine.

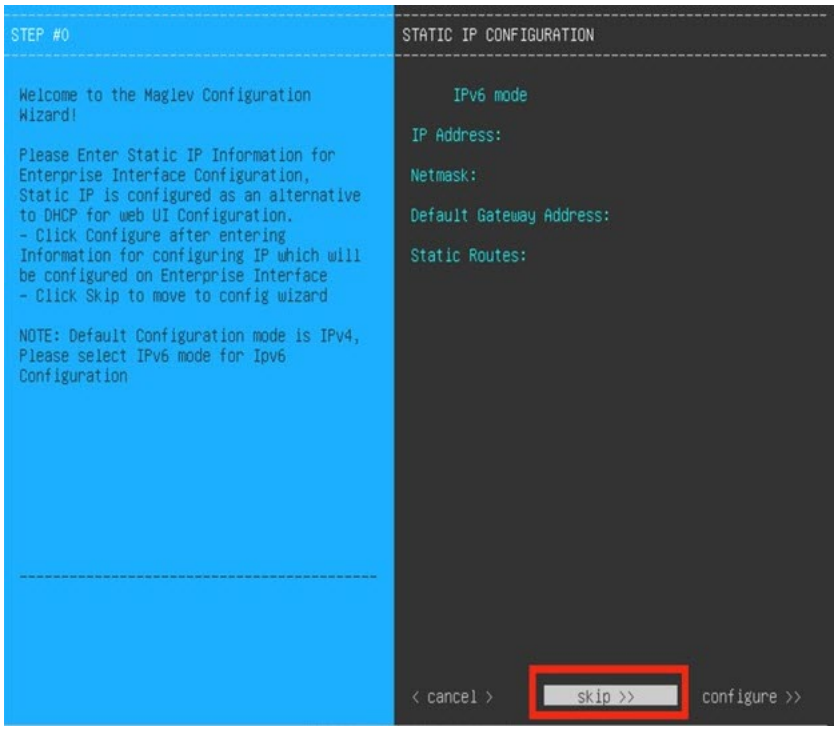
b) Choose **Power** > **Power On**.

Step 2 Launch either the remote console or web console by clicking the appropriate link.

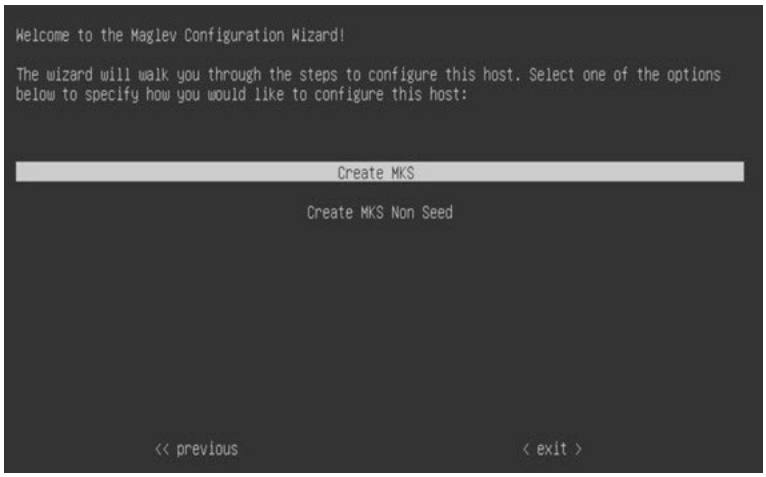
Step 3 Configure the virtual machine by completing the Maglev Configuration Wizard:

a) You don't need to enter any settings in the wizard's **STATIC IP CONFIGURATION** page, so click **skip>>**.

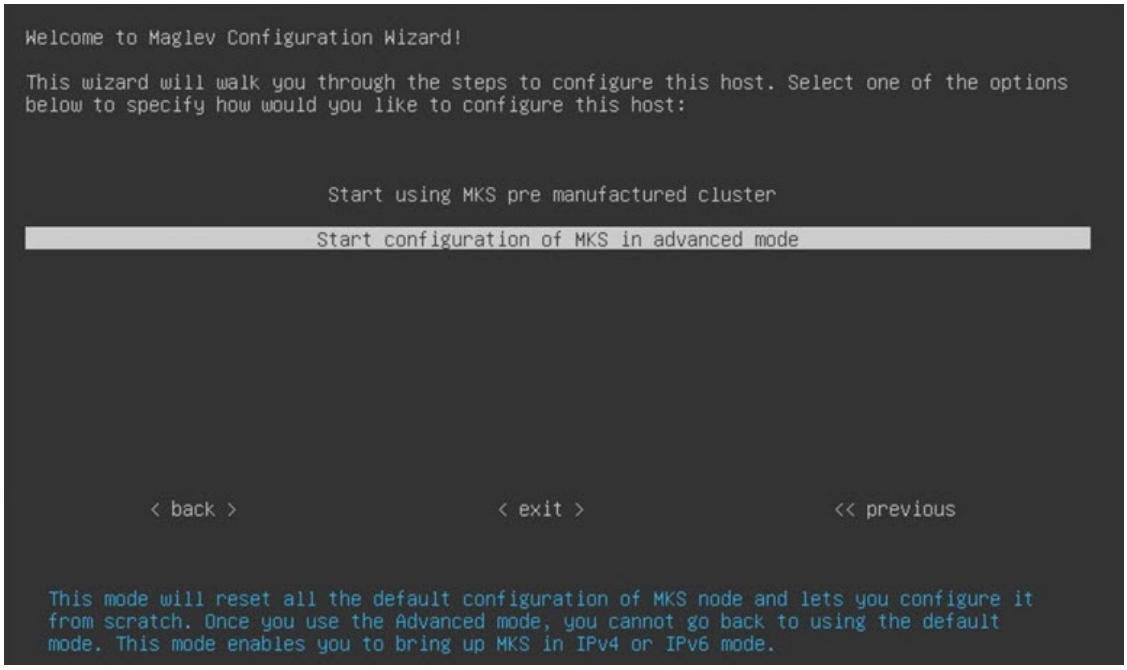
Static IP configuration is needed only when configuring a virtual appliance using a browser-based WEB UI mode of installation.



b) Click **Create MKS**.

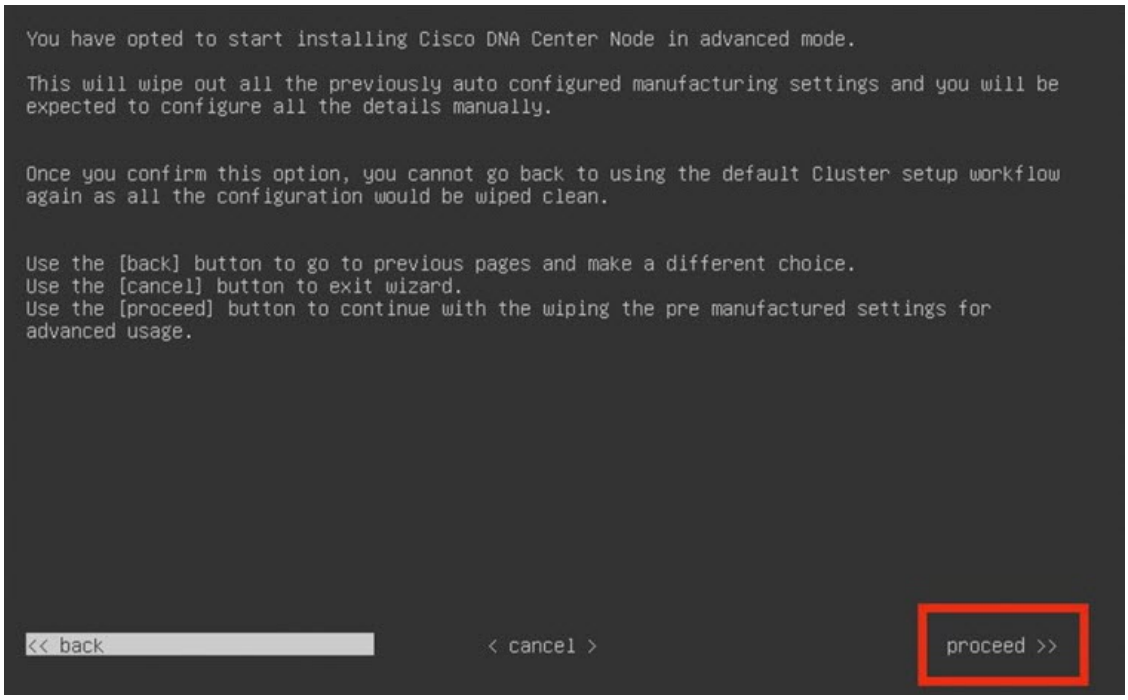


c) Click the **Start configuration of MKS in advanced mode** option.



The next wizard page opens, indicating that all preconfigured appliance settings (except for the container and cluster subnets) will be erased. You'll need to enter values for these settings.

This page also indicates that if you choose this option, you won't be able to go back and use the default appliance setup workflow instead. Keep this in mind before you complete the next step.

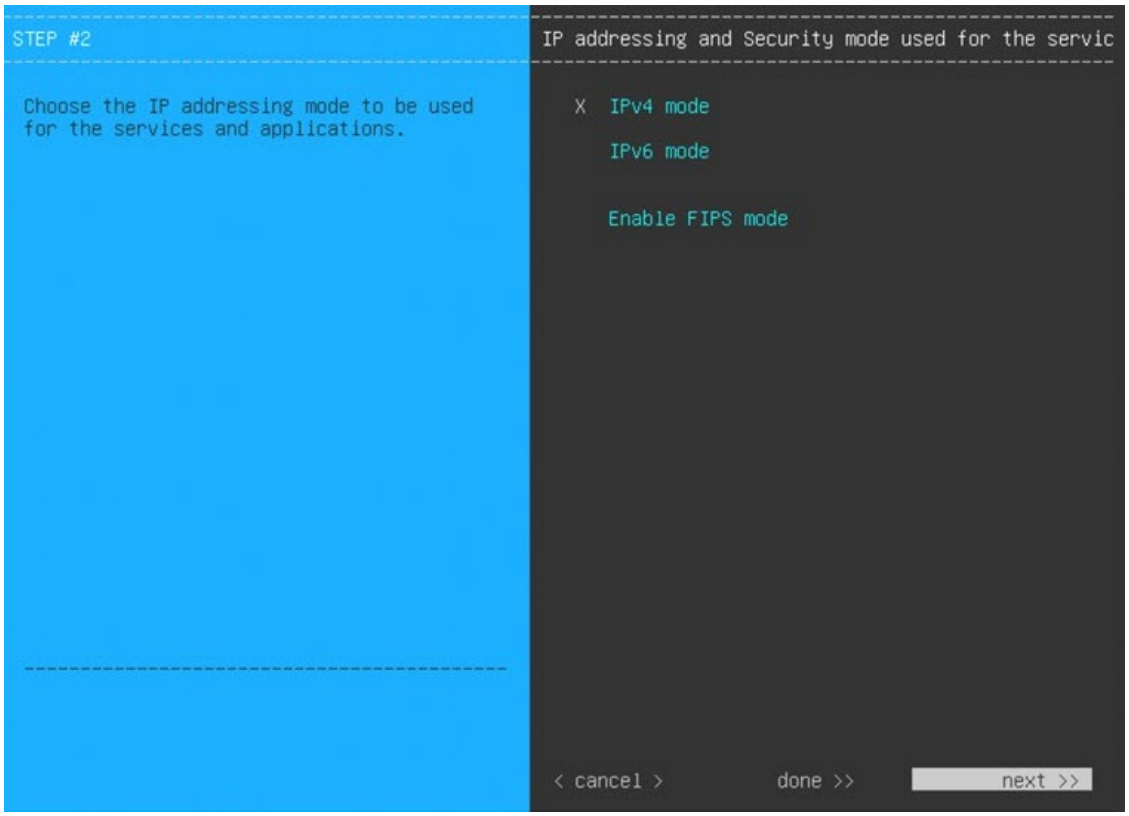


d) Click **proceed**>>.

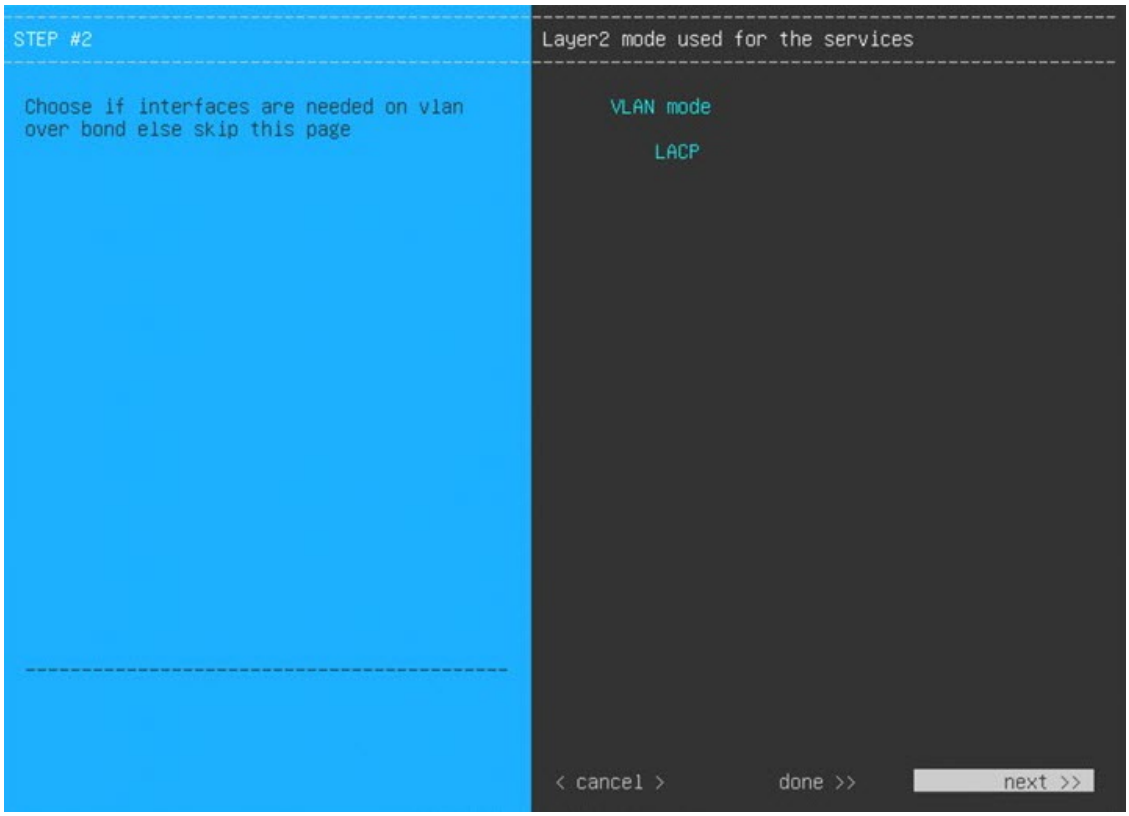
After all of the preconfigured appliance settings have been erased, the next wizard page opens.

e) Do one or more of the following, then click **next**>>:

- Choose IPv4 addressing.
-
- If you want to enable FIPS mode, click its corresponding option. For more information regarding FIPS mode, see the "FIPS Mode Support" topic in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.



f) You don't need to enter any settings in the **Layer2 mode used for the services** wizard page, so click **next>>**.

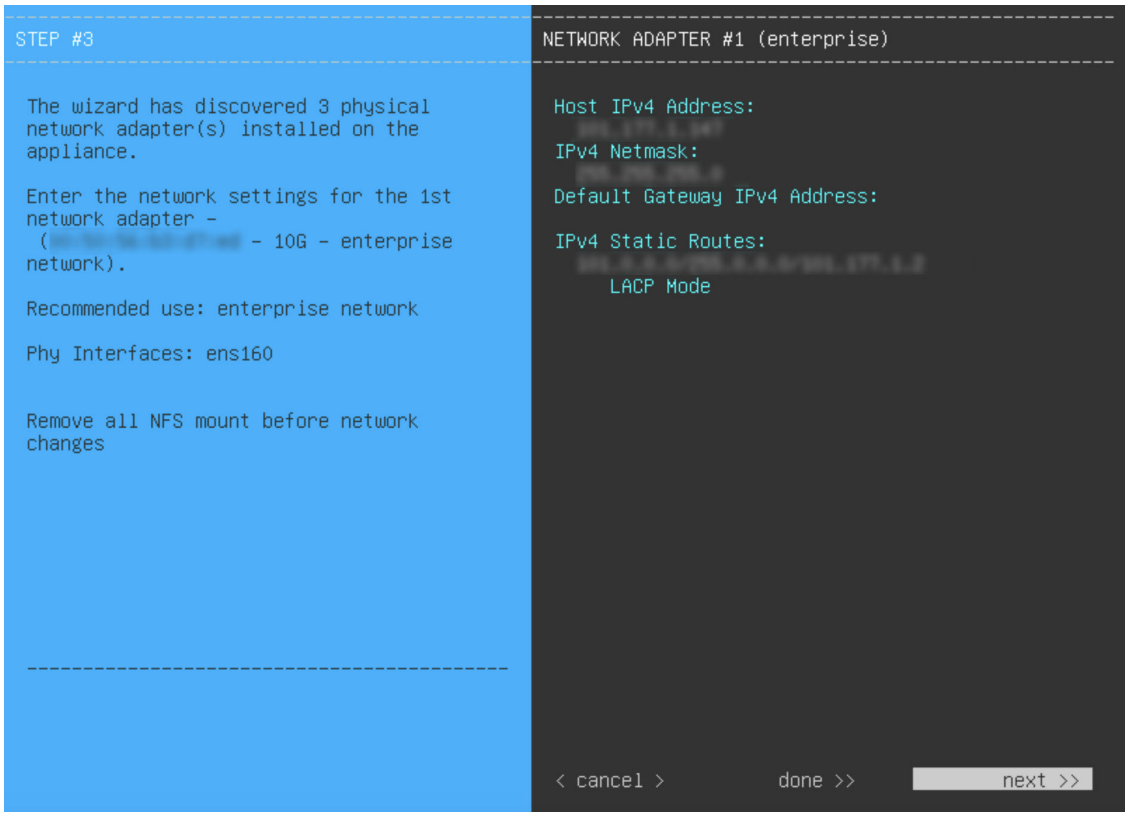


g) Enter the configuration values for **NETWORK ADAPTER #1**, as shown in the following table, then click **next>>**.

Catalyst Center on ESXi uses this interface to link the virtual appliance with your network.

Host IPv4 Address field	Enter the IP address for the Enterprise interface. This is required.
IPv4 Netmask field	Enter the netmask for the interface's IP address. This is required.
Default Gateway IPv4 Address field	Enter a default gateway IP address to use for the interface. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Management interface only.
Cluster Link field	Leave this field blank. It is required on the Intracluster interface only.
LACP Mode field	Leave this field blank, as it's not applicable to virtual appliances.

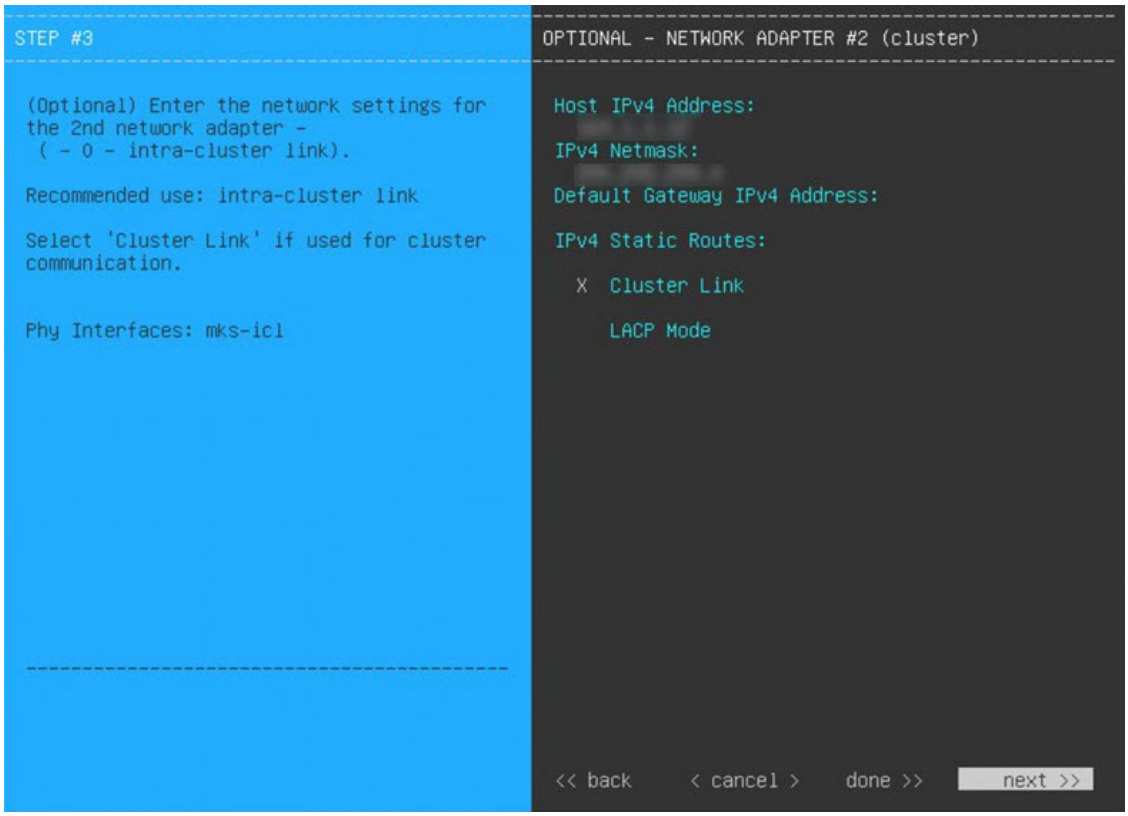
The wizard validates the values you entered and issues an error message if any are incorrect. If you receive an error message, check that the value you entered is correct, then reenter it. If necessary, click **<<back** to reenter it.



h) Enter the configuration values for **NETWORK ADAPTER #2**, as shown in the following table, then click **next>>**.

Host IPv4 Address field	Enter the IP address for the Intracluster interface. This is required. Note that you cannot change the address of the Intracluster interface later.
IPv4 Netmask field	Enter the netmask for the interface's IP address. This is required.
Default Gateway IPv4 Address field	Leave this field blank.
IPv4 Static Routes field	Leave this field blank.
Cluster Link field	Check the check box to set this interface as the link to a Catalyst Center on ESXi cluster. This is required on the Intracluster interface only.
LACP Mode field	Leave this field blank, as it's not applicable to virtual appliances.

Correct validation errors, if any, to proceed. The wizard validates and applies your network adapter configurations.



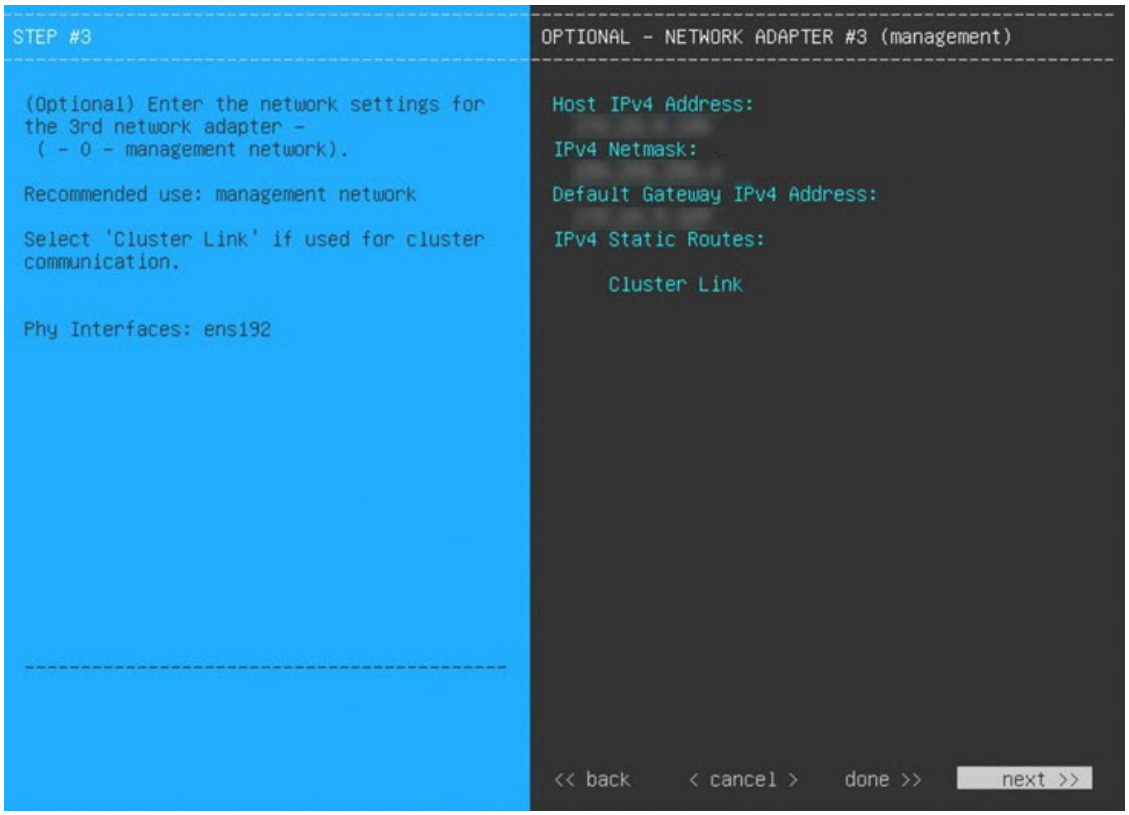
i) Enter the configuration values for **NETWORK ADAPTER #3**, as shown in the following table, then click **next>>**.

This interface allows you to access the Catalyst Center on ESXi GUI from the virtual appliance.

Note You will see this wizard page only if you have already Configure an Additional Network Adapter for the Management interface.

Host IPv4 Address field	Enter the IP address for the Management interface. This is required only if you are using this interface to access the Catalyst Center on ESXi GUI from your management network; otherwise, you can leave it blank.
IPv4 Netmask field	Enter the netmask for the interface's IP address. This is required.
Default Gateway IPv4 Address field	Enter a default gateway IP address to use for the interface. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*.
Cluster Link field	Leave this field blank. It is required on the Intracluster interface only.

Correct validation errors, if any, to proceed. The wizard validates and applies your network adapter configurations.

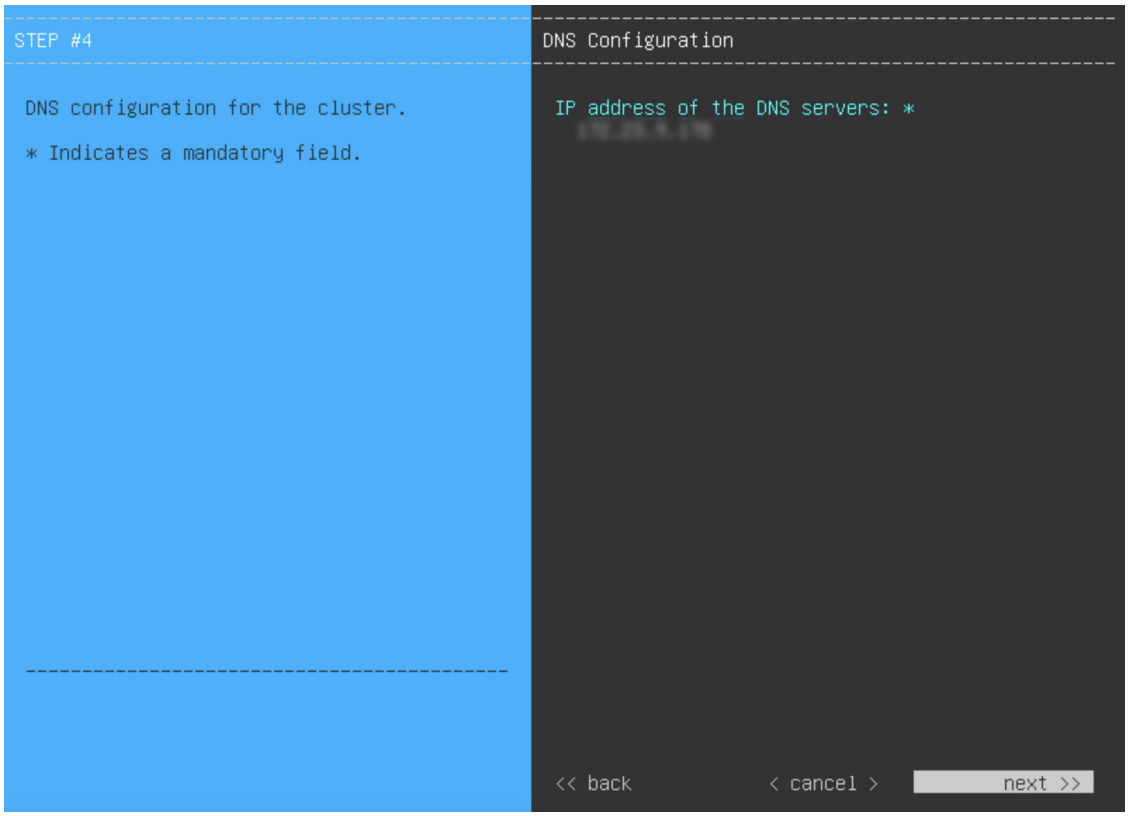


j) In the **DNS Configuration** page, enter the IP address of the preferred DNS server and then click **next>>**. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.

Important

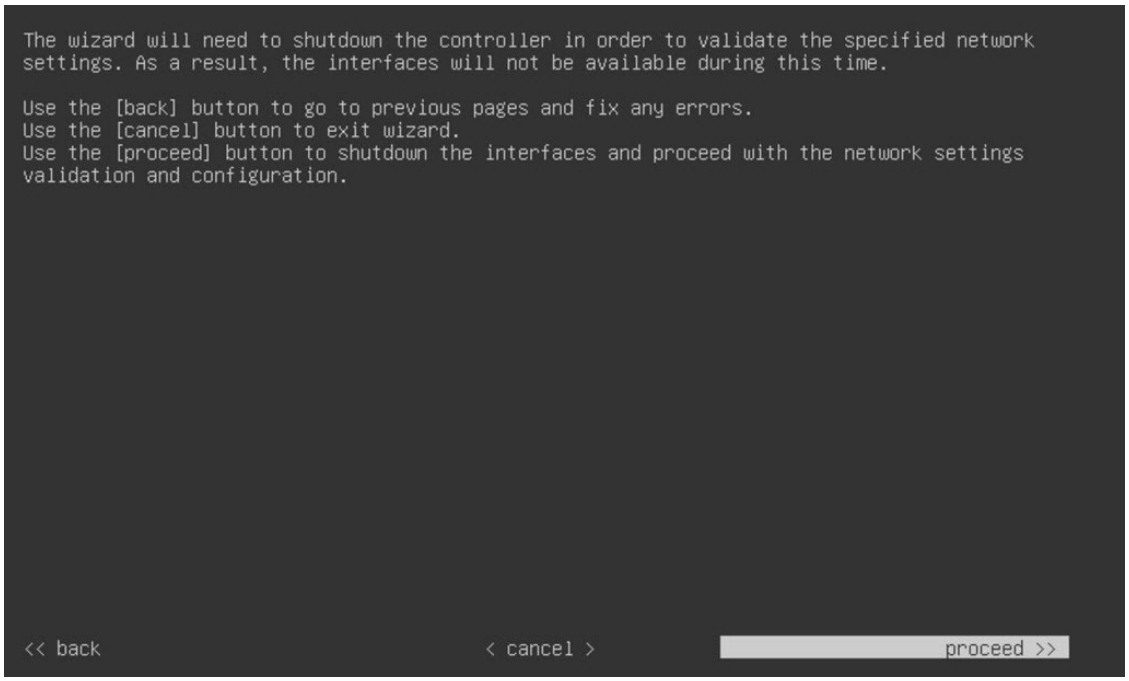
- For NTP, ensure port 123 (UDP) is open between Catalyst Center on ESXi and your NTP server.
- Configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for a virtual appliance.

The wizard updates, indicating that it needs to shut down the controller in order to validate the settings you've entered so far.

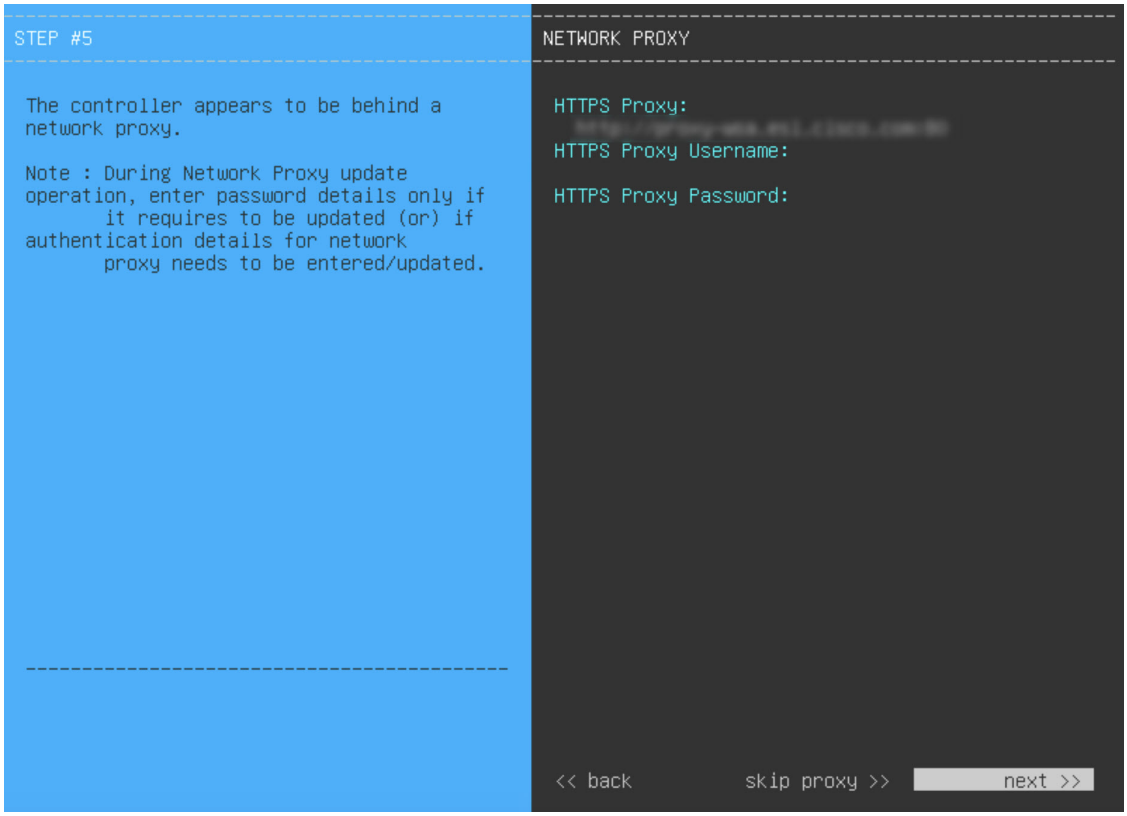


k) Do one of the following:

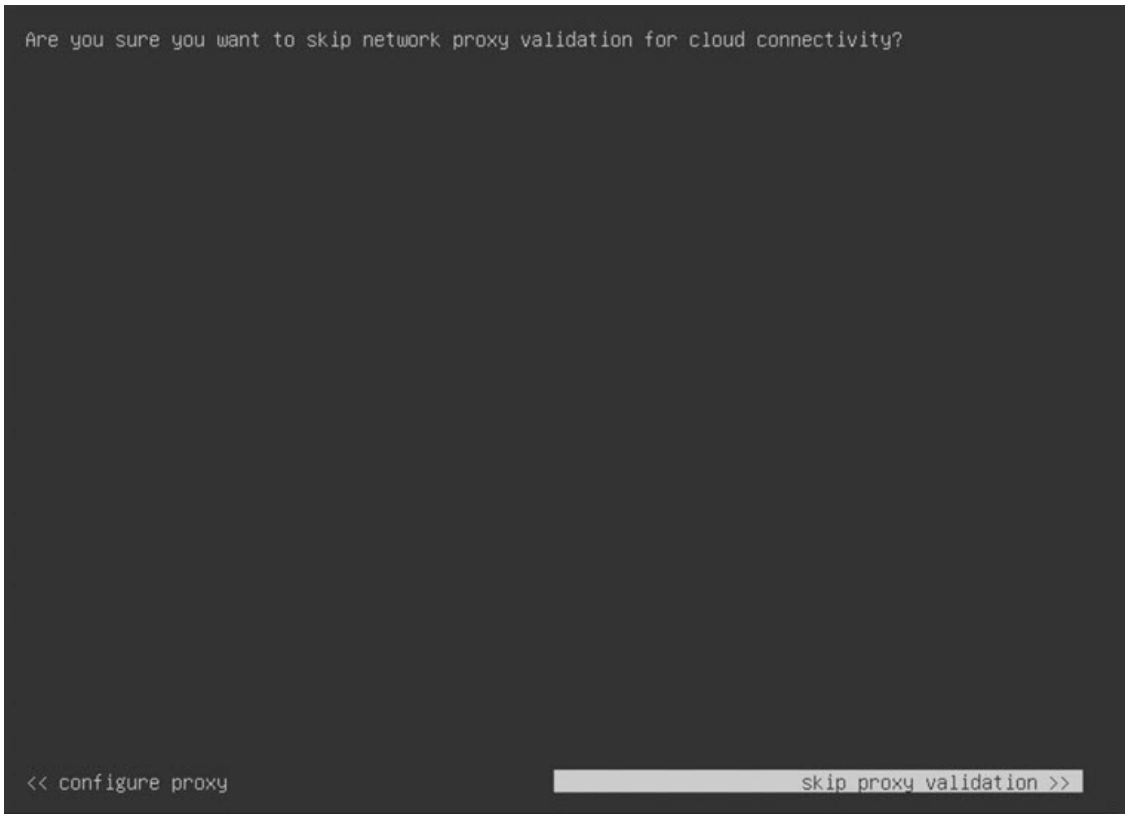
- If you need to change any settings, click **<<back** as needed, make the necessary changes, and then return to this wizard page.
- If you're happy with the settings you've entered, click **proceed**>>.



l) After validation successfully completes, the **NETWORK PROXY** wizard page opens. Click **skip proxy>>** to proceed.



m) Confirm that you want to skip network proxy configuration by clicking **skip proxy validation>>**.

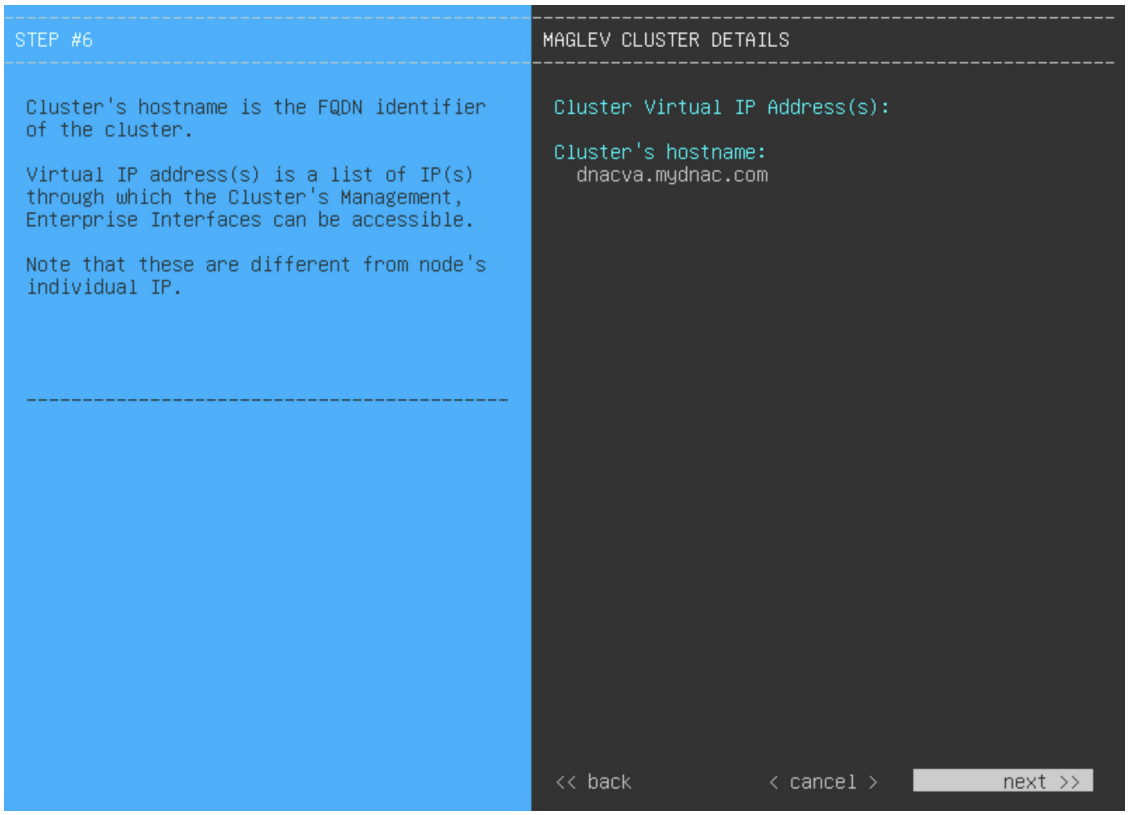


n) Next, you are prompted to enter the virtual appliance's virtual IP addresses in the **MAGLEV CLUSTER DETAILS** wizard page. Since clusters are not supported by Catalyst Center on ESXi, you can leave the **Cluster Virtual IP Address(s)** field on this page blank.

You can also specify the fully qualified domain name (FQDN) for your virtual appliance. Catalyst Center on ESXi uses this domain name to do the following:

- It uses this hostname to access your virtual appliance’s web interface and the Representational State Transfer (REST) APIs used by devices in the enterprise network that Catalyst Center on ESXi manages.
- In the Subject Alternative Name (SAN) field of Catalyst Center on ESXi certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.

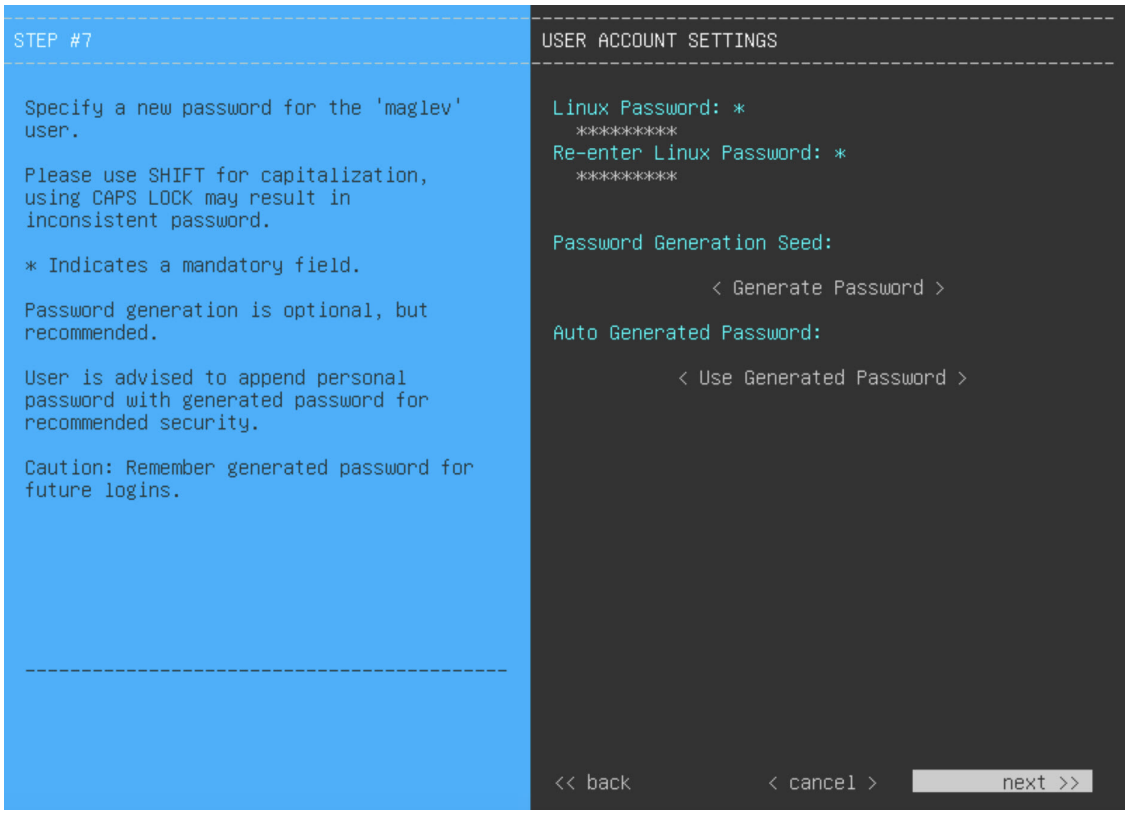
After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.



o) Enter the configuration values for the settings provided in the wizard's **USER ACCOUNT SETTINGS** page (as described in the following table), then click **next>>**.

Linux Password field	Enter and confirm the password for the `maglev` user.
Re-enter Linux Password field	Confirm the Linux password by entering it a second time.
Password Generation Seed field	If you do not want to create the Linux password yourself, enter a seed phrase in this field and then press <**Generate Password**> to generate the password.
Auto Generated Password field	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto-generated password. Press <**Use Generated Password**> to save the password.

After you provide the necessary information, correct any validation errors to proceed (if necessary).

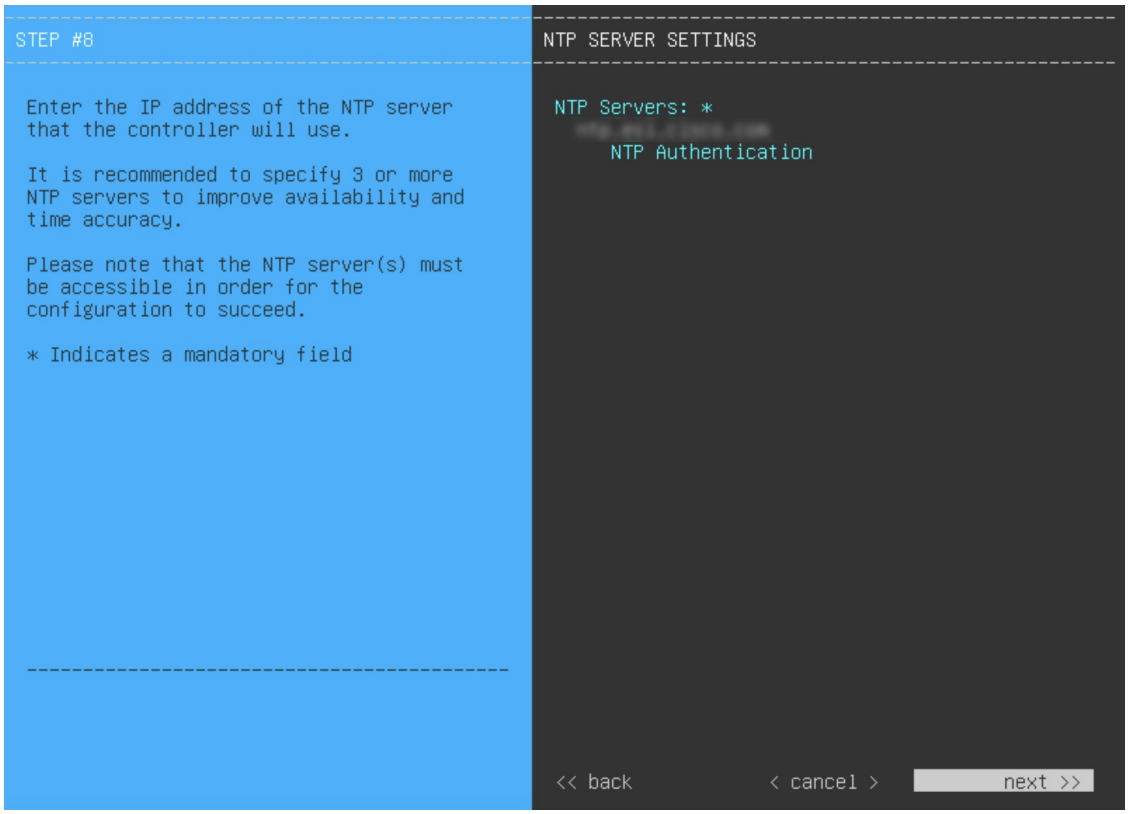


p) Enter the configuration values for the settings provided in the wizard's **NTP SERVER SETTINGS** page (as described in the following table), then click **next>>**.

NTP Servers field	Enter one or more NTP server addresses or hostnames, separated by spaces. At least one NTP address or hostname is required. For a production deployment, we recommend that you configure a minimum of three NTP servers.
NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center on ESXi, check this check box and then enter the following information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file. **Note** Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

After you provide the necessary information, correct any validation errors to proceed (if necessary).

A final message appears, stating that the wizard is ready to apply the configuration.

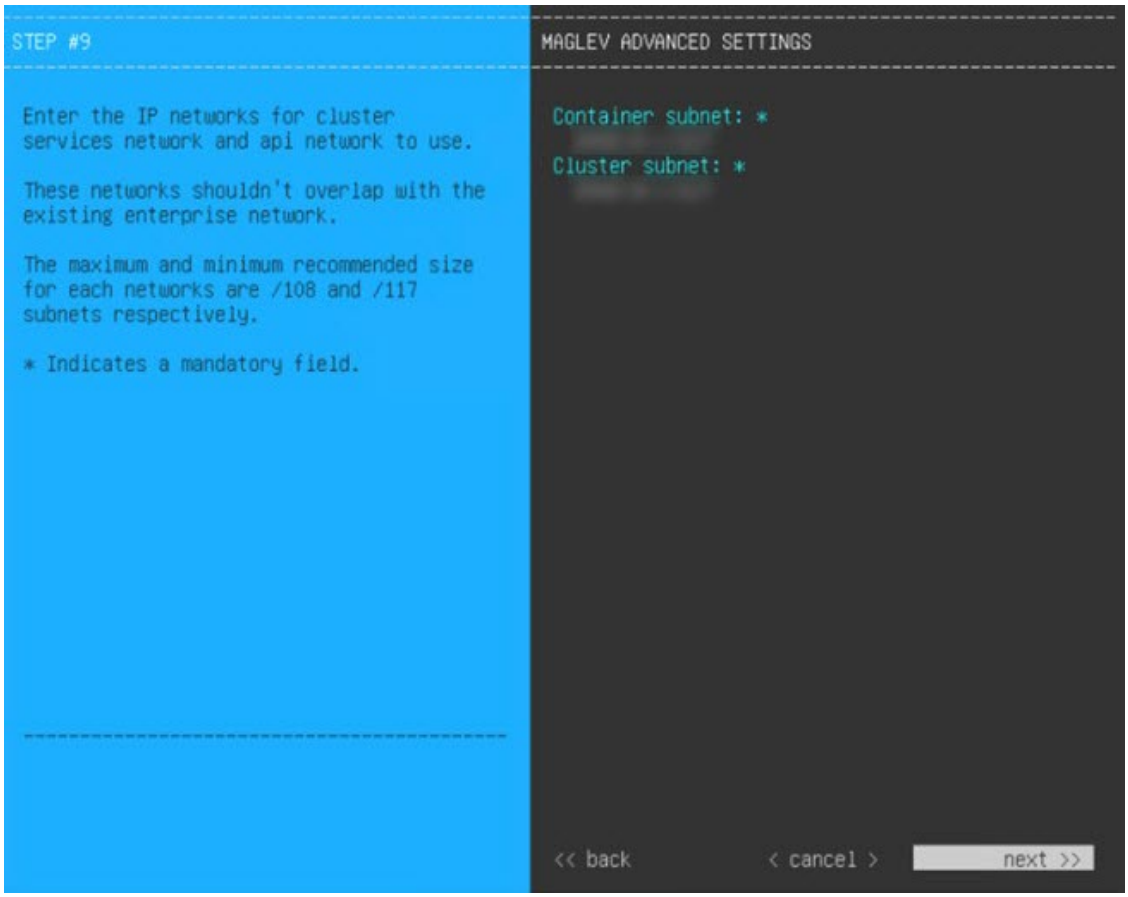


q) Enter the configuration values for the settings provided in the wizard's **MAGLEV ADVANCED SETTINGS** page, (as described in the following table), then click **next>>**.

Container Subnet field	A dedicated, non-routed IP subnet that Catalyst Center on ESXi uses to manage internal services. By default, this is already set to **169.254.32.0/20**, and we recommend that you use this subnet. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Catalyst Center on ESXi internal network or an external network. For more information, see the Container Subnet description in the *Catalyst Center Second-Generation Appliance Installation Guide's* "Required IP Addresses and Subnets" topic.
Cluster Subnet field	A dedicated, non-routed IP subnet that Catalyst Center on ESXi uses to manage internal cluster services. By default, this is already set to **169.254.48.0/20**, and we recommend that you use this subnet. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Catalyst Center on ESXi internal network or an external network. For more information, see the Cluster Subnet description in the *Catalyst Center Second-Generation Appliance Installation Guide's* "Required IP Addresses and Subnets" topic.

After you provide the necessary information, correct any validation errors to proceed (if necessary).

A final message appears, stating that the wizard is ready to apply the configuration.



r) To apply the settings you've entered to the virtual appliance, click **proceed>>**.

After the configuration process completes, the virtual appliance powers on again and displays a **CONFIGURATION SUCCEEDED!** message.

It takes around 180 to 210 minutes for the virtual machine to become operational. The actual time will depend on things like available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.

```
The wizard is now ready to apply the configuration on the controller.

Use the [back] button below to verify/modify controller settings.
Use the [cancel] button to discard your changes and exit the wizard.
Use the [proceed] button to save your changes and proceed with applying them on the
controller.

<< back                                  < cancel >                    proceed >>

WARNING - Existing disk partition(s) detected. Maglev might have been previously
installed. Proceeding would overwrite any existing Maglev installation(s).
```

```
Welcome to the Maglev Appliance (tty1)

Hint: Num Lock on

maglev-master-[redacted] login:
```

Step 4 Complete the Quick Start Workflow, on page 106.

Configure a Virtual Appliance Using the Maglev Configuration Wizard: Advanced Mode for IPv6 Deployments

Gather the following information for the virtual appliance before you start this procedure:

- Static IP address
- Subnet mask
- Default gateway
- DNS address
- NTP server details
- Proxy server details

Important If you plan to configure the appliance's Management interface, also Configure an Additional Network Adapter for this interface to reside on before you start this wizard.

If you want to configure a virtual appliance using the Maglev Configuration wizard and need to specify settings that are different from the preset appliance settings, complete the following procedure.

Procedure

Step 1 After deployment completes, power on the newly-created virtual machine:

a) In the vSphere Client, right-click the virtual machine.

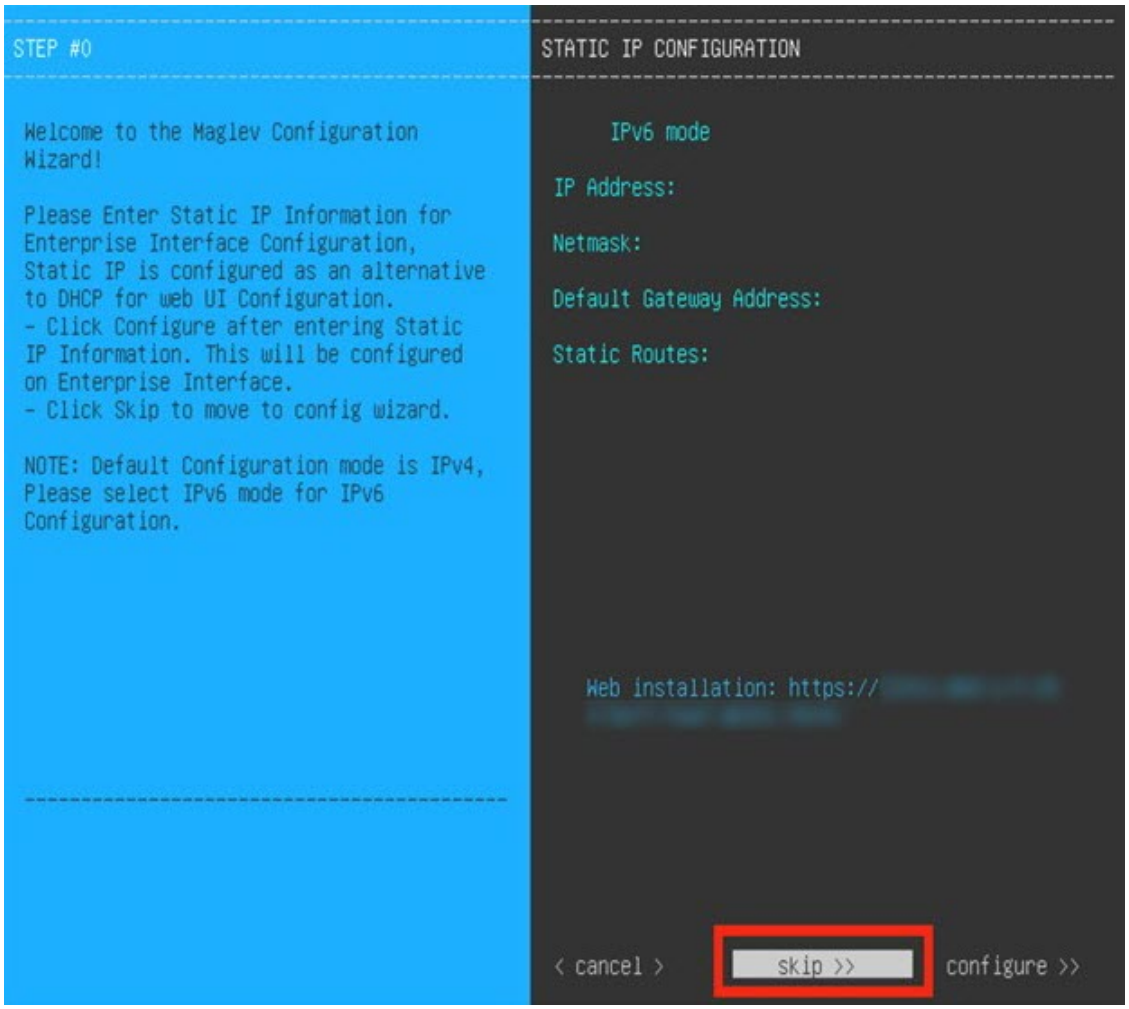
b) Choose **Power** > **Power On**.

Step 2 Launch either the remote console or web console by clicking the appropriate link.

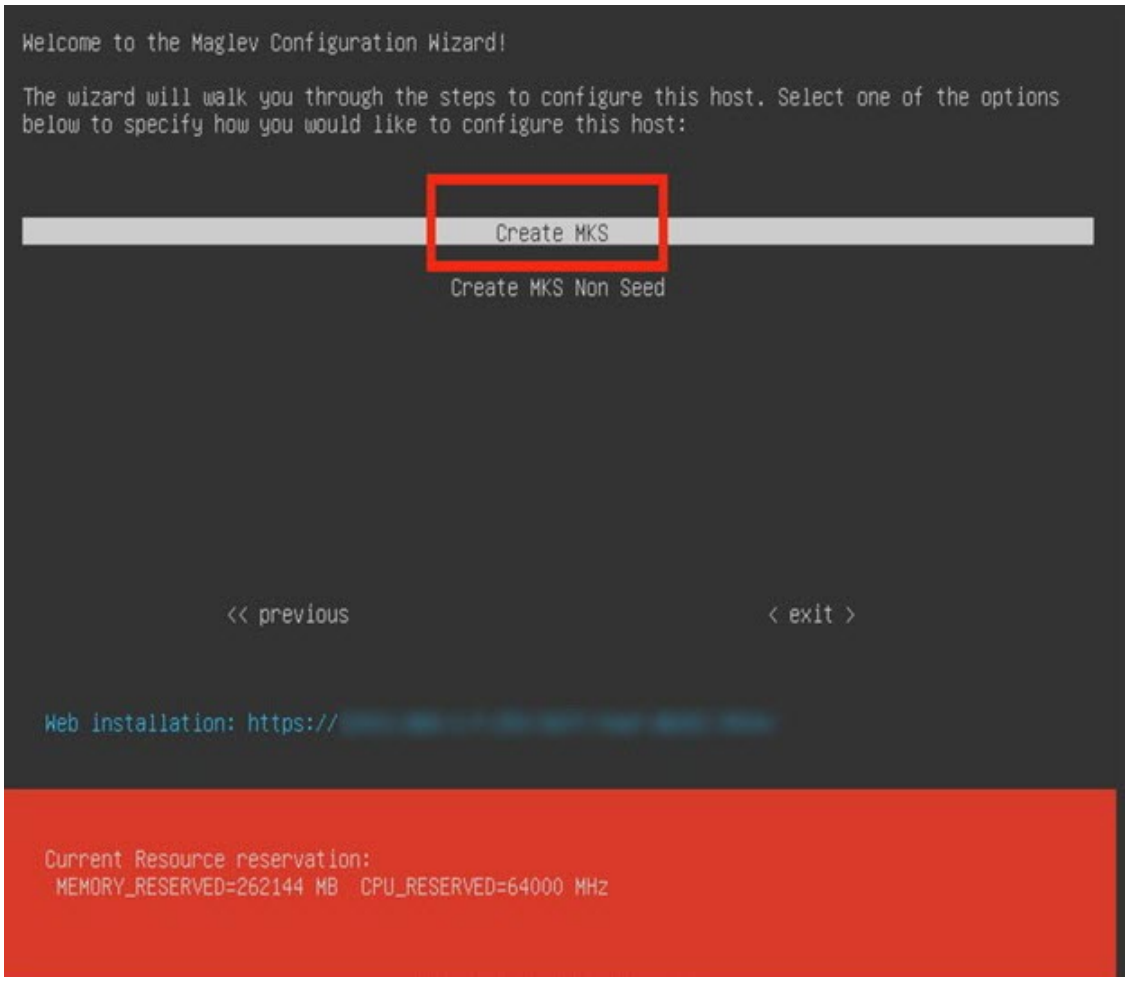
Step 3 Configure the virtual machine by completing the Maglev Configuration Wizard:

a) You don't need to enter any settings in the wizard's **STATIC IP CONFIGURATION** page, so click **skip>>**.

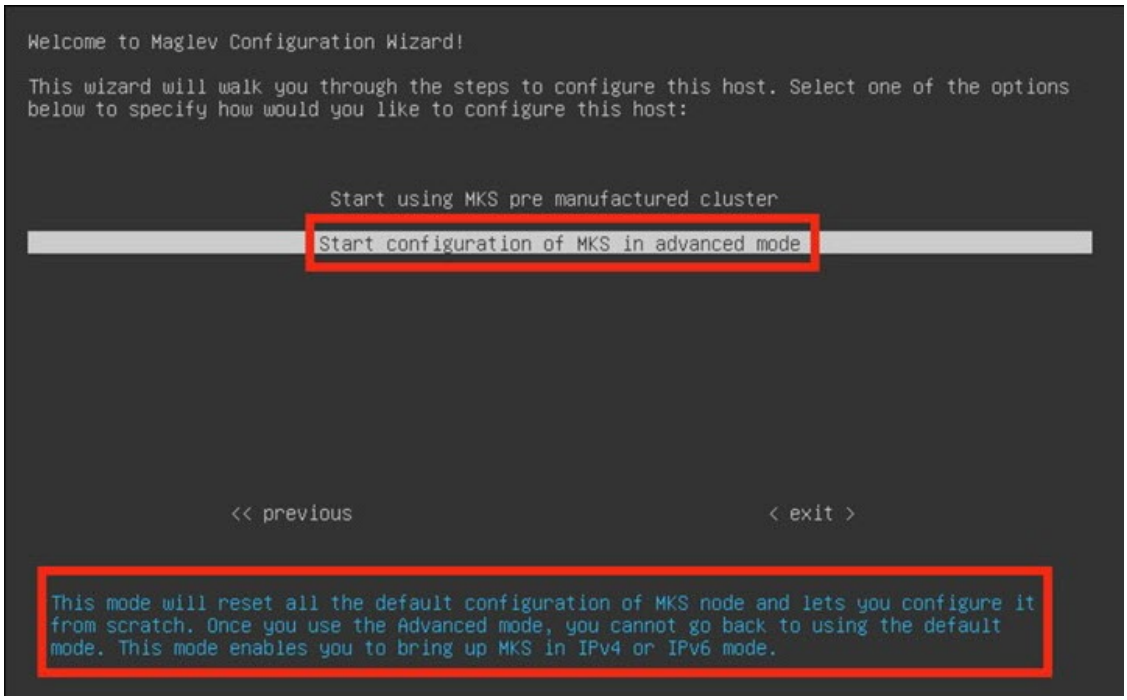
Static IP configuration is needed only when configuring a virtual appliance using a browser-based WEB UI mode of installatoin.



b) Click **Create MKS**.



c) Click the **Start configuration of MKS in advanced mode** option.

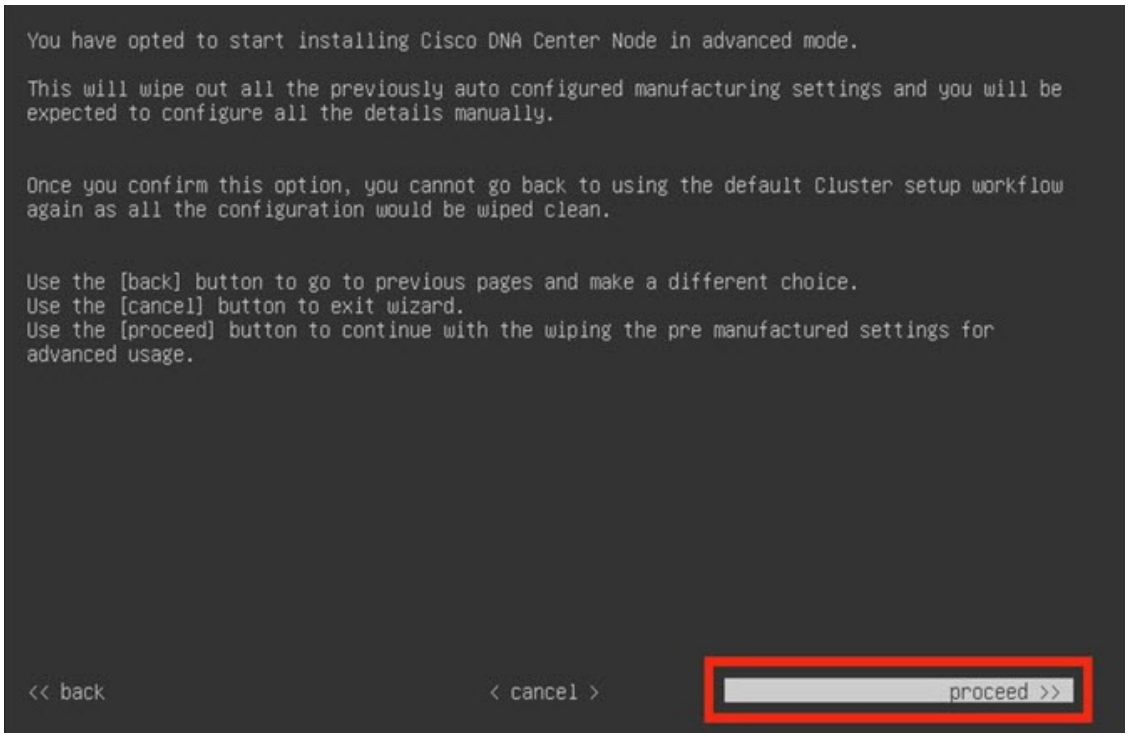


The next wizard page opens, indicating that all preconfigured appliance settings (except for the container and cluster subnets) will be erased. You'll need to enter values for these settings.

This page also indicates that if you choose this option, you won't be able to go back and use the default appliance setup workflow instead. Keep this in mind before you complete the next step.

d) Click **proceed**>>.

After all of the preconfigured appliance settings have been erased, the next wizard page opens.



e) Deselect IPv4 mode and select IPv6 mode to configure IPv6 parameters.

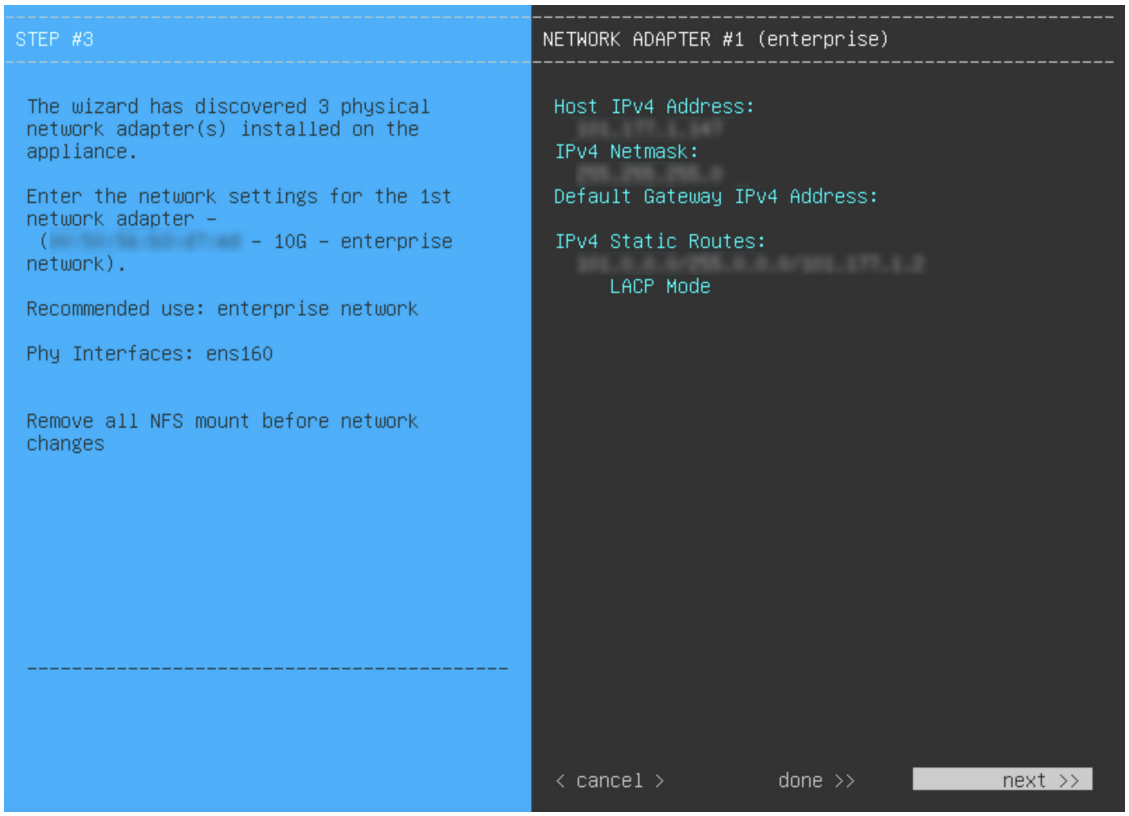
f) You don't need to enter any settings in the **Layer2 mode used for the services** wizard page, so click **next>>**.

g) Enter the configuration values for **NETWORK ADAPTER #1**, as shown in the following table, then click **next>>**.

Catalyst Center on ESXi uses this interface to link the virtual appliance with your network.

Host IPv6 Address field	Enter the IPv6 address for the Enterprise interface. This is required.
IPv6 Prefix Length field	Enter the prefix length (in bits) for the interface's IPv6 address.
Default Gateway IPv4/IPv6 Address field	Enter a default gateway IPv6 address to use for the interface. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Catalyst Center on ESXi Management interface only.
Cluster Link field	Leave this field blank. It is required on the Intracluster interface only.
LACP Mode field	Leave this field blank, as it's not applicable to virtual appliances.

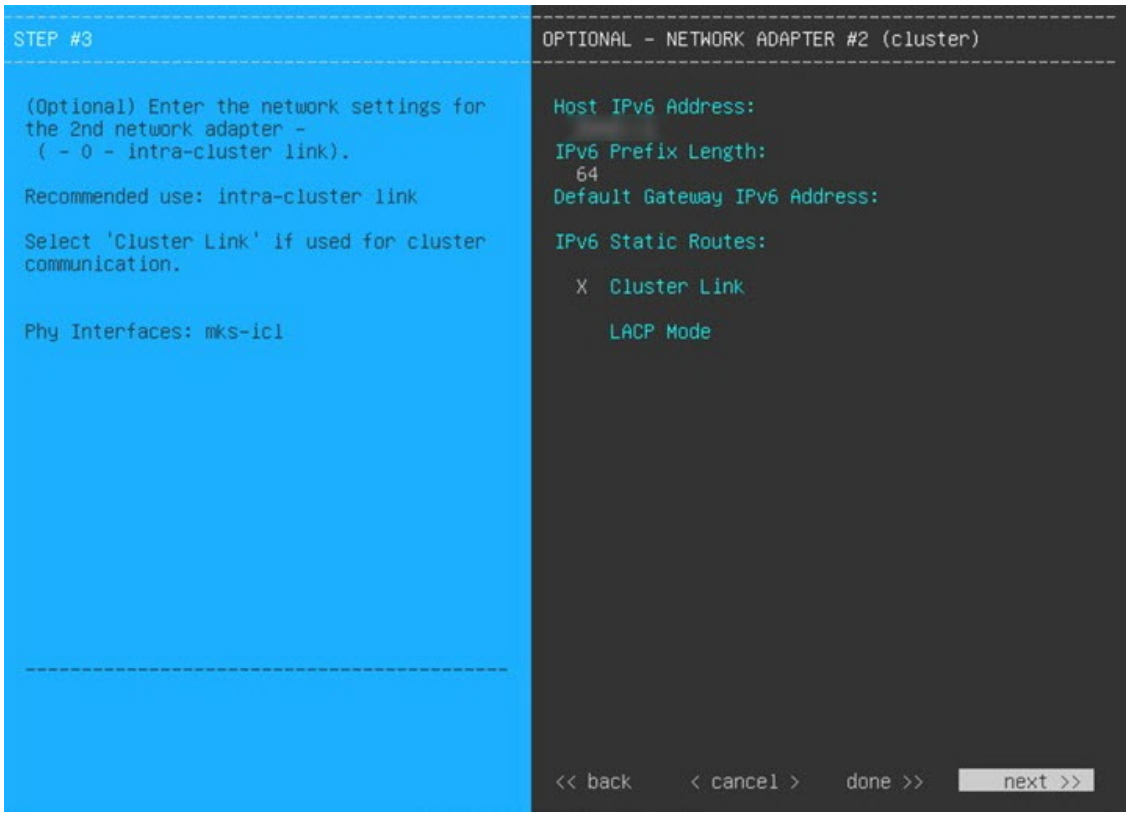
The wizard validates the values you entered and issues an error message if any are incorrect. If you receive an error message, check that the value you entered is correct, then reenter it. If necessary, click **<<back** to reenter it.



h) Enter the configuration values for **NETWORK ADAPTER #2**, as shown in the following table, then click **next>>**.

Host IPv6 Address field	Enter the IP address for the Intracluster interface. This is required. Note that you cannot change the address of the Intracluster interface later.
IPv6 Prefix Length field	Enter the prefix length for the interface's IPv6 address. This is required.
Default Gateway IPv6 Address field	Leave this field blank.
IPv6 Static Routes field	Leave this field blank.
Cluster Link field	Check the check box to set this interface as the link to a Catalyst Center on ESXi cluster. This is required on the Intracluster interface only.
LACP Mode field	Leave this field blank, as it's not applicable to virtual appliances.

Correct validation errors, if any, to proceed. The wizard validates and applies your network adapter configurations.



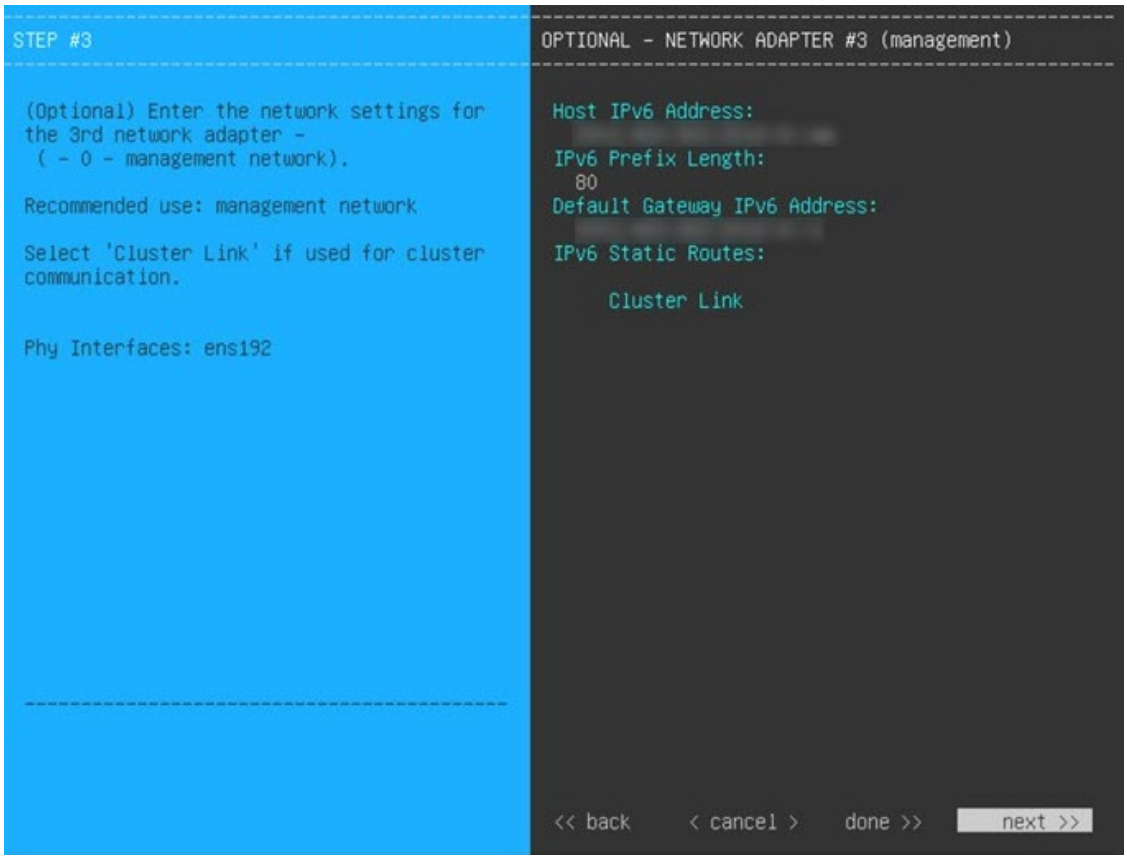
i) Enter the configuration values for **NETWORK ADAPTER #3**, as shown in the following table, then click **next>>**.

This interface allows you to access the Catalyst Center on ESXi GUI from the virtual appliance.

Note You will see this wizard page only if you have already Configure an Additional Network Adapter for the Management interface.

Host IPv6 Address field	Enter the IPv6 address for the Management interface. This is required only if you are using this interface to access the Catalyst Center on ESXi GUI from your management network; otherwise, you can leave it blank.
IPv6 Prefix Length field	Enter the prefix length for the interface's IPv6 address. This is required.
Default Gateway IPv6 Address field	Enter a default gateway IP address to use for the interface. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*.
Cluster Link field	Leave this field blank. It is required on the Intracluster interface only.

Correct validation errors, if any, to proceed. The wizard validates and applies your network adapter configurations.

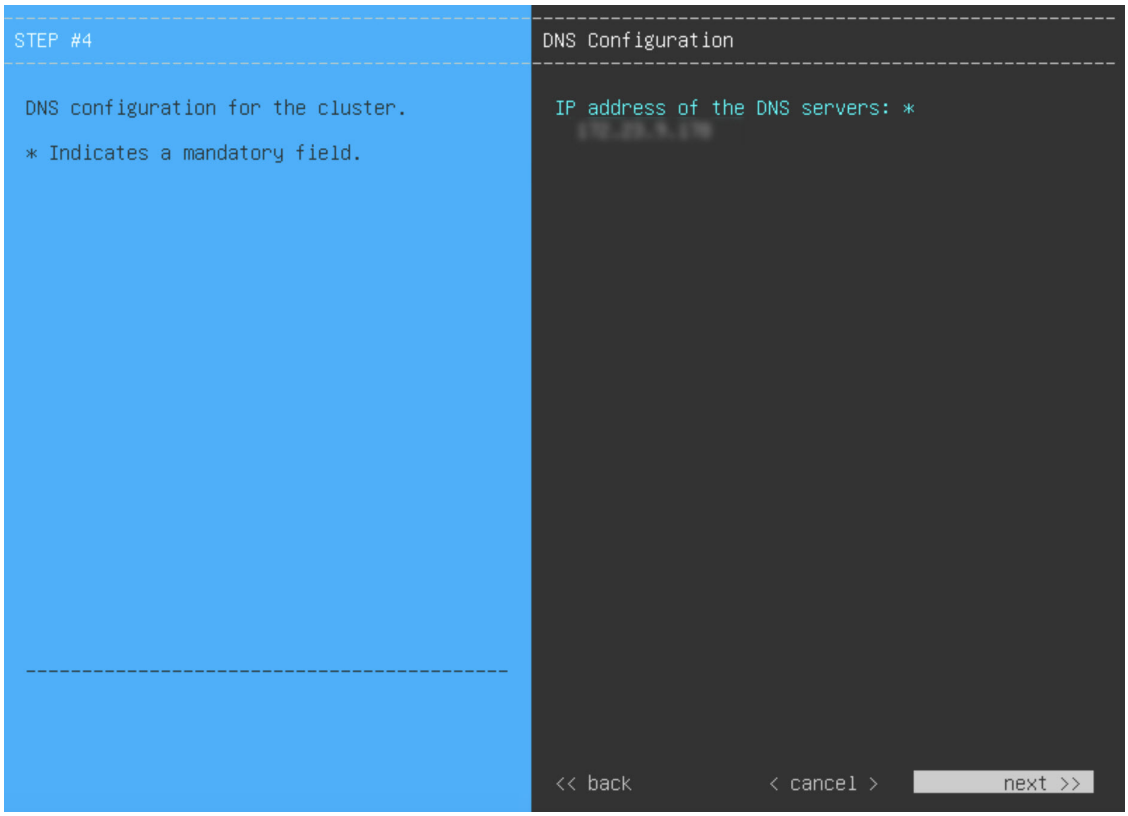


j) In the **DNS Configuration** page, enter the IPv6 address of the preferred DNS server and then click **next**>>. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.

Important

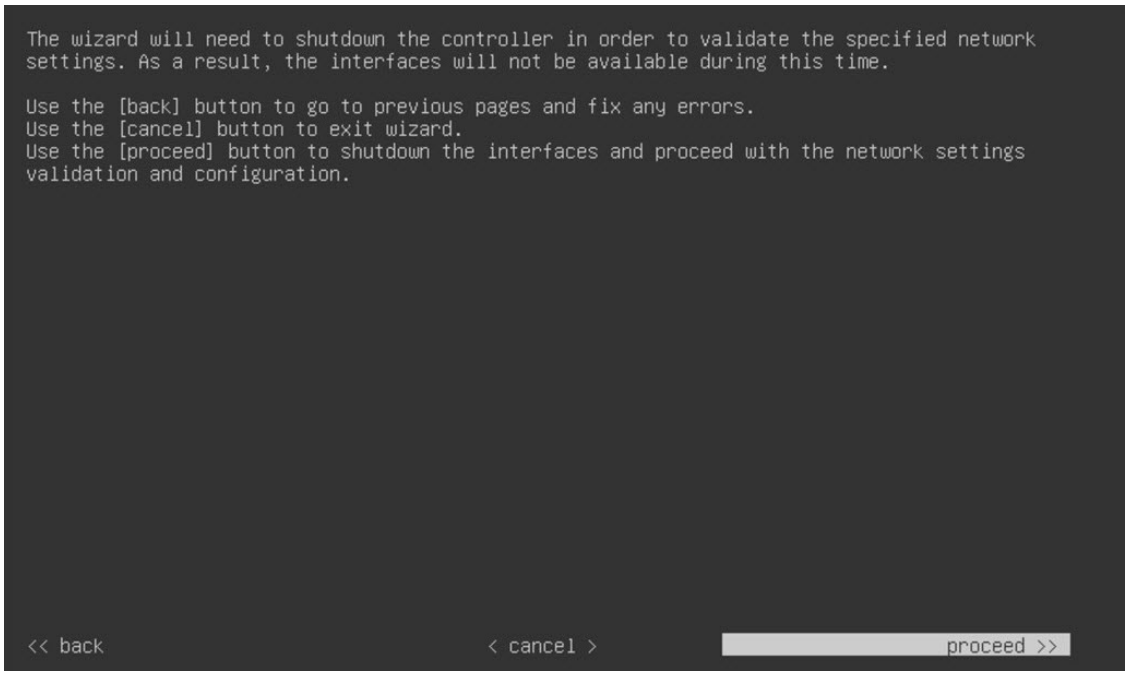
- For NTP, ensure port 123 (UDP) is open between Catalyst Center on ESXi and your NTP server.
- Configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for a virtual appliance.

The wizard updates, indicating that it needs to shut down the controller in order to validate the settings you've entered so far.



k) Do one of the following:

- If you need to change any settings, click **<<back** as needed, make the necessary changes, and then return to this wizard page.
- If you're happy with the settings you've entered, click **proceed**>>.

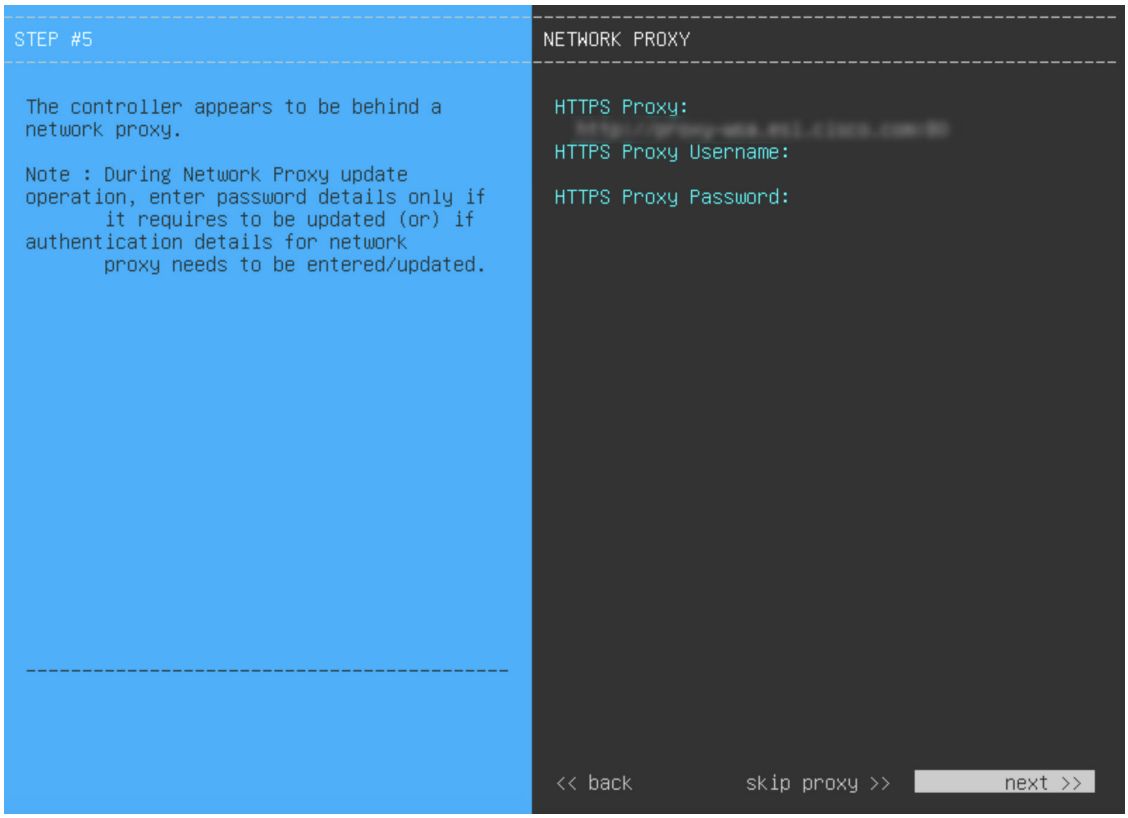


l) After validation successfully completes, do one of the following:

- If your network does *not* use a proxy server to access the internet, click **skip proxy**>> to proceed.
- If your network does use a proxy server, enter the configuration values in the **NETWORK PROXY** wizard page (as shown in the following table), then click **next**>>.

HTTPS Proxy field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** Connection from Catalyst Center on ESXi to the HTTPS proxy is supported only through HTTP in this release.
HTTPS Proxy Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
HTTPS Proxy Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

After you provide the necessary information, correct any validation errors to proceed (if necessary).

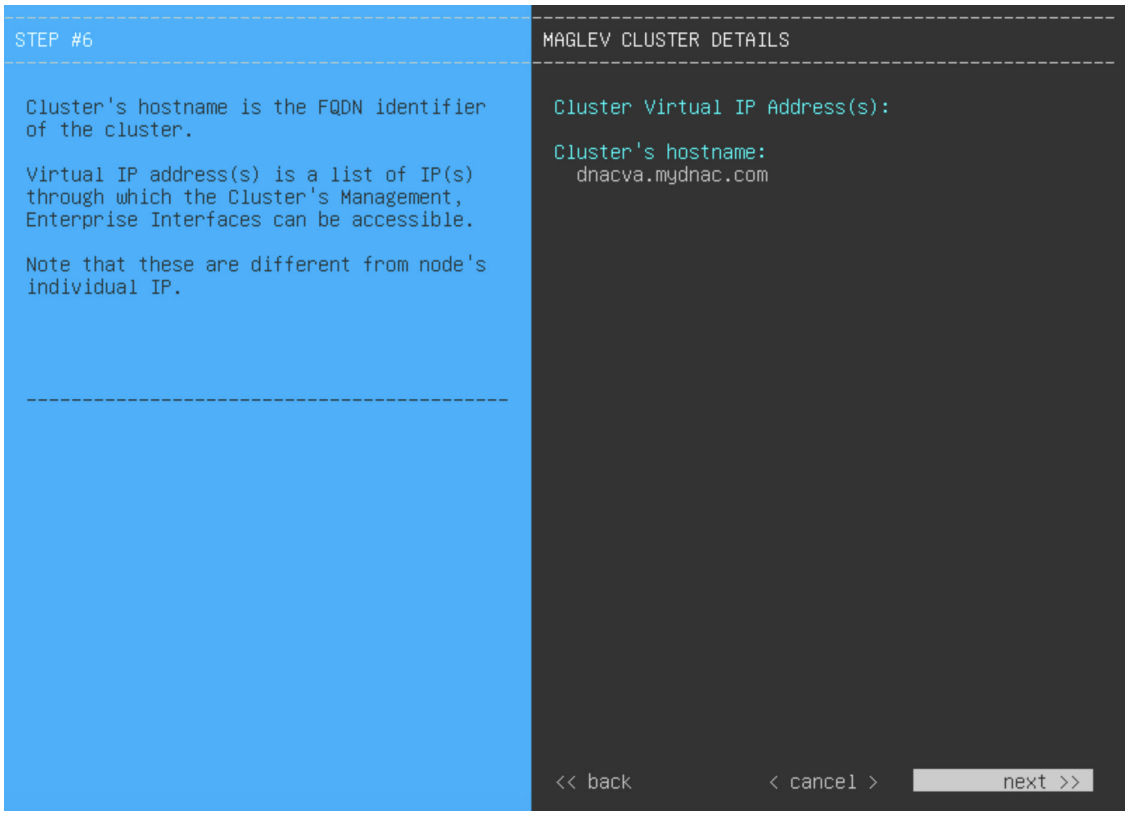


m) Next, you are prompted to enter the virtual appliance's virtual IP addresses in the **MAGLEV CLUSTER DETAILS** wizard page. Since clusters are not supported by Catalyst Center on ESXi, you can leave the **Cluster Virtual IP Address(s)** field on this page blank.

You can also specify the fully qualified domain name (FQDN) for your virtual appliance. Catalyst Center on ESXi uses this domain name to do the following:

- It uses this hostname to access your virtual appliance's web interface and the Representational State Transfer (REST) APIs used by devices in the enterprise network that Catalyst Center on ESXi manages.
- In the Subject Alternative Name (SAN) field of Catalyst Center on ESXi certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.

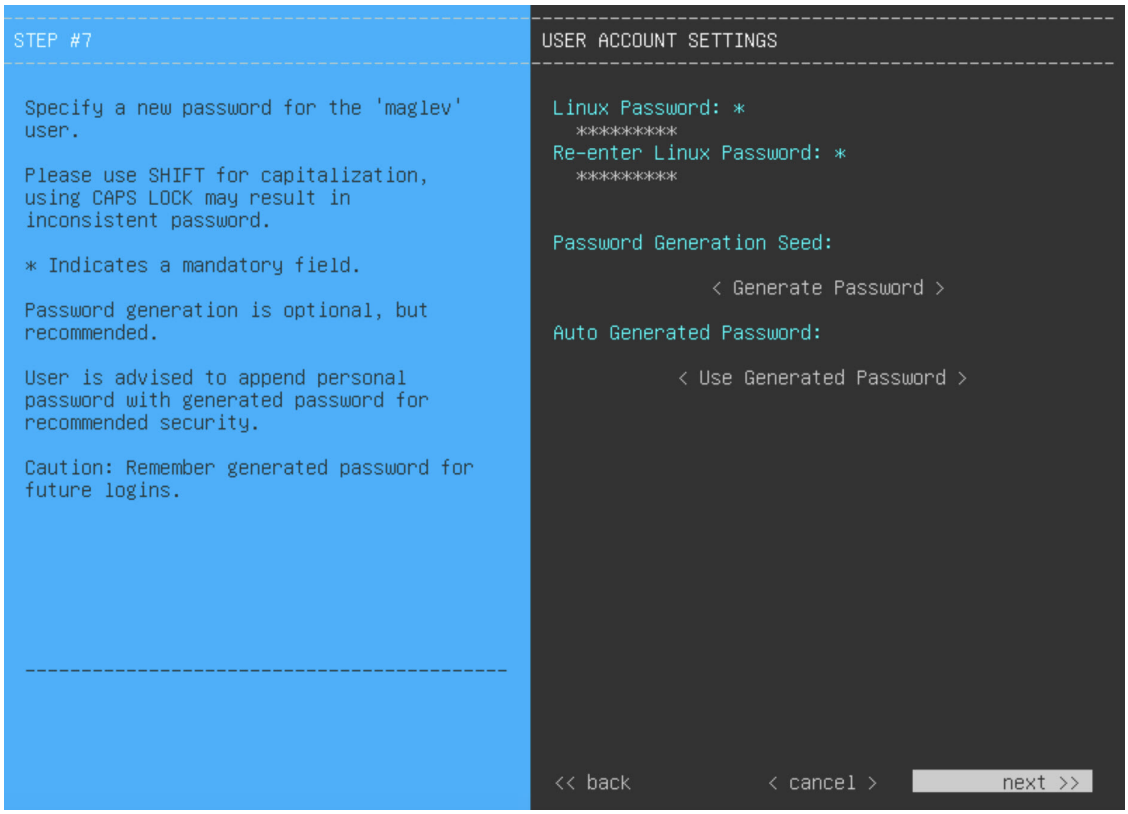
After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.



n) Enter the configuration values for the settings provided in the wizard's **USER ACCOUNT SETTINGS** page (as described in the following table), then click **next>>**.

Linux Password field	Enter and confirm the password for the `maglev` user.
Re-enter Linux Password field	Confirm the Linux password by entering it a second time.
Password Generation Seed field	If you do not want to create the Linux password yourself, enter a seed phrase in this field and then press <**Generate Password**> to generate the password.
Auto Generated Password field	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto-generated password. Press <**Use Generated Password**> to save the password.

After you provide the necessary information, correct any validation errors to proceed (if necessary).

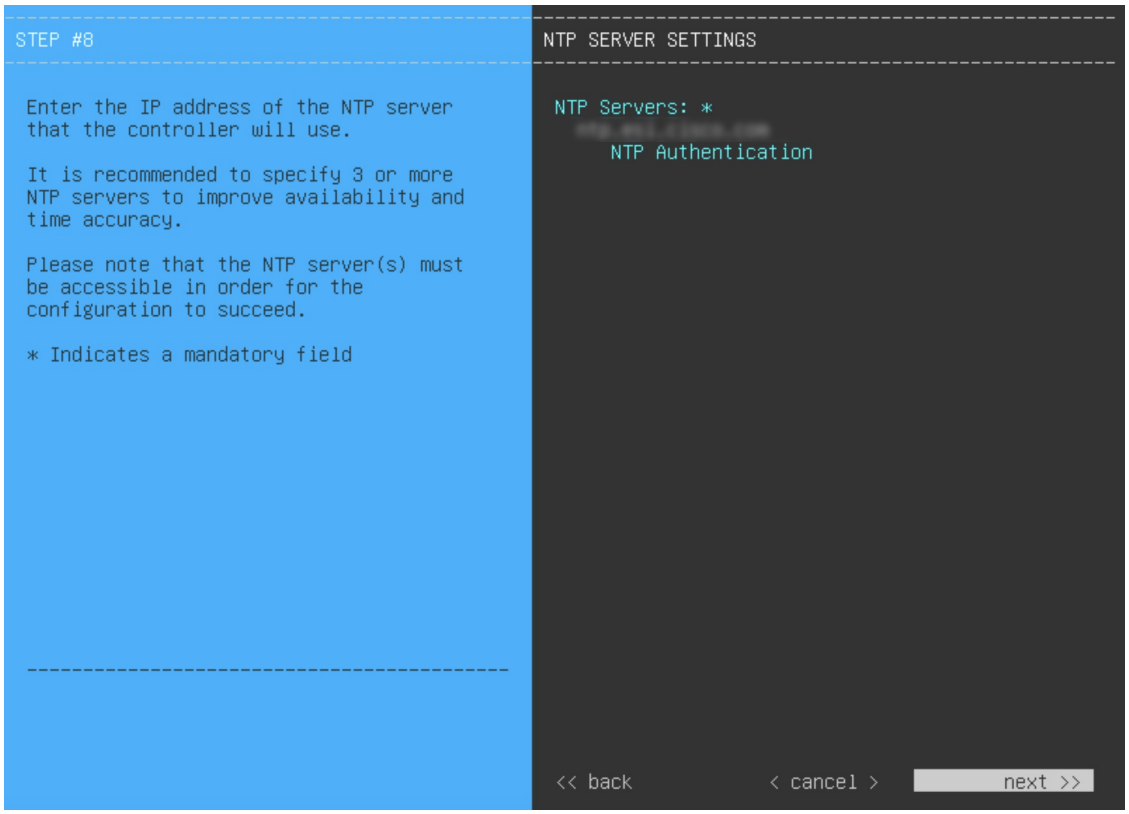


o) Enter the configuration values for the settings provided in the wizard's **NTP SERVER SETTINGS** page (as described in the following table), then click **next>>**.

NTP Servers field	Enter one or more NTP server addresses or hostnames, separated by spaces. At least one NTP address or hostname is required. For a production deployment, we recommend that you configure a minimum of three NTP servers to improve availability, time, and accuracy.
NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center on ESXi, check this check box and then enter the following information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file. **Note** Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

After you provide the necessary information, correct any validation errors to proceed (if necessary).

A final message appears, stating that the wizard is ready to apply the configuration.

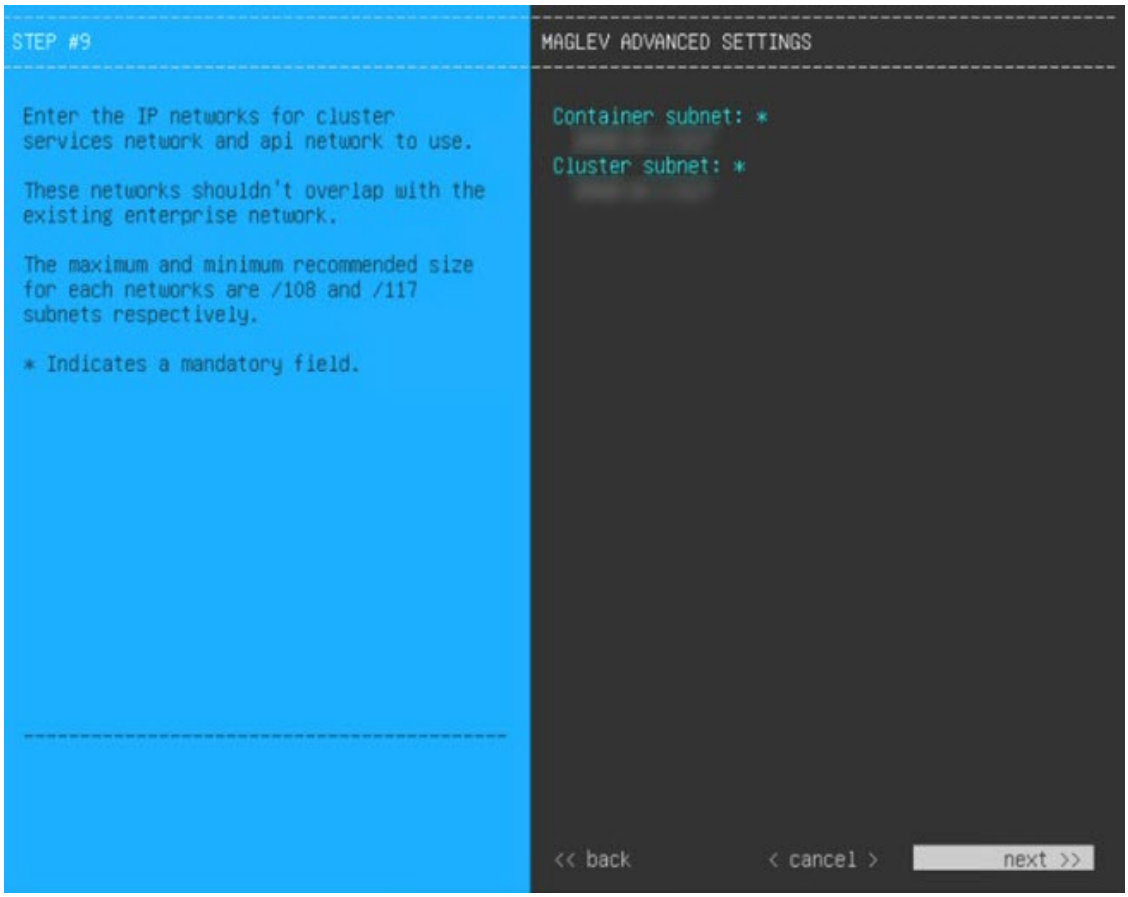


p) Enter the configuration values for the settings provided in the wizard's **MAGLEV ADVANCED SETTINGS** page, (as described in the following table), then click **next>>**.

Container Subnet field	A dedicated, non-routed IPv6 subnet that Catalyst Center on ESXi uses to manage internal services. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Catalyst Center on ESXi internal network or an external network.
Cluster Subnet field	A dedicated, non-routed IPv6 subnet that Catalyst Center on ESXi uses to manage internal cluster services. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Catalyst Center on ESXi internal network or an external network.

After you provide the necessary information, correct any validation errors to proceed (if necessary).

A final message appears, stating that the wizard is ready to apply the configuration.



q) To apply the settings you've entered to the virtual appliance, click **proceed>>**.

After the configuration process completes, the virtual appliance powers on again and displays a **CONFIGURATION SUCCEEDED!** message.

It takes around 180 to 210 minutes for the virtual machine to become operational. The actual time will depend on things like available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.

Step 4 Complete the Quick Start Workflow, on page 106.

Configure a Virtual Appliance Using the Web UI Install Configuration Wizard

If you want to configure a virtual appliance as quickly as possible using the browser-based Install configuration wizard and are okay with using preset appliance settings, complete the following procedure.

Important Ensure that all of the IP addresses you enter while completing this procedure are valid IPv4 addresses with valid IPv4 netmasks. Also make sure that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.

Before you begin

Ensure that you collected the following information:

- Static IP address
- Subnet mask
- Default gateway
- DNS address
- NTP server details
- Proxy server details

Ensure that you are using a supported browser. See Deployment Requirements, on page 3.

Ensure that you enabled ICMP on the firewall between Catalyst Center on ESXi and the DNS servers you will specify in the following procedure. This wizard uses Ping to verify the DNS server you specify. This ping can be blocked if there is a firewall between Catalyst Center on ESXi and the DNS server and ICMP is not enabled on that firewall. When this happens, you will not be able to complete the wizard.

Note The Intracluster interface is preconfigured when using this wizard. If you don't want to use the default settings for this interface, you'll need to complete the Configure a Virtual Appliance Using the Web UI Advanced Install Configuration Wizard for IPv4 Deployments.

Procedure

Step 1 After deployment completes, power on the newly-created virtual machine:

a) In the vSphere Web Client, right-click the virtual machine.

b) Choose **Power** > **Power On**.

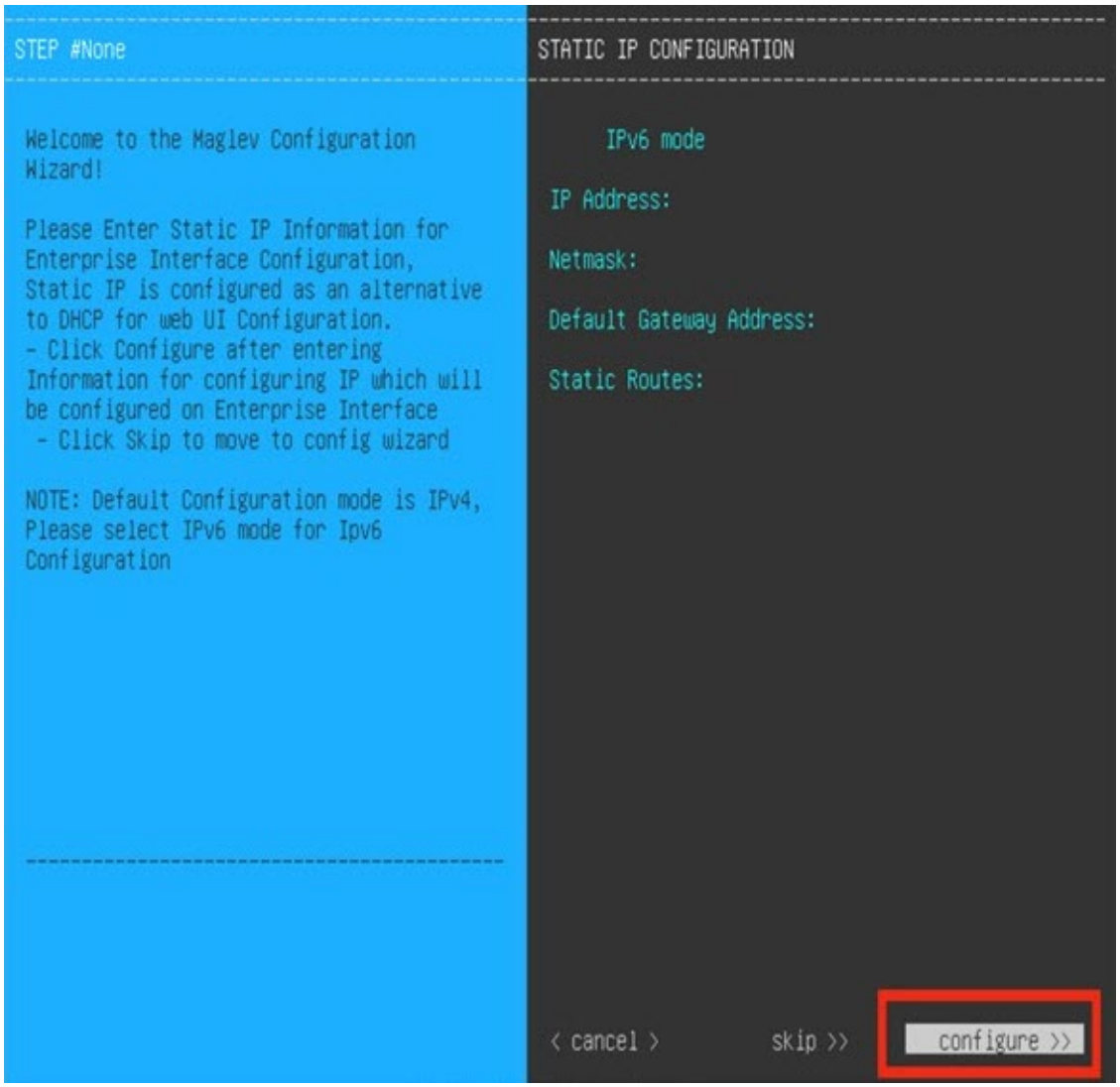
It takes around 45 minutes for the virtual machine to become operational. The actual time will depend on things like available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.

Step 2 Launch either the remote console or web console by clicking the appropriate link.

Step 3 Open the Install Configuration wizard:

a) In the **STATIC IP CONFIGURATION** page, do one of the following:

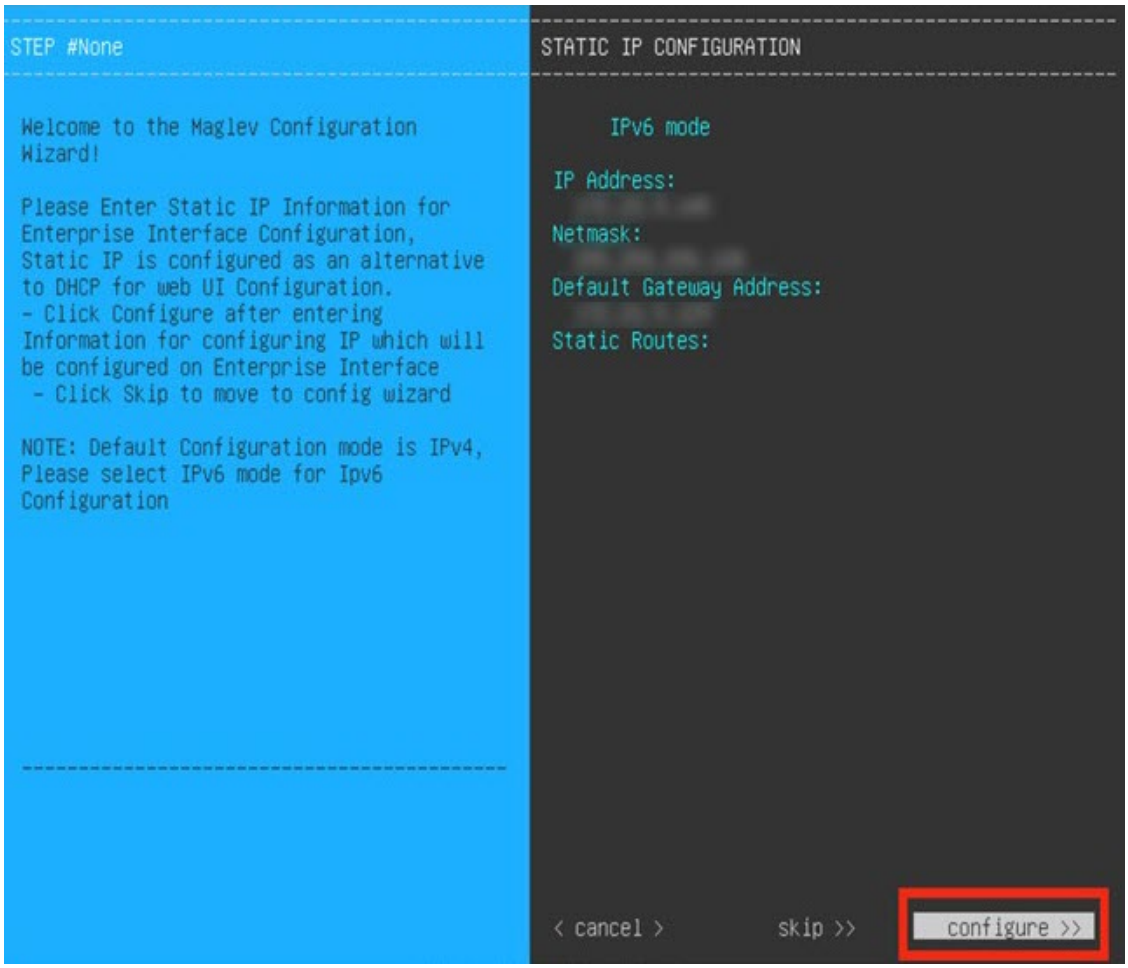
- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your virtual appliance's Enterprise interface, click **skip**>>.
- If you want to assign your own IP address, subnet mask, and default gateway to your virtual appliance's Enterprise interface, enter the information described in the following table and then click **configure**>>.



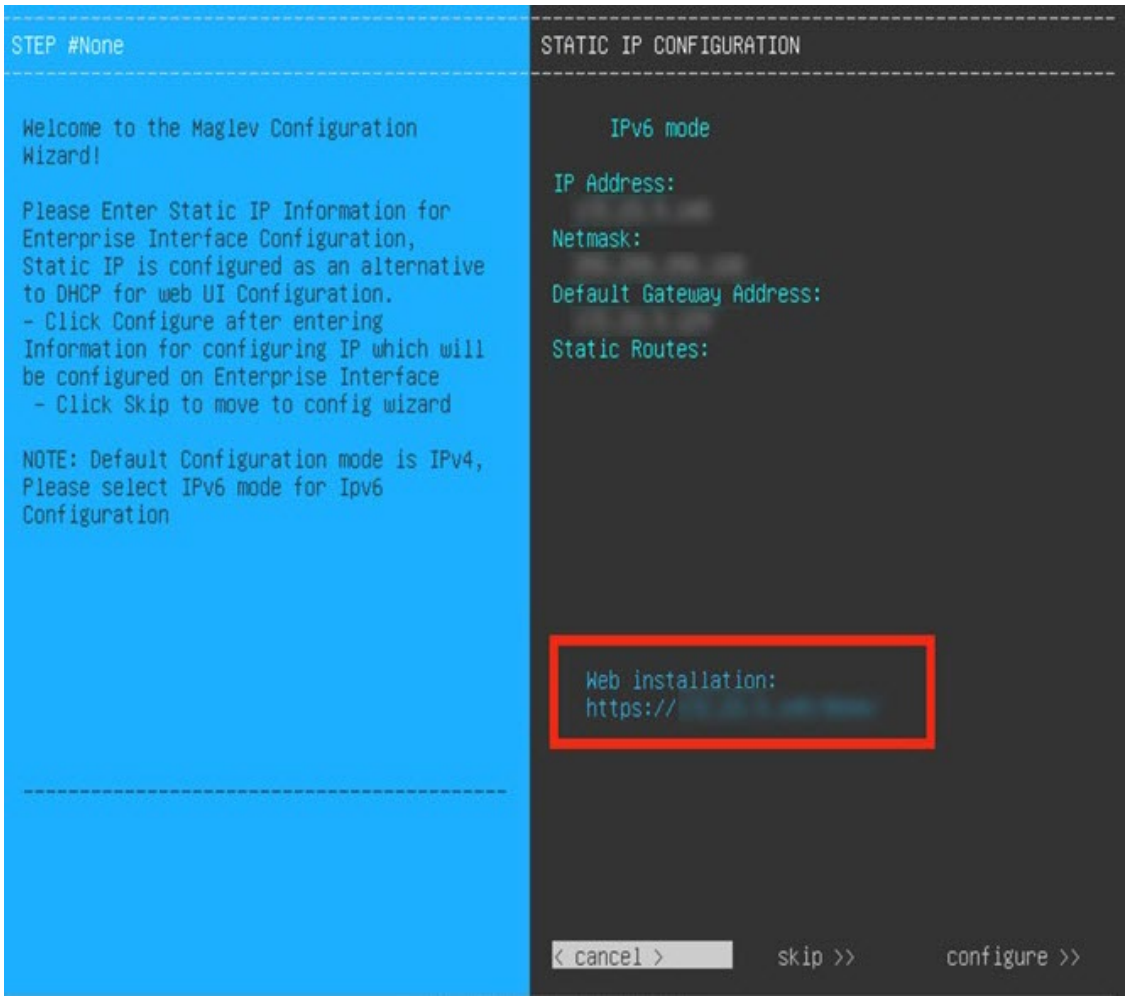
Note The **IPv6 Mode** check box is for enabling IPv6 addressing in advanced mode only. For IPv4 deployments, this check box needs to be unchecked.

IPv6 Mode check box	If you want to enable IPv6 addressing, you'll need to do so using the Configure a Virtual Appliance Using the Web UI Advanced Install Configuration Wizard for IPv4 Deployments. Leave this check box unchecked to use IPv4 addressing.
IP Address field	Enter the static IP address that you want to use.
Netmask field	Enter the netmask for the IP address you specified in the previous field. You can enter either a netmask or CIDR address.
Default Gateway Address field	Specify the default gateway that will be used to route traffic.
Static Routes field	You can't specify static routes when using this wizard, so leave this field blank.

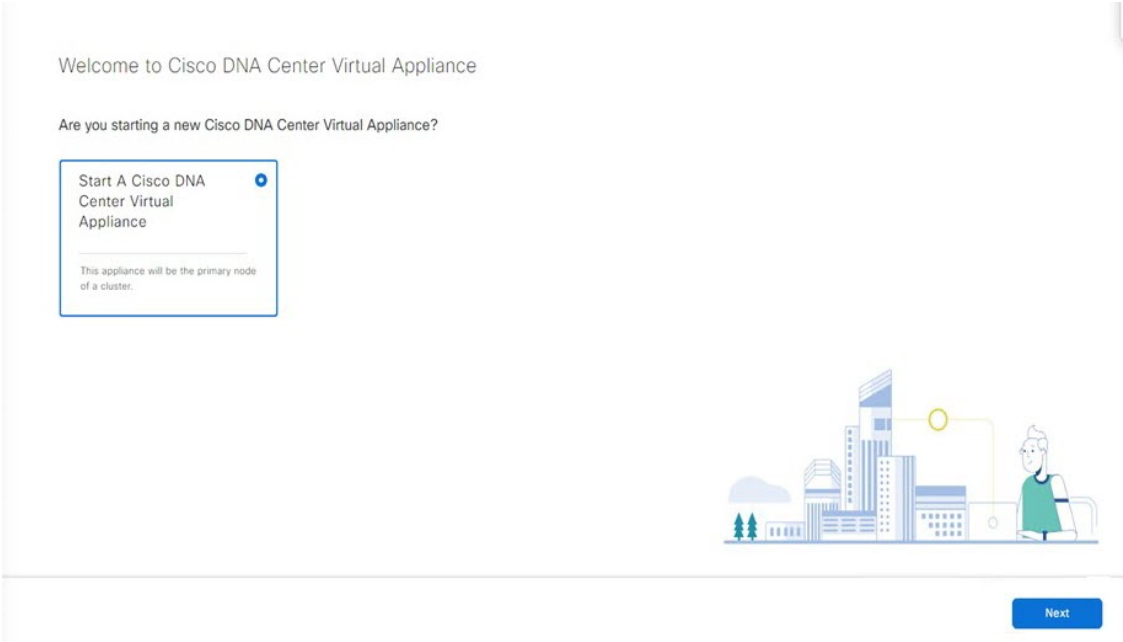
Note the URL listed in the **Web Installation** field. You'll need this for the next step.



b) Open the URL that was displayed in the **Static IP Configuration** page.

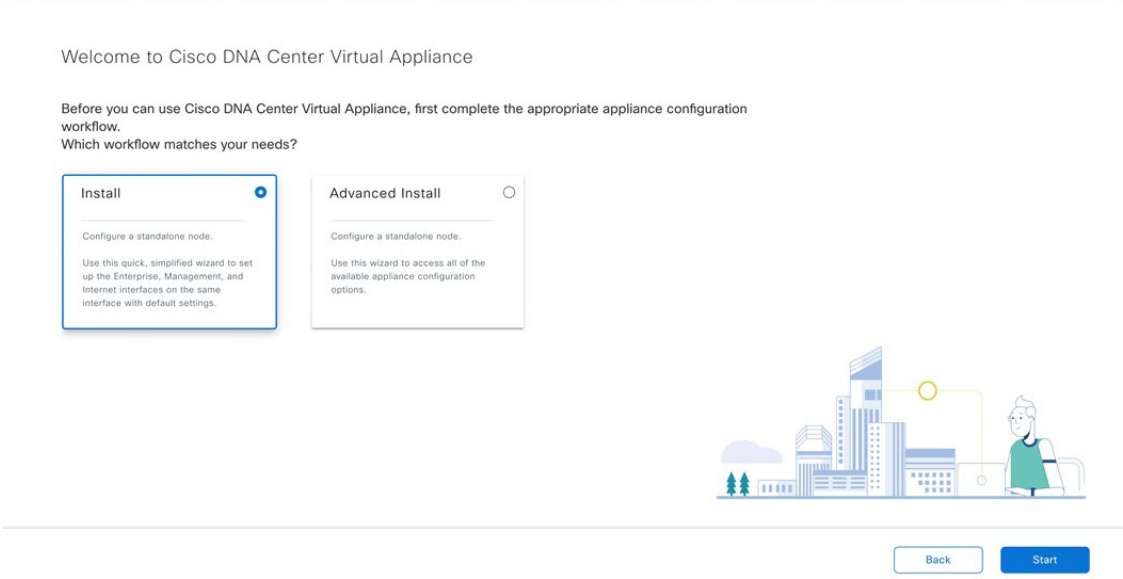


c) Click the **Start a Catalyst Center Virtual Appliance** radio button, then click **Next**.



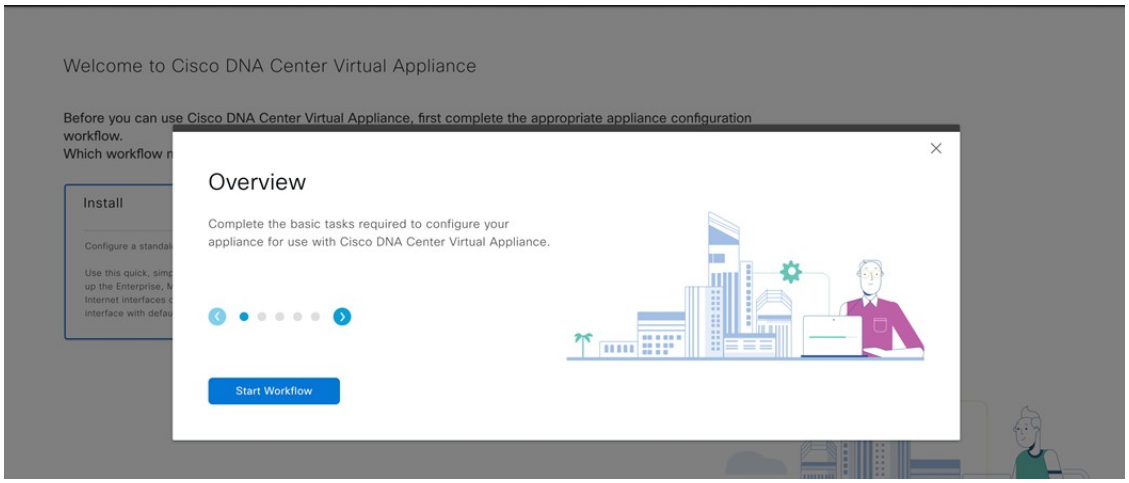
d) Click the **Install** radio button, then click **Start**.

The **Overview** slider opens. Click > to view a summary of the tasks that the wizard will help you complete.



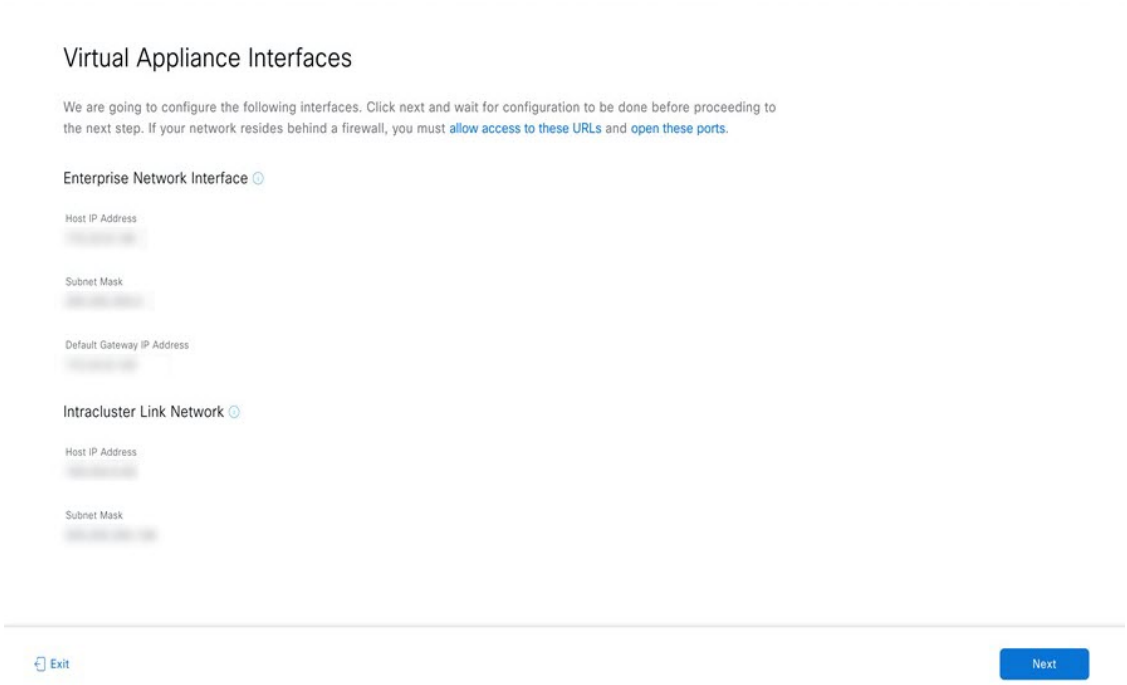
e) Click **Start Workflow** to start the wizard.

The **Virtual Appliance Interfaces** page opens.



Step 4 Configure your virtual appliance by completing the Install Configuration wizard:

a) Click **Next**.

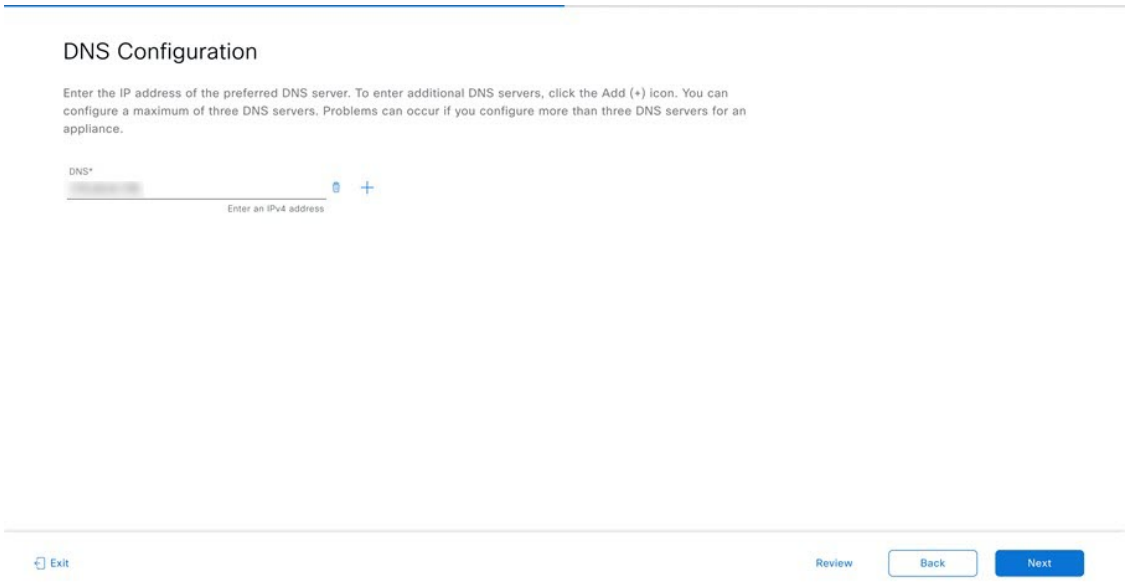


The **DNS Configuration** page opens.

b) In the **DNS** field, enter the IP address of the preferred DNS server. To enter additional DNS servers, click the **Add** (+) icon.

Important You can configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.

c) Click **Next**.

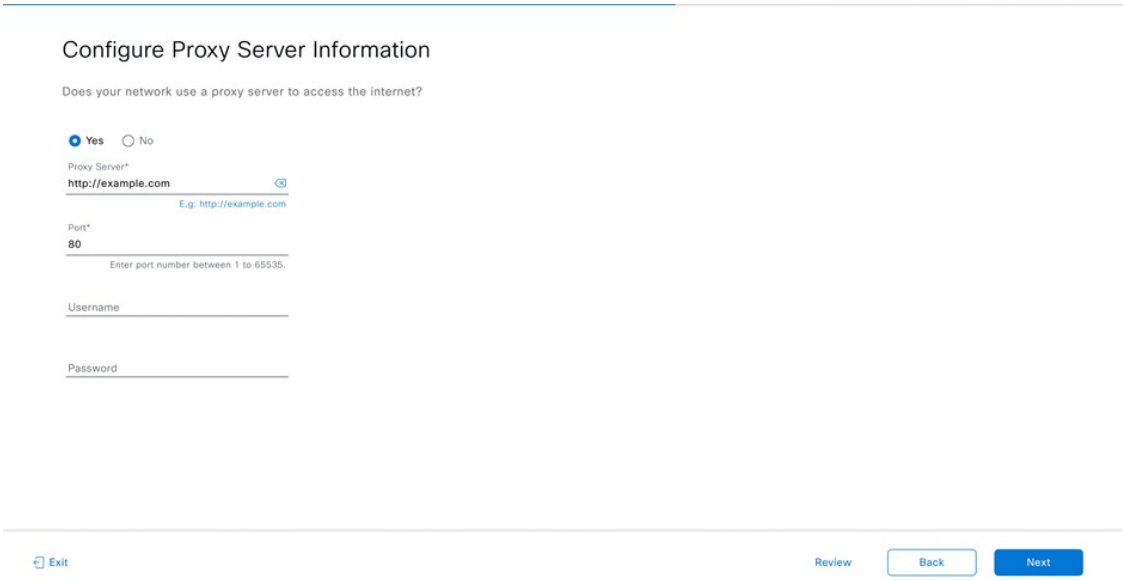


The **Configure Proxy Server Information** page opens.

d) Do one of the following:

- If your network does *not* use a proxy server to access the internet, click the **No** radio button and then click **Next**.
- If your network does use a proxy server to access the internet, enter the values described in the following table and then click **Next**.

Proxy Server field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** Connection from Catalyst Center on ESXi to the HTTPS proxy is supported only via HTTP in this release.
Port field	Enter the port that your appliance used to access the network proxy.
Username field	Enter the username used to access the network proxy. If no proxy login is required, leave this field blank.
Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

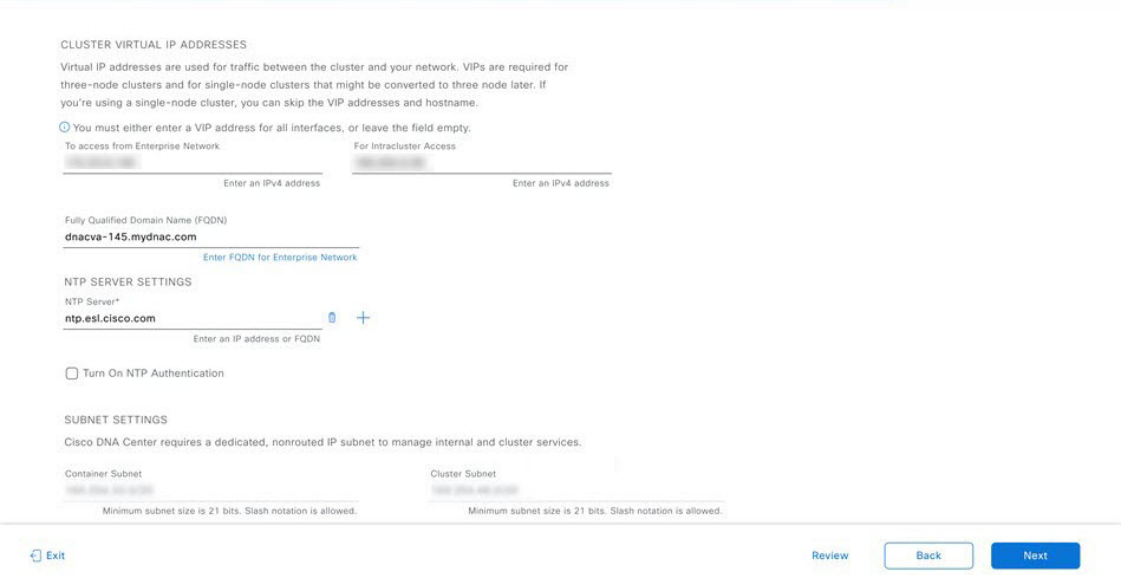


The wizard's **Advanced Appliance Settings** page opens.

e) Enter configuration values for your appliance, then click **Next**.

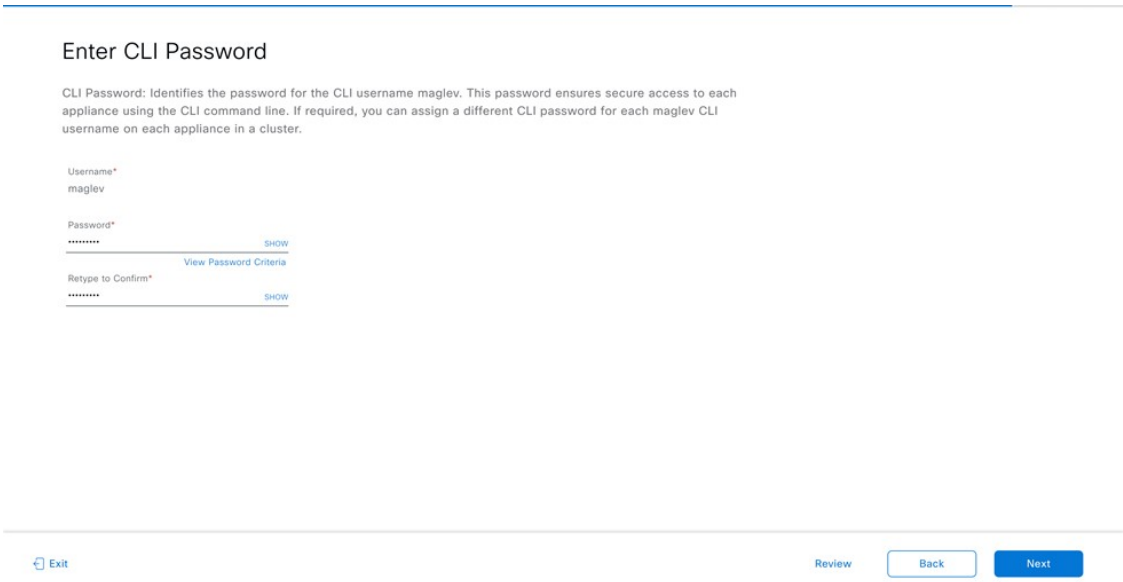
Cluster Virtual IP Addresses	
To access from Enterprise Network and For Intracluster Access fields	Enter the virtual IP address configured for the Enterprise interface. If you configured a virtual IP address for the Management interface, enter this address as well (using a comma to separate the two IP addresses).
Fully Qualified Domain Name (FQDN) field	You can also specify the fully qualified domain name (FQDN) for your virtual appliance. Catalyst Center on ESXi uses this domain name to do the following: • It uses this hostname to access your virtual appliance's web interface and the Representational State Transfer (REST) APIs used by devices in the enterprise network that Catalyst Center on ESXi manages. • In the Subject Alternative Name (SAN) field of Catalyst Center on ESXi certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.
NTP Server Settings	
NTP Server field	Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the **Add** (+) icon. For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.

Turn on NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center on ESXi, check this check box and then enter the following information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file. **Note** Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.
Subnet Settings	
Container Subnet field	A dedicated, non-routed IP subnet that Catalyst Center on ESXi uses to manage internal services. By default, this is already set to **169.254.32.0/20**, and you cannot enter another subnet.
Cluster Subnet field	A dedicated, non-routed IP subnet that Catalyst Center on ESXi uses to manage internal cluster services. By default, this is already set to **169.254.48.0/20**, and you cannot enter another subnet.



The **Enter CLI Password** page opens.

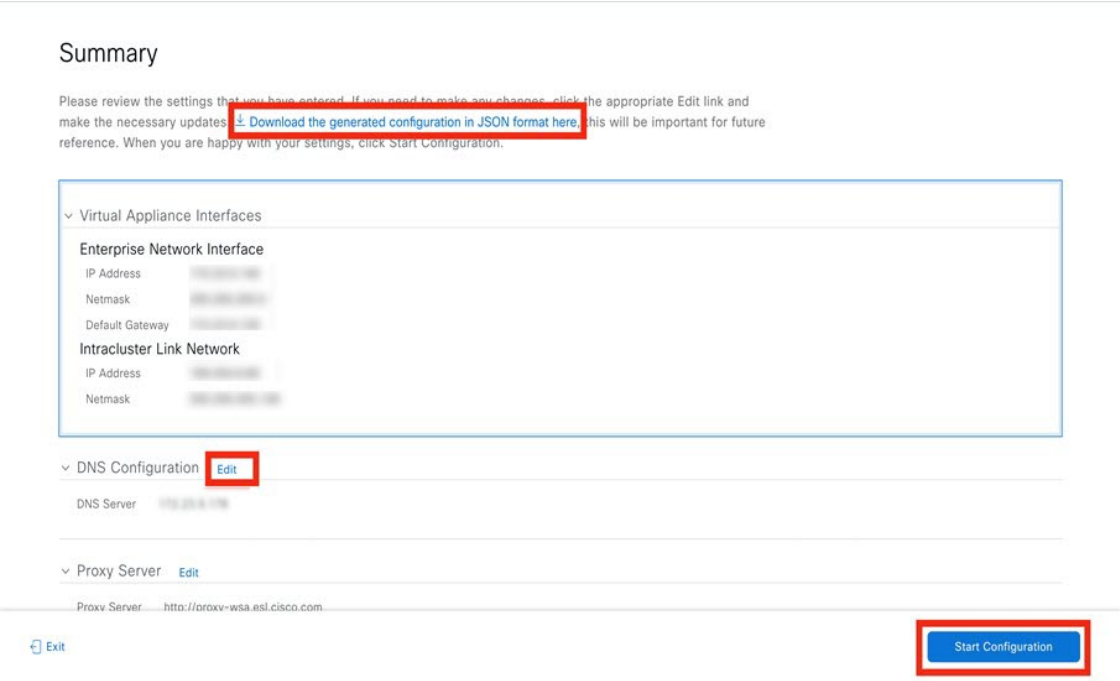
f) Enter and confirm the password for the `maglev` user, then click **Next**.



The wizard validates the information that you entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you entered are valid, the wizard's **Summary** page opens.

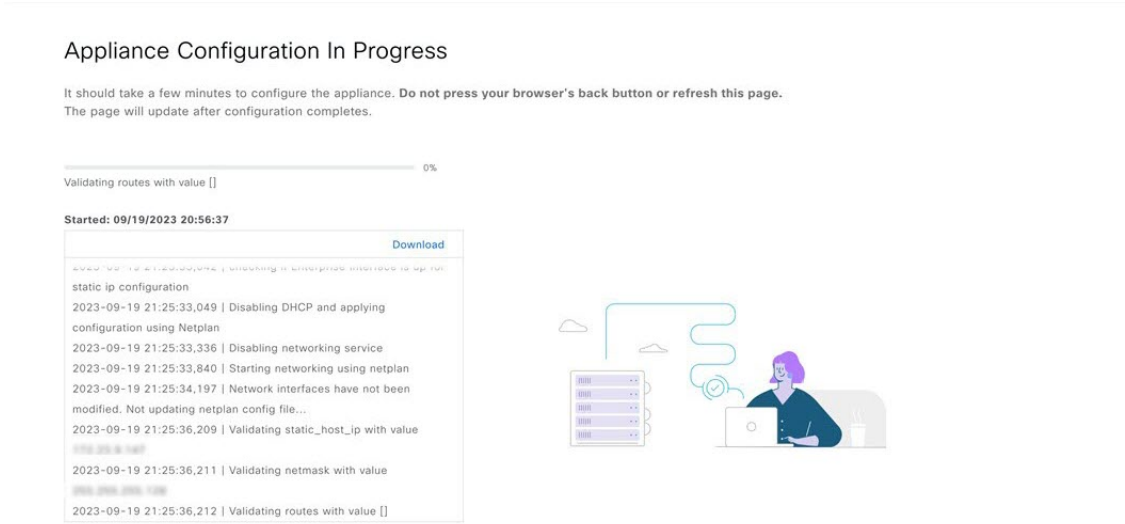
Note To download the appliance configuration as a JSON file, click the corresponding link.

g) Scroll to the bottom of the screen and review all of the settings that you have entered while completing the wizard. If necessary, click the appropriate **Edit** link to open the wizard screen in which you want to make updates.

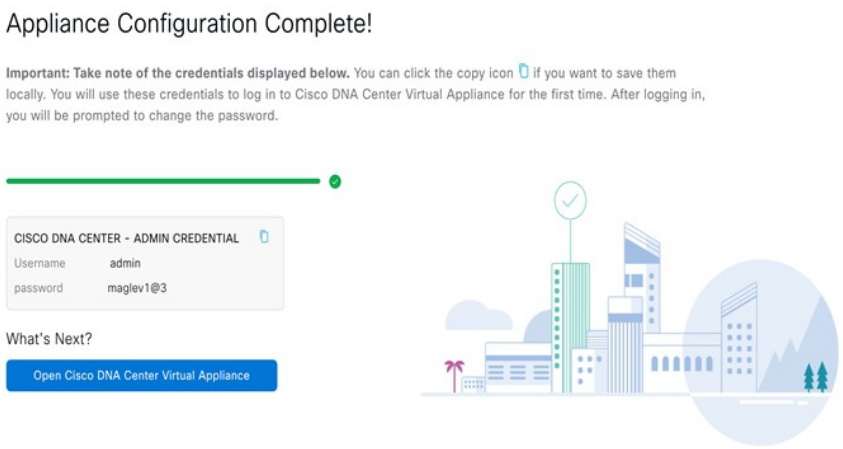


h) To complete the configuration of your Catalyst Center on ESXi virtual appliance, click **Start Configuration**.

The wizard screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred. To save a local copy of this information as a text file, click the **Download** link.



Step 5 After appliance configuration completes, click the copy icon to copy the default admin superuser password.



Important Catalyst Center on ESXi automatically sets this password when you complete the Install configuration wizard. Ensure that you click the copy icon before you proceed. Otherwise, you will not be able to log in to Catalyst Center on ESXi for the first time.

Note As a security measure, you'll be prompted to change this password after you log in. For more information, see Complete the Quick Start Workflow, on page 106.

Configure a Virtual Appliance Using the Web UI Advanced Install Configuration Wizard for IPv4 Deployments

If you want to configure a virtual appliance using the browser-based Advanced Install configuration wizard and need to specify settings that are different from the preset appliance settings, complete the following procedure.

Important Ensure that all of the IP addresses you enter while completing this procedure are valid IPv4 addresses with valid IPv4 netmasks. Also make sure that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.

Before you begin

Ensure that you collected the following information:

- Static IP address
- Subnet mask
- Default gateway
- DNS address
- NTP server details
- Proxy server details

Ensure you are using a supported browser. See Deployment Requirements, on page 3.

Ensure you enabled ICMP on the firewall between Catalyst Center on ESXi and both the default gateway and the DNS server you specify in the following procedure. The wizard uses ping to verify the gateway and DNS server you specify. This ping might get blocked if a firewall is in place and ICMP is not enabled on that firewall. When this happens, you will not be able to complete the wizard.

Procedure

Step 1 After deployment completes, power on the newly-created virtual machine:

a) In the vSphere Web Client, right-click the virtual machine.

b) Choose **Power** > **Power On**.

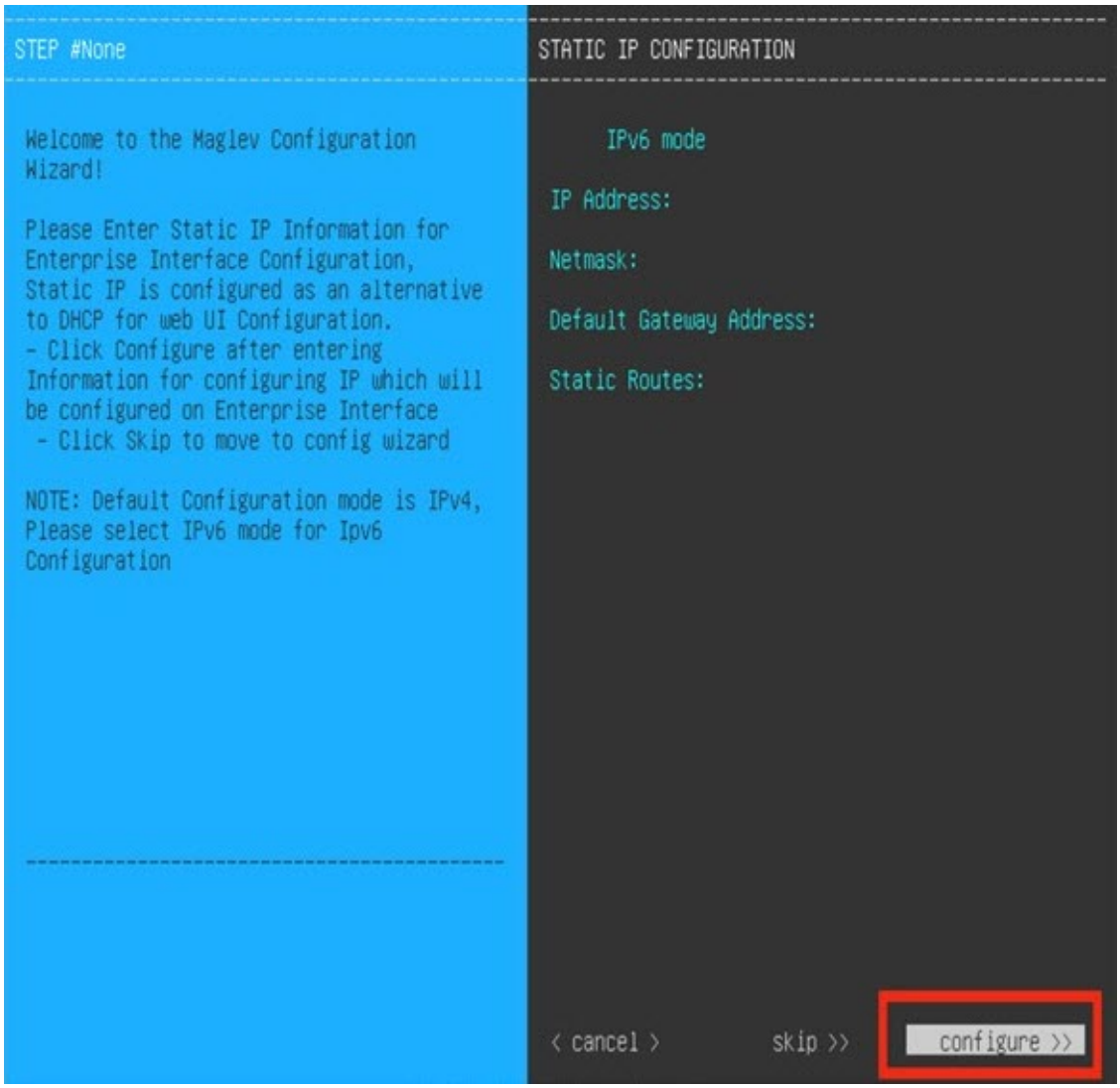
It takes around 90 to 120 minutes for the virtual machine to become operational. The actual time will depend on things like available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.

Step 2 Launch either the remote console or web console by clicking the appropriate link.

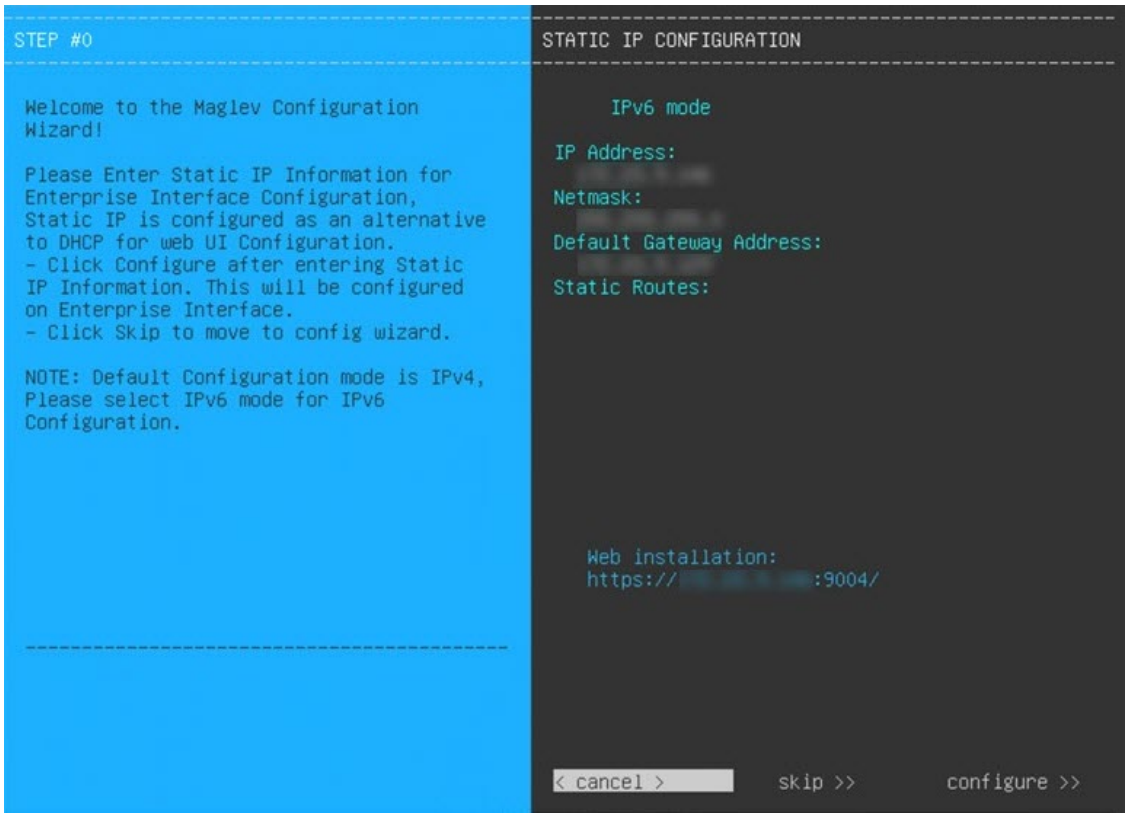
Step 3 Open the Advanced Install Configuration wizard:

a) In the **STATIC IP CONFIGURATION** page, do one of the following:

- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your virtual appliance's Enterprise interface, click **skip**>>.
- If you want to assign your own IP address, subnet mask, and default gateway to your virtual appliance's Enterprise interface, enter the information described in the following table and then click **configure**>>.



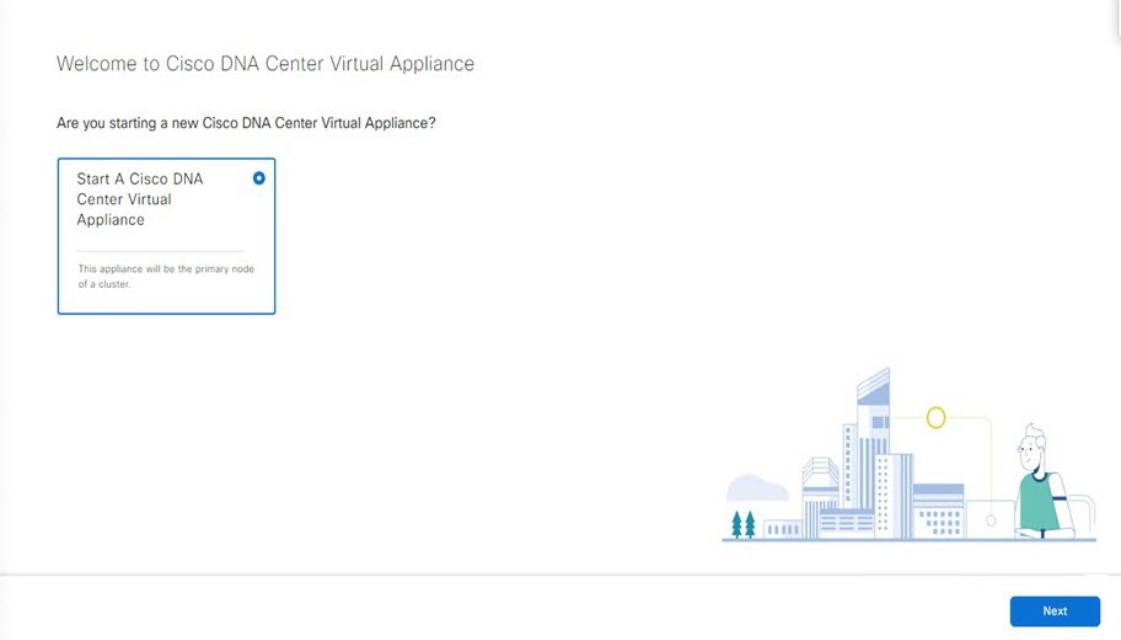
IPv6 Mode check box	IPv6 is supported. However, if you want to deploy IPv4, leave this check box unchecked.
IP Address field	Enter the static IP address that you want to use.
Netmask field	Enter either a netmask or CIDR address for the IP address you specified in the previous field.
Default Gateway Address field	Specify the default gateway that will be used to route traffic.
Static Routes field	You can't specify static routes when using this wizard, so leave this field blank.



Note the URL listed in the **Web Installation** field. You'll need this for the next step.

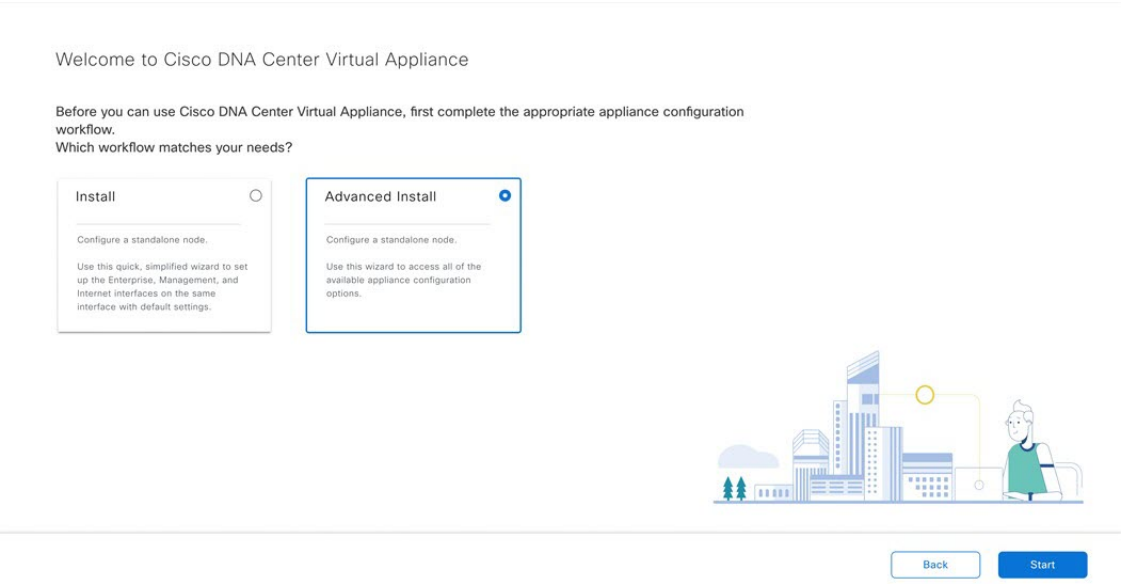
b) Open the URL that was displayed in the **Static IP Configuration** page.

c) Click the **Start a Catalyst Center Virtual Appliance** radio button, then click **Next**.



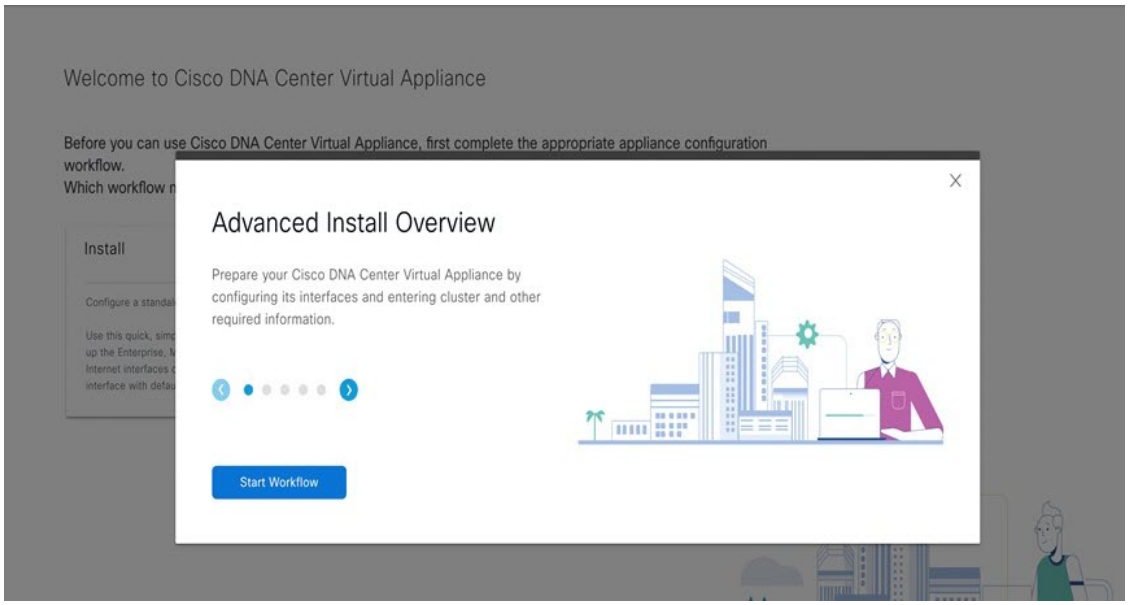
d) Click the **Advanced Install** radio button, then click **Start**.

The **Advanced Install Overview** slider opens. Click > to view a summary of the tasks that the wizard will help you complete.



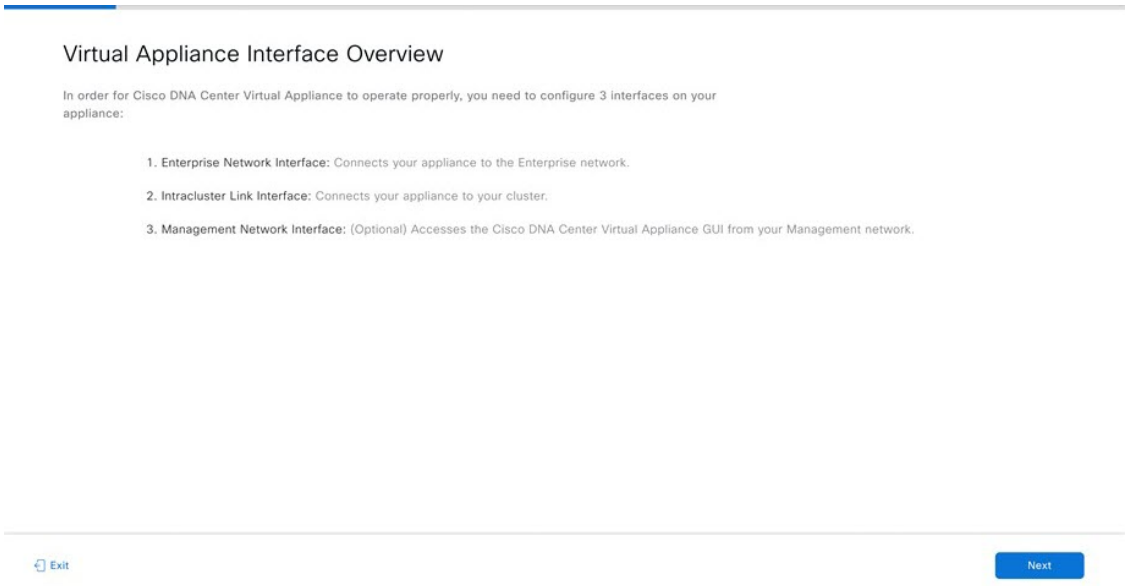
e) Click **Start Workflow** to start the wizard.

The **Virtual Appliance Interface Overview** page opens, providing a description of the four appliance interfaces that you can configure.

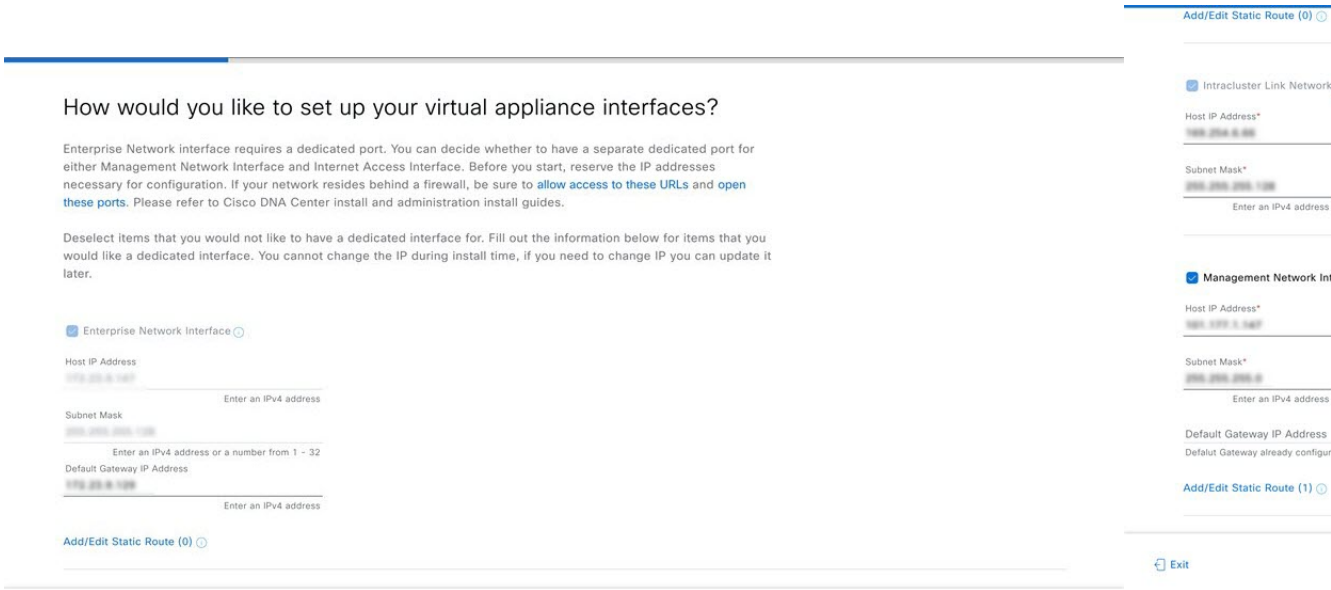


Step 4 Configure your virtual appliance by completing the Advanced Install Configuration wizard:

a) Click **Next**.



The **How would you like to set up your appliance interfaces?** page opens



If your network resides behind a firewall, do the following:

- Click the **allow access to these URLs** link to view a pop-up window that lists the URLs that Catalyst Center on ESXi must be able to access.
- Click the **open these ports** link to view a pop-up window that lists the network service ports that must be available for Catalyst Center on ESXi to use.

By default, the **Enterprise Network Interface** check box is already checked. It's also prepopulated with the values you entered in the **STATIC IP CONFIGURATION** page.

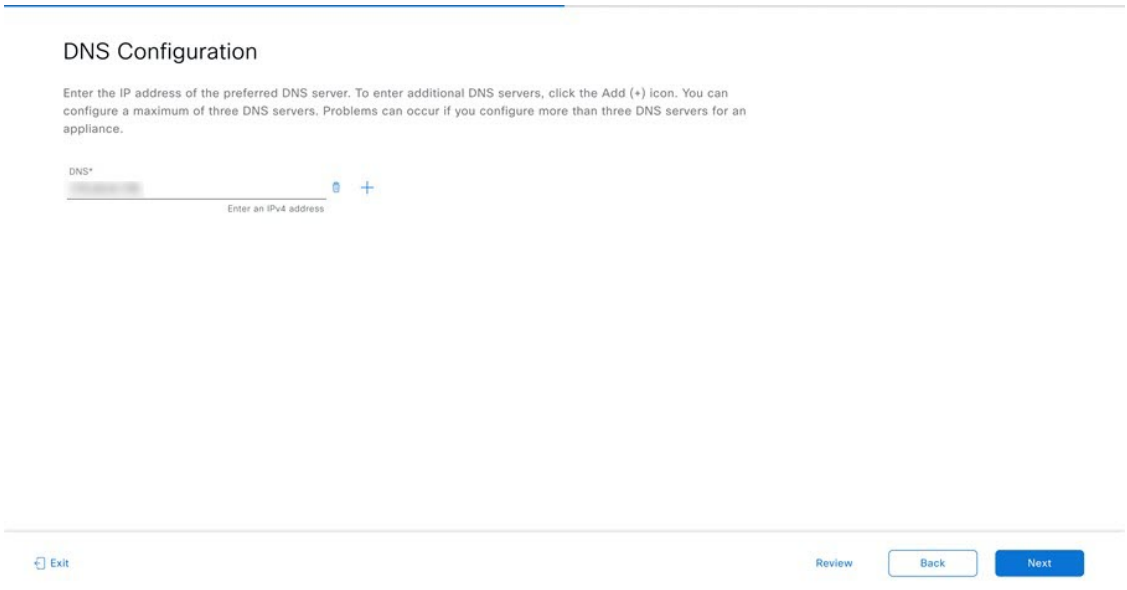
b) Do the following for each appliance interface you want to use, then click **Next**:

- Click its check box and enter the appropriate configuration values.
- If necessary, click its **Add/Edit Static Route** link to configure static routes. Click **+** as needed to configure additional routes. When you're done, click **Add**.

The **DNS Configuration** screen opens.

c) Enter the IP address of the preferred DNS server, then click **Next**. To enter additional DNS servers, click the **Add** (+) icon.

Important
- For each node in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
- For NTP, ensure port 123 (UDP) is open between Catalyst Center on ESXi and your NTP server.

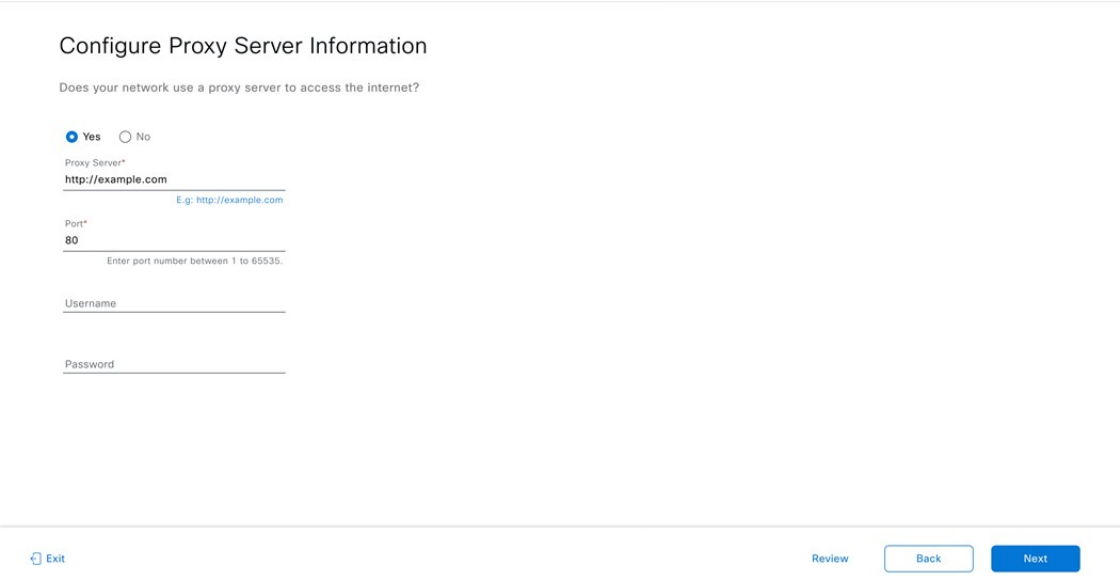


The **Configure Proxy Server Information** screen opens.

d) Do one of the following and then click **Next**:
- If your network does *not* use a proxy server to access the internet, click the **No** radio button.
- If your network does use a proxy server to access the internet, enter the values described in the following table:

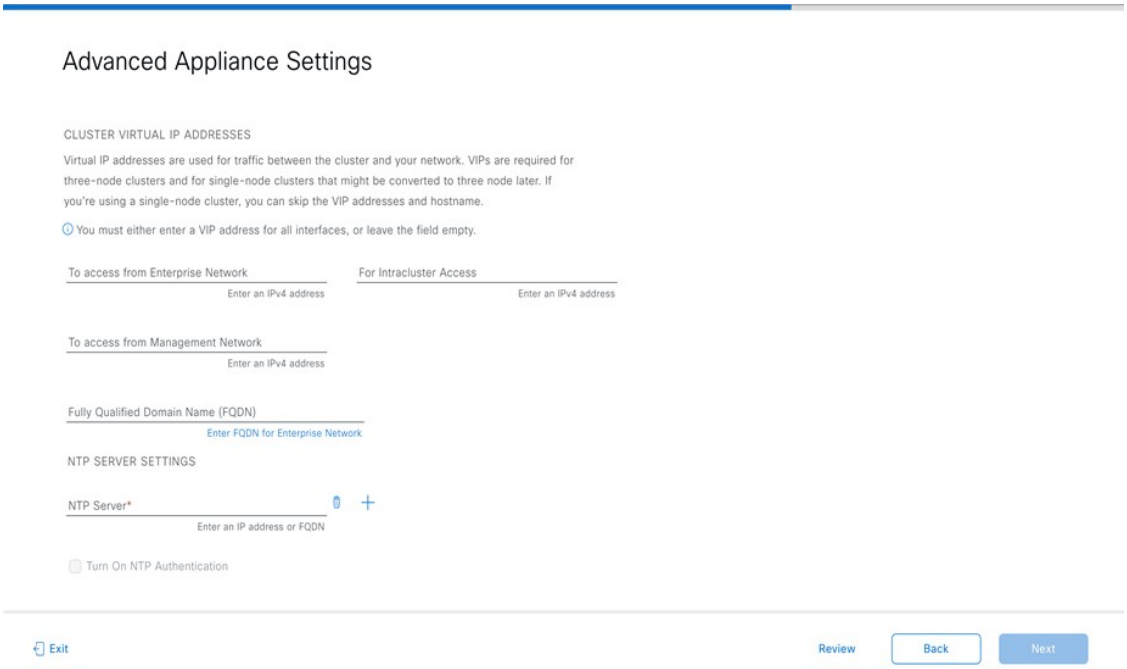
Proxy Server field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** Connection from Catalyst Center on ESXi to the HTTPS proxy is supported only via HTTP in this release.
Port field	Enter the port your appliance used to access the network proxy.
Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.

Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.



The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Advanced Appliance Settings** screen opens.

e) Enter configuration values for your appliance, then click **Next**.

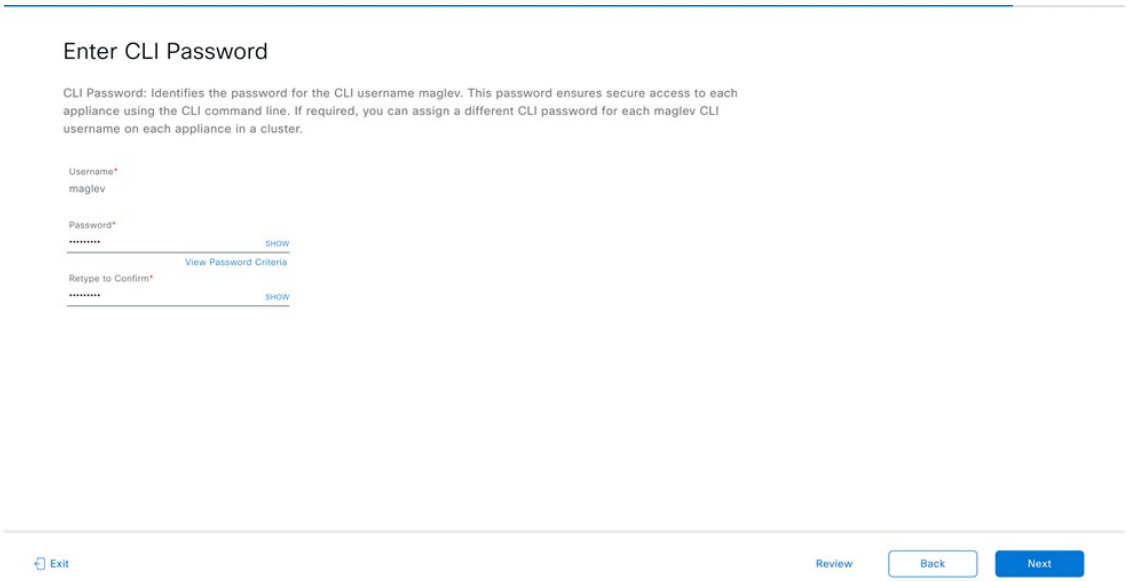


Cluster Virtual IP Addresses

To access from Enterprise Network and For Intracluster Access fields	Enter the virtual IP address configured for the Enterprise interface. If you configured a virtual IP address for the Management interface, enter this address as well (using a comma to separate the two IP addresses).
Fully Qualified Domain Name (FQDN) field	You can also specify the fully qualified domain name (FQDN) for your virtual appliance. Catalyst Center on ESXi uses this domain name to do the following: • It uses this hostname to access your virtual appliance's web interface and the Representational State Transfer (REST) APIs used by devices in the enterprise network that Catalyst Center on ESXi manages. • In the Subject Alternative Name (SAN) field of Catalyst Center on ESXi certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.
NTP Server Settings	
NTP Server field	Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the **Add** (+) icon. For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.
Turn On NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center on ESXi, check this check box and then enter the following information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file. **Note** Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.
Subnet Settings	
Container Subnet field	A dedicated, non-routed IP subnet that Catalyst Center on ESXi uses to manage internal services. By default, this is already set to **169.254.32.0/20**, and we recommend that you use this subnet.
Cluster Subnet field	A dedicated, non-routed IP subnet that Catalyst Center on ESXi uses to manage internal cluster services. By default, this is already set to **169.254.48.0/20**, and we recommend that you use this subnet.

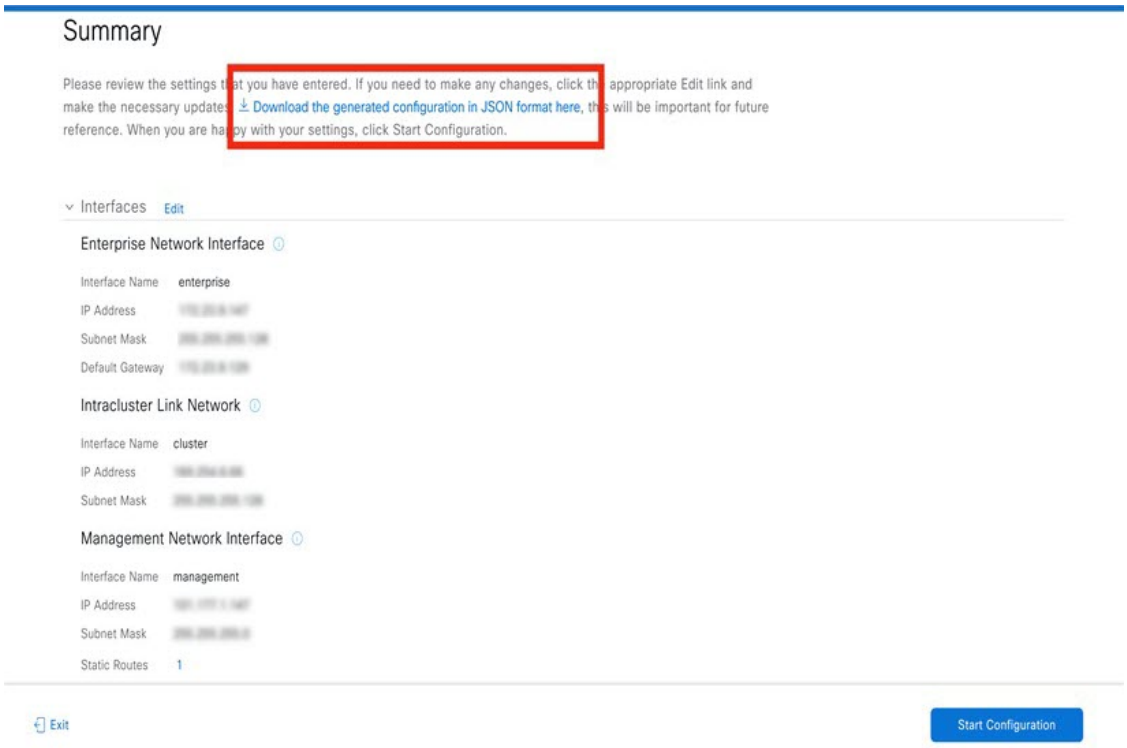
The **Enter CLI Password** page opens.

f) Enter and confirm the password for the `maglev` user, then click **Next**.



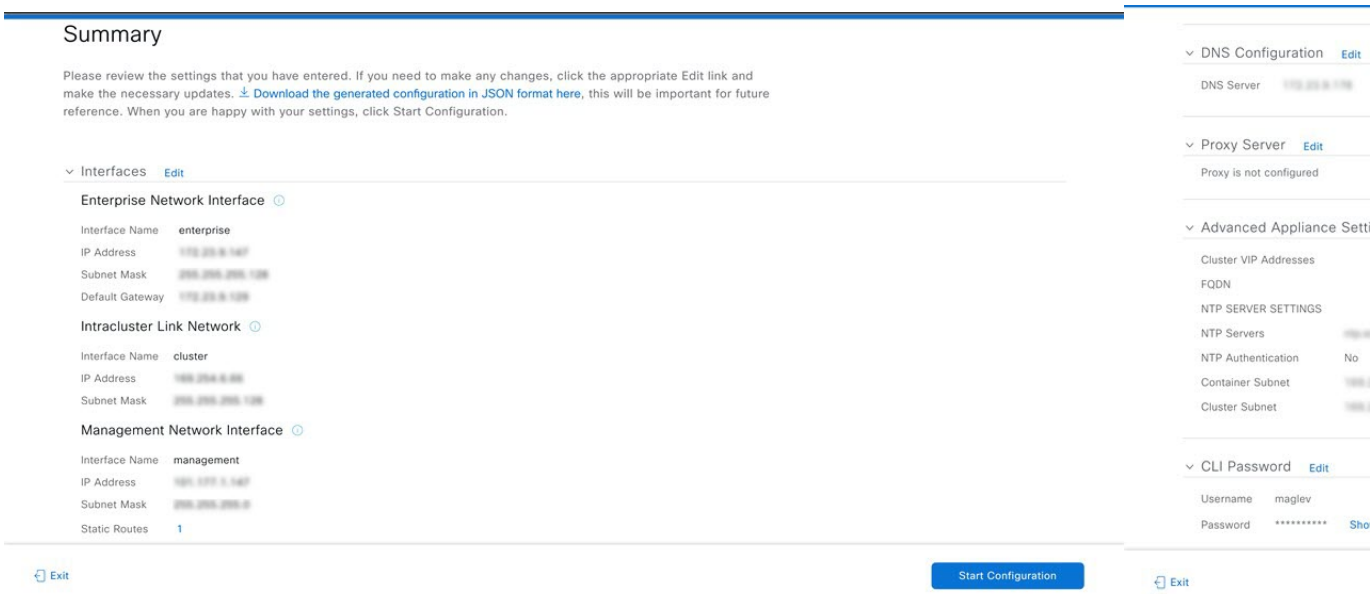
The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Summary** page opens.

Note To download the appliance configuration as a JSON file, click the corresponding link.



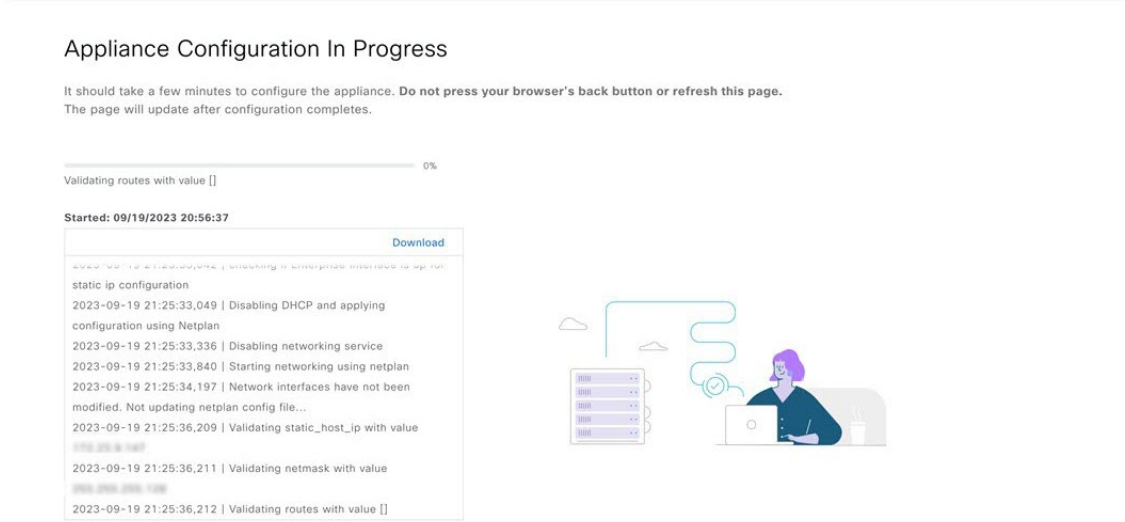
g) Scroll to the bottom of the screen and review all of the settings that you have entered while completing the wizard. If necessary, click the appropriate **Edit** link to open the wizard screen in which you want to make updates.

h) To complete the configuration of your Catalyst Center on ESXi virtual appliance, click **Start Configuration**.



The wizard screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred. To save a local copy of this information as a text file, click the **Download** link.

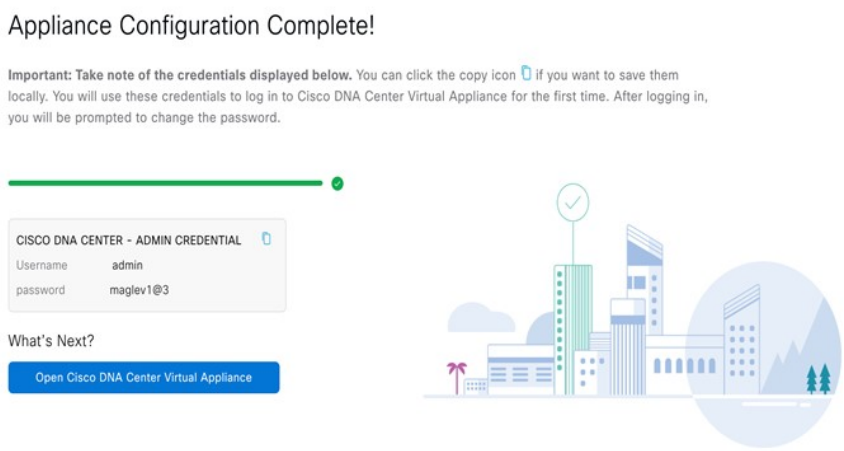
It takes around 180 to 210 minutes for the virtual machine to become operational. The actual time will depend on things like available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.



Step 5 After appliance configuration completes, click the copy icon to copy the default admin superuser password.

It can take from 15-30 mins for services to be stabilized before you can login to the UI.

Important Catalyst Center on ESXi automatically sets this password when you complete the Install configuration wizard. Ensure that you click the copy icon before you proceed. Otherwise, you will not be able to log in to Catalyst Center on ESXi for the first time.



Note As a security measure, you'll be prompted to change this password after you log in. For more information, see Complete the Quick Start Workflow, on page 106.

Configure a Virtual Appliance Using the Web UI Advanced Install Configuration Wizard for IPv6 Deployments

If you want to configure a virtual appliance using the browser-based Advanced Install configuration wizard and need to specify settings that are different from the preset appliance settings, complete the following procedure.

Important Ensure that all of the IP addresses you enter while completing this procedure are valid IPv4 addresses with valid IPv4 netmasks. Also make sure that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.

Before you begin

Ensure that you collected the following information:

- Static IP address
- Subnet mask
- Default gateway
- DNS address
- NTP server details
- Proxy server details

Ensure that you are using a supported browser. See Deployment Requirements, on page 3.

Ensure that you enabled ICMP on the firewall between Catalyst Center on ESXi and both the default gateway and the DNS server you specify in the following procedure. The wizard uses ping to verify the gateway and DNS server you specify. This ping might get blocked if a firewall is in place and ICMP is not enabled on that firewall. When this happens, you will not be able to complete the wizard.

Procedure

Step 1 After deployment completes, power on the newly-created virtual machine:

a) In the vSphere Web Client, right-click the virtual machine.

b) Choose **Power** > **Power On**.

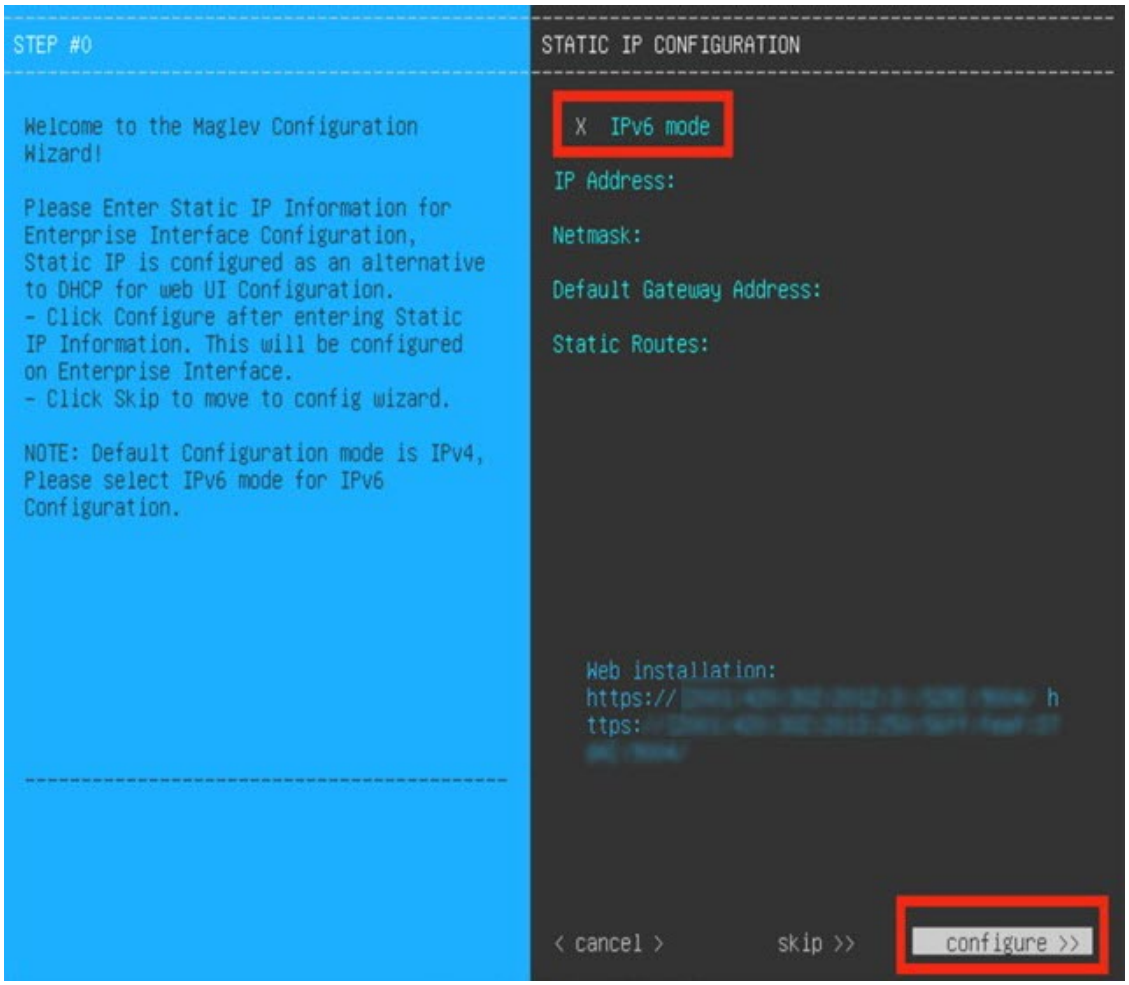
It takes around 90 to 120 minutes for the virtual machine to become operational. The actual time will depend on things like available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.

Step 2 Launch either the remote console or web console by clicking the appropriate link.

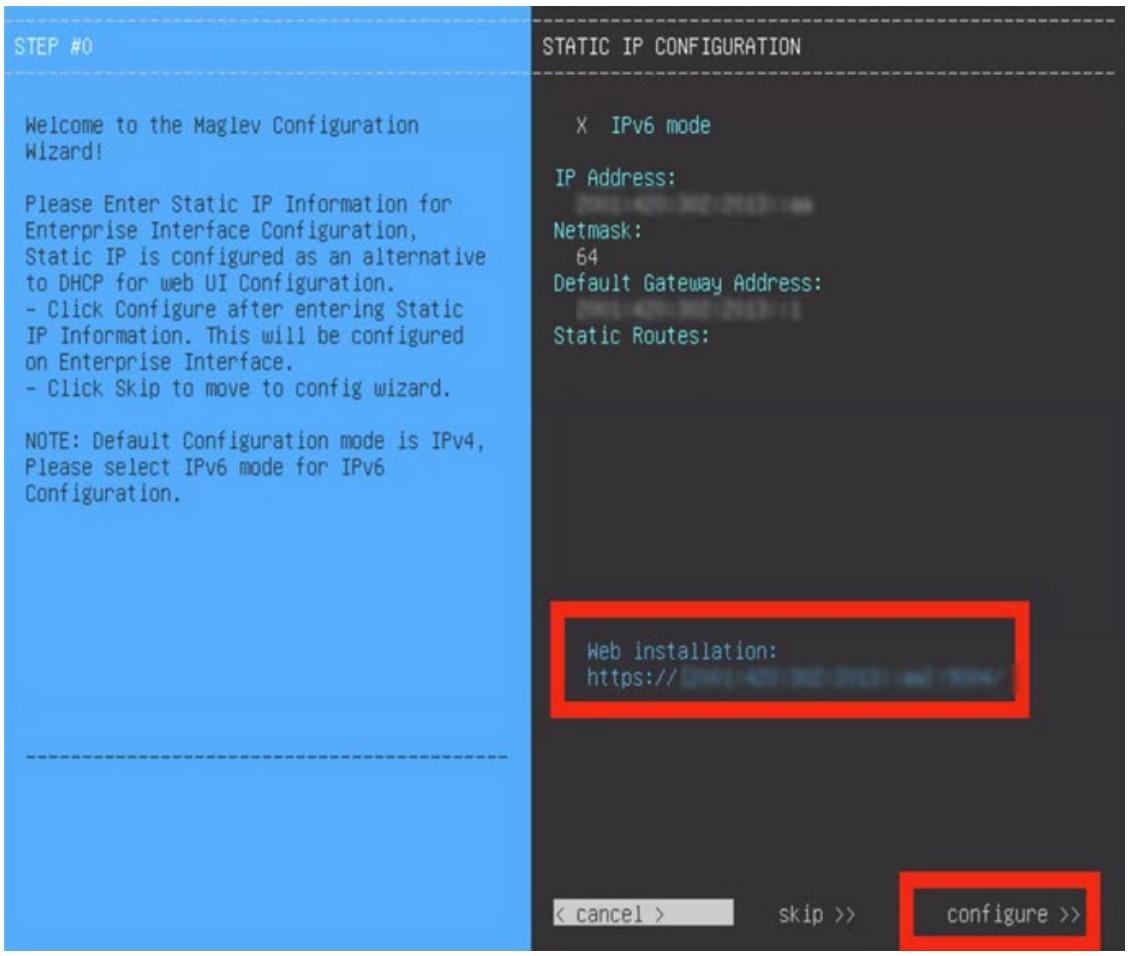
Step 3 Open the Advanced Install Configuration wizard:

a) In the **STATIC IP CONFIGURATION** page, do one of the following:

- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your virtual appliance's Enterprise interface, click **skip**>>.
- If you want to assign your own IP address, subnet mask, and default gateway to your virtual appliance's Enterprise interface, enter the information described in the following table and then click **configure**>>.



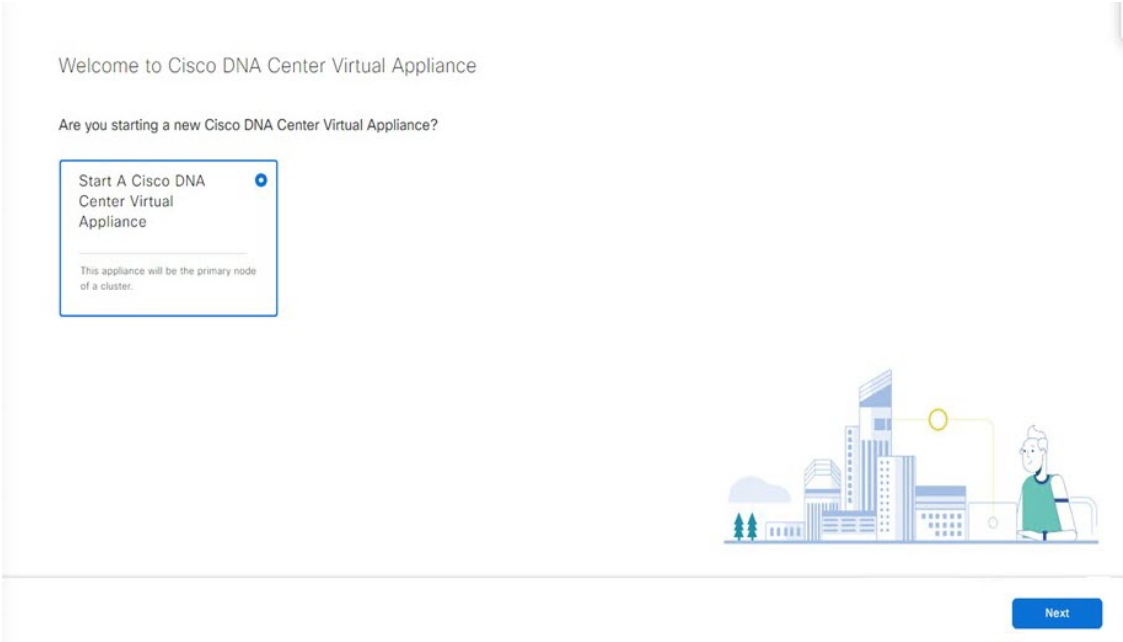
IPv6 Mode check box	IPv6 is supported. However, if you want to deploy IPv4, leave this check box unchecked.
IP Address field	Enter the static IPv6 address that you want to use.
Netmask field	Enter either a netmask or CIDR address for the IP address you specified in the previous field.
Default Gateway Address field	Specify the default gateway that will be used to route traffic.
Static Routes field	You can't specify static routes when using this wizard, so leave this field blank.



Note the URL listed in the **Web Installation** field. You'll need this for the next step.

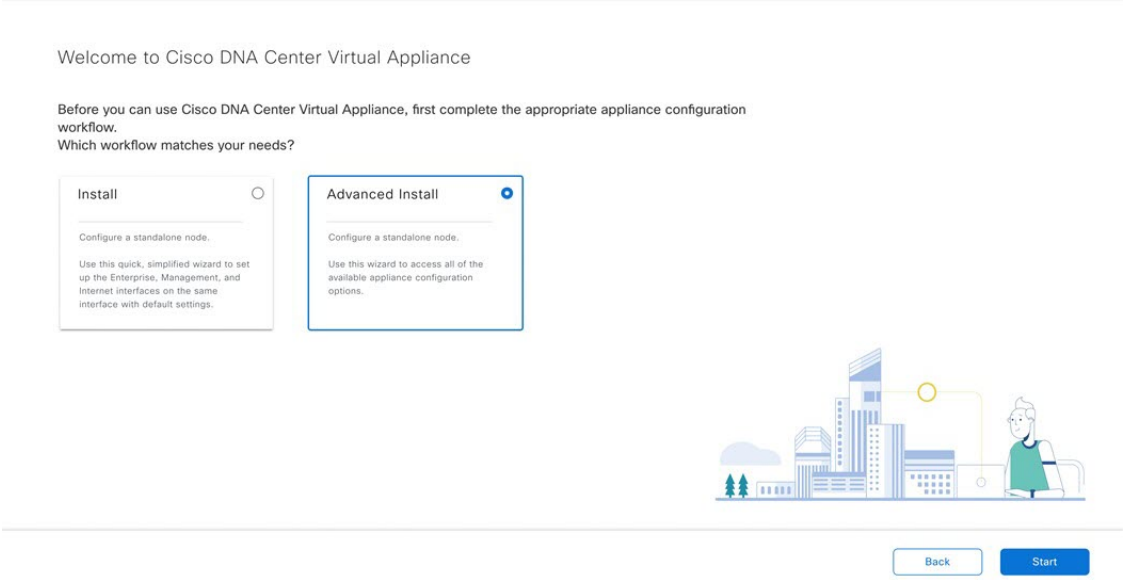
b) Open the URL that was displayed in the **Static IP Configuration** page.

c) Click the **Start a Catalyst Center Virtual Appliance** radio button, then click **Next**.



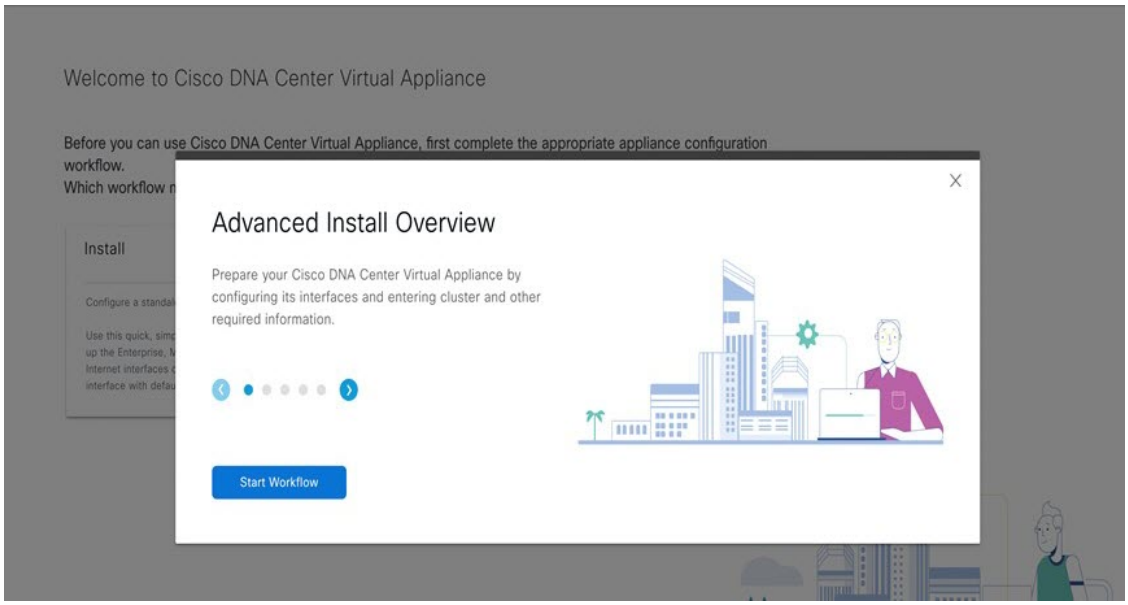
d) Click the **Advanced Install** radio button, then click **Start**.

The **Advanced Install Overview** slider opens. Click > to view a summary of the tasks that the wizard will help you complete.



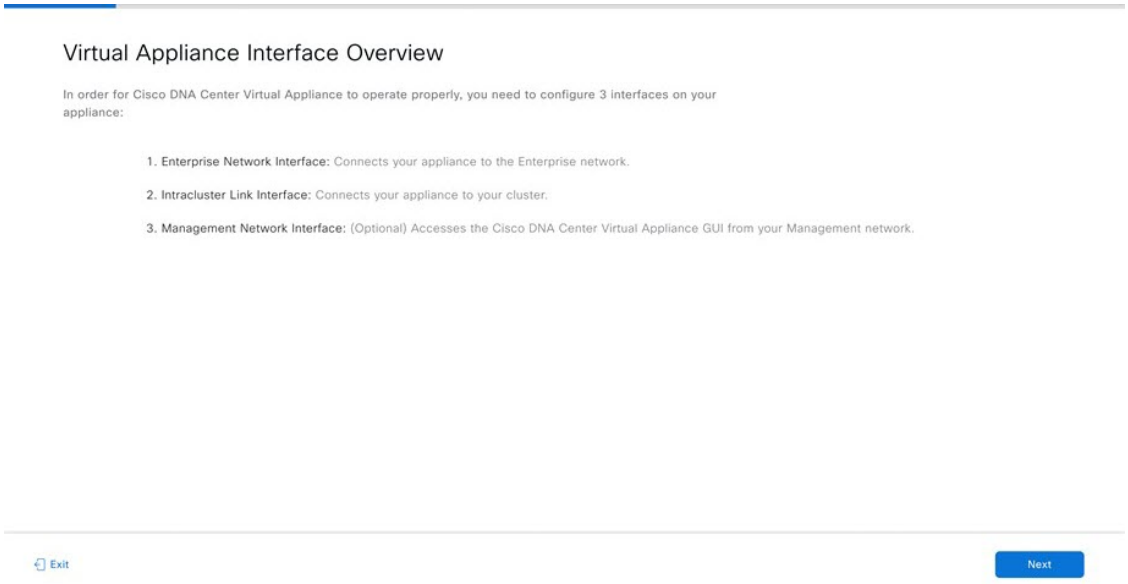
e) Click **Start Workflow** to start the wizard.

The **Virtual Appliance Interface Overview** page opens, providing a description of the four appliance interfaces that you can configure.

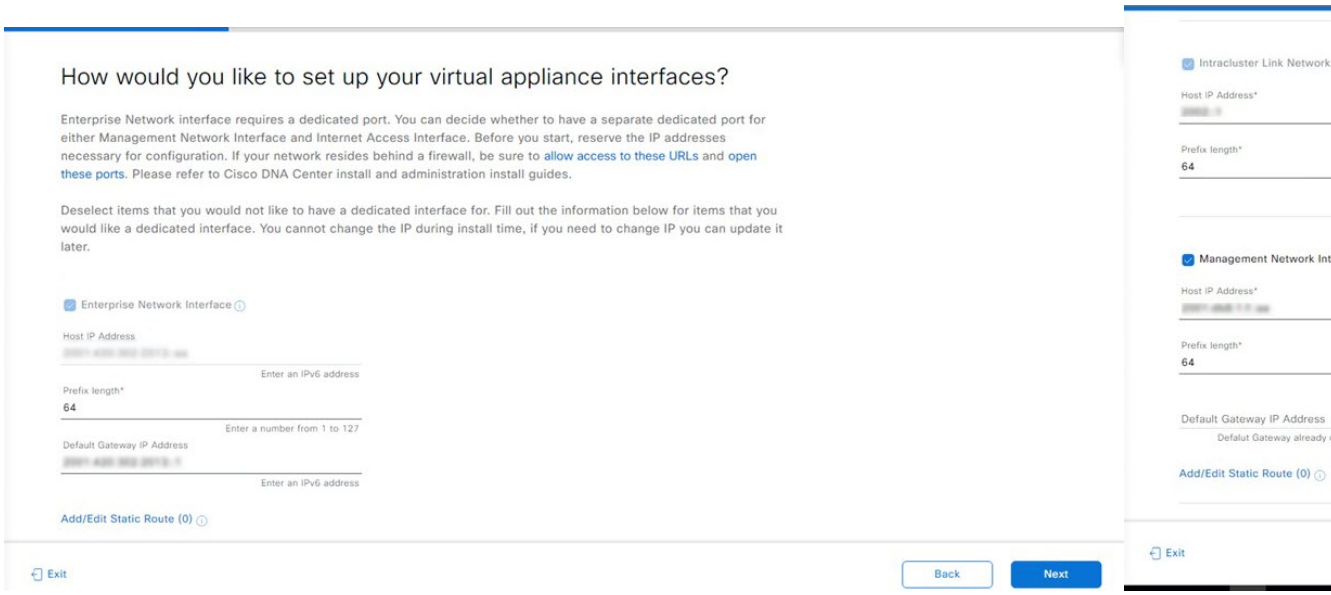


Step 4 Configure your virtual appliance by completing the Advanced Install Configuration wizard:

a) Click **Next**.



The **How would you like to set up your appliance interfaces?** page opens.



If your network resides behind a firewall, do the following:

- Click the **allow access to these URLs** link to view a pop-up window that lists the URLs that Catalyst Center on ESXi must be able to access.
- Click the **open these ports** link to view a pop-up window that lists the network service ports that must be available for Catalyst Center on ESXi to use.

By default, the **Enterprise Network Interface** check box is already checked. It's also prepopulated with the values you entered in the **STATIC IP CONFIGURATION** page.

b) Do the following for each appliance interface you want to use, then click **Next**:

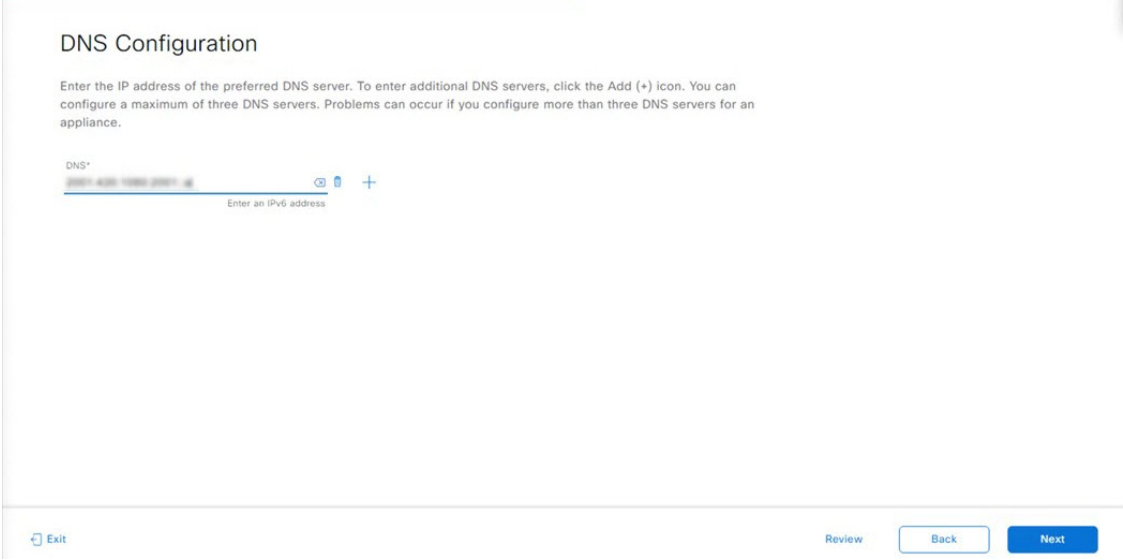
- Click its check box and enter the appropriate configuration values.
- If necessary, click its **Add/Edit Static Route** link to configure static routes. Click **+** as needed to configure additional routes. When you're done, click **Add**.

The **DNS Configuration** screen opens.

c) Enter the IP address of the preferred DNS server, then click **Next**. To enter additional DNS servers, click the **Add** (+) icon.

Important

- For each node in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
- For NTP, ensure port 123 (UDP) is open between Catalyst Center on ESXi and your NTP server.

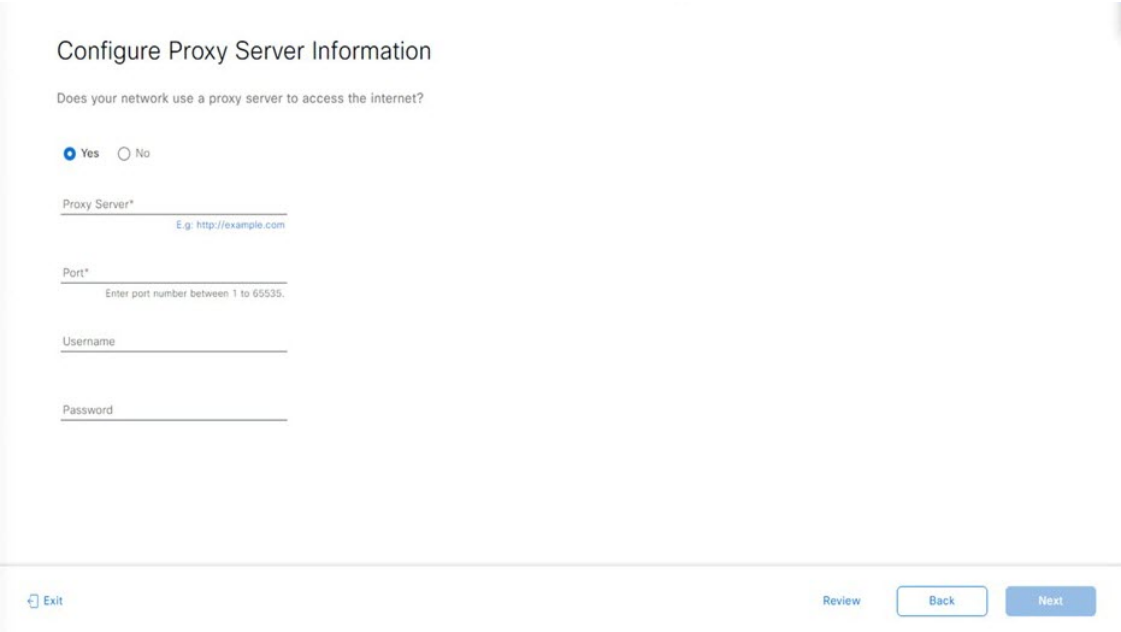


The **Configure Proxy Server Information** screen opens.

d) Do one of the following and then click **Next**:

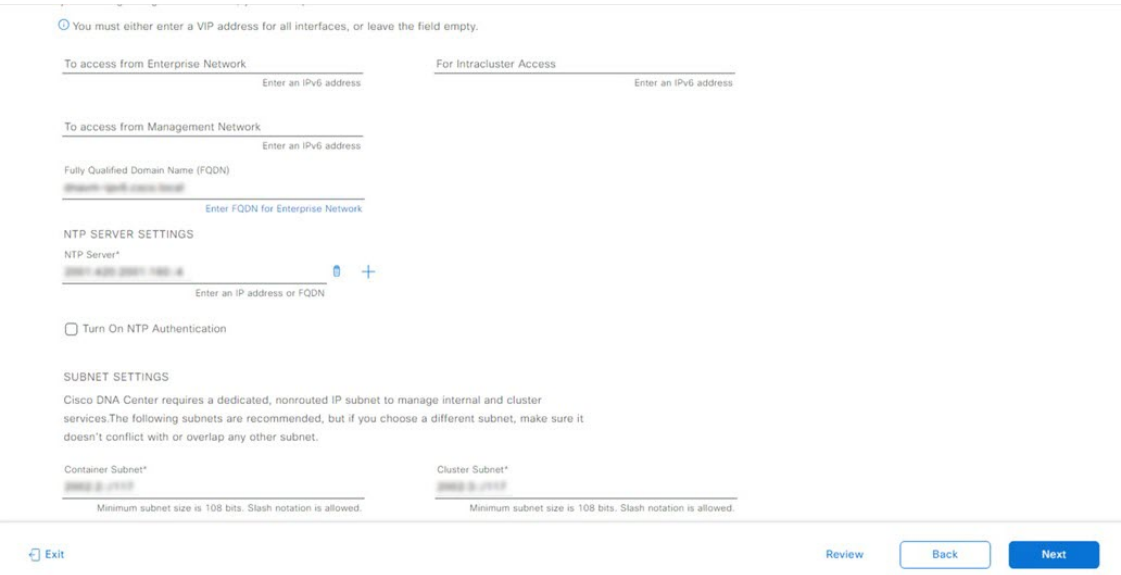
- If your network does *not* use a proxy server to access the internet, click the **No** radio button.
- If your network does use a proxy server to access the internet, enter the values described in the following table:

Proxy Server field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** Connection from Catalyst Center on ESXi to the HTTPS proxy is supported only via HTTP in this release.
Port field	Enter the port your appliance used to access the network proxy.
Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.



The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Advanced Appliance Settings** screen opens.

e) Enter configuration values for your appliance, then click **Next**.

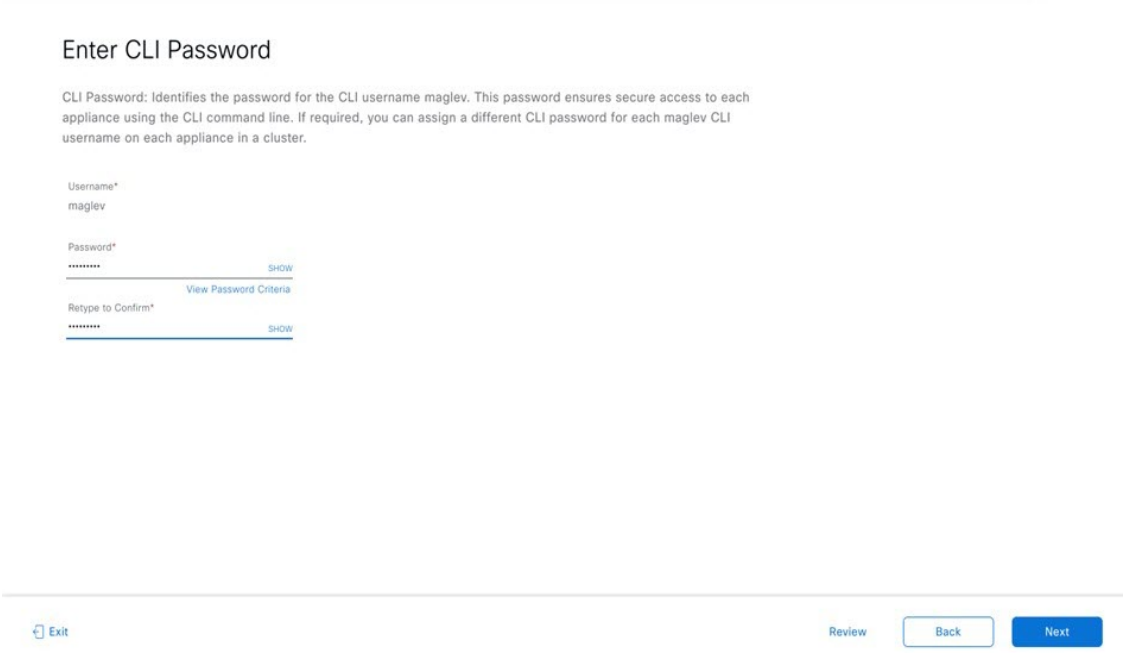


Cluster Virtual IP Addresses	
To access from Enterprise Network and For Intracluster Access fields	Enter the virtual IP address configured for the Enterprise interface. If you configured a virtual IP address for the Management interface, enter this address as well (using a comma to separate the two IP addresses).

Fully Qualified Domain Name (FQDN) field	You can also specify the fully qualified domain name (FQDN) for your virtual appliance. Catalyst Center on ESXi uses this domain name to do the following: • It uses this hostname to access your virtual appliance's web interface and the Representational State Transfer (REST) APIs used by devices in the enterprise network that Catalyst Center on ESXi manages. • In the Subject Alternative Name (SAN) field of Catalyst Center on ESXi certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.
NTP Server Settings	
NTP Server field	Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the **Add** (+) icon. For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.
Turn On NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center on ESXi, check this check box and then enter the following information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file. **Note** Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.
Subnet Settings	
Container Subnet field	A dedicated, non-routed IPv6 subnet that Catalyst Center on ESXi uses to manage internal services. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Catalyst Center on ESXi internal network or an external network.
Cluster Subnet field	A dedicated, non-routed IP subnet that Catalyst Center on ESXi uses to manage internal cluster services. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Catalyst Center on ESXi internal network or an external network.

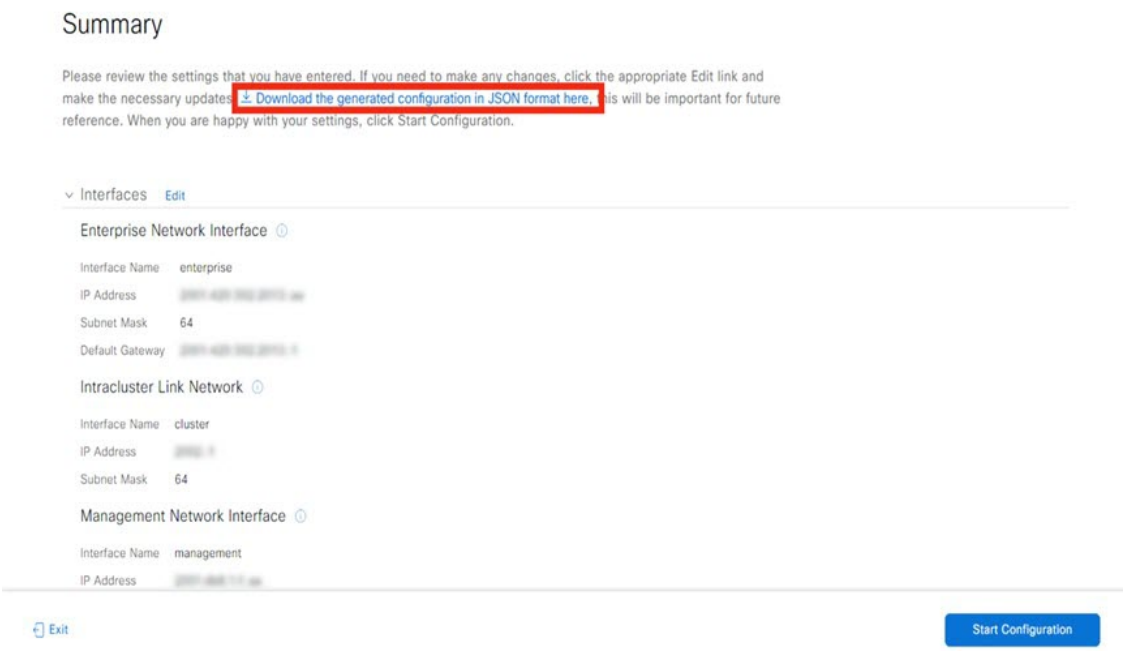
The **Enter CLI Password** page opens.

f) Enter and confirm the password for the `maglev` user, then click **Next**.



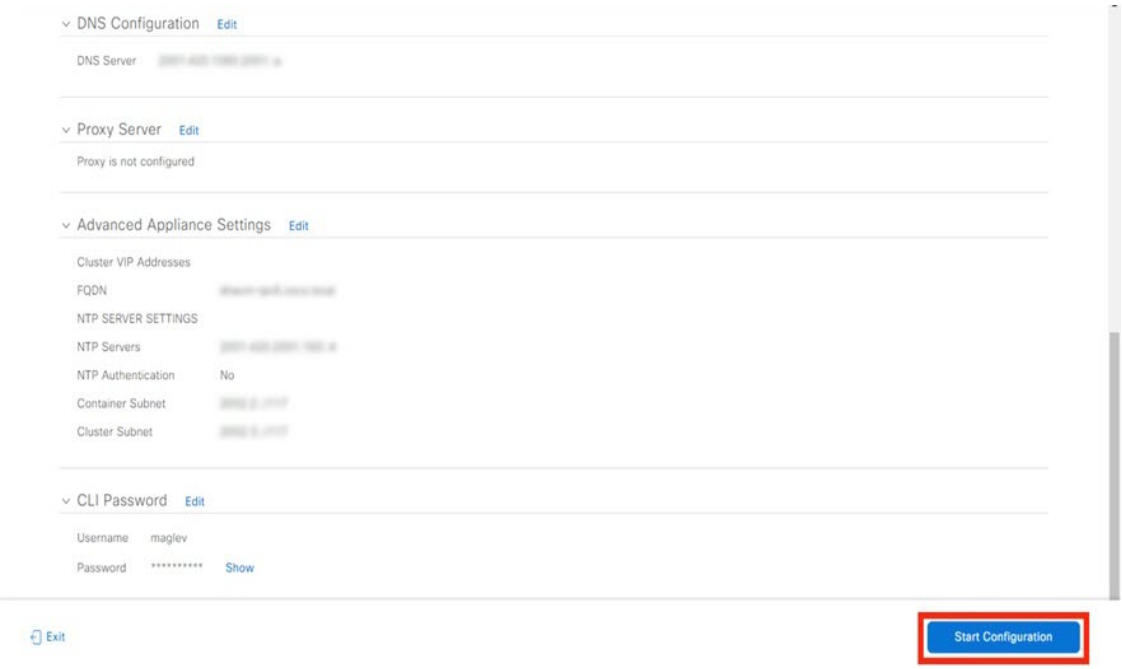
The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Summary** page opens.

Note To download the appliance configuration as a JSON file, click the corresponding link.



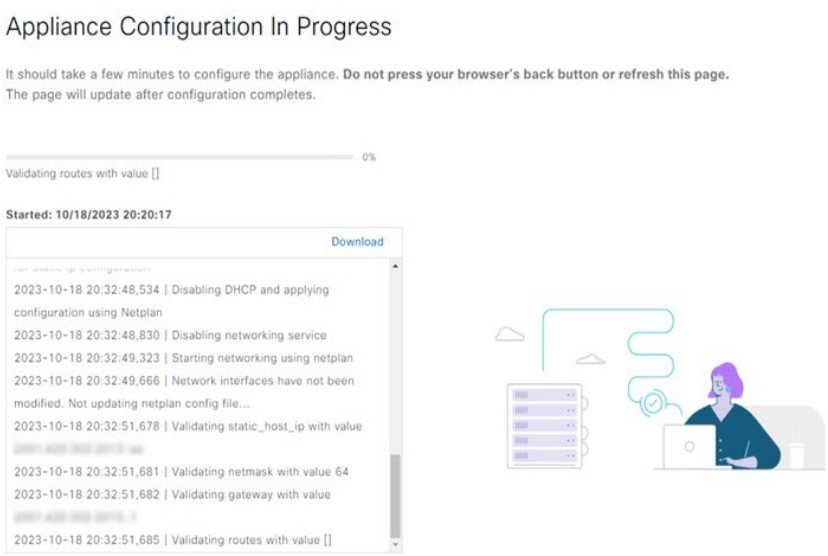
g) Scroll to the bottom of the screen and review all of the settings that you have entered while completing the wizard. If necessary, click the appropriate **Edit** link to open the wizard screen in which you want to make updates.

h) To complete the configuration of your Catalyst Center on ESXi virtual appliance, click **Start Configuration**.



The wizard screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred. To save a local copy of this information as a text file, click the **Download** link.

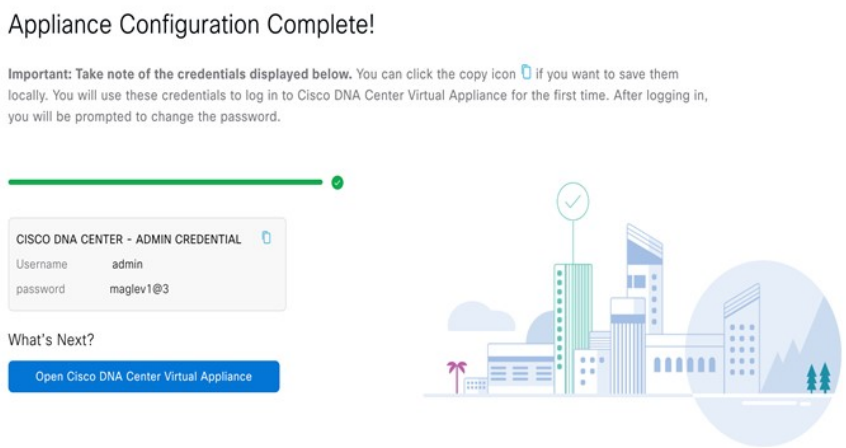
It takes around 180 to 210 minutes for the virtual machine to become operational. The actual time will depend on things like available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.



Step 5 After appliance configuration completes, click the copy icon to copy the default admin superuser password.

It can take from 15-30 mins for services to be stabilized before you can login to the UI.

Important Catalyst Center on ESXi automatically sets this password when you complete the Install configuration wizard. Ensure that you click the copy icon before you proceed. Otherwise, you will not be able to log in to Catalyst Center on ESXi for the first time.



Note As a security measure, you'll be prompted to change this password after you log in. For more information, see Complete the Quick Start Workflow, on page 106.

Configure a Virtual Appliance Using the Interactive CC VA Launcher

To configure a Catalyst Center on ESXi virtual appliance using the CC VA Launcher, complete the following procedure.

Procedure

Step 1 From the location specified by Cisco, download the Catalyst Center on ESXi OVA file.

Step 2 From the same URL, download the CC VA Launcher bundle (**DNAC-SW-Launcher-2.3.7.4-VA.tar.gz**) and extract it.

The bundle contains the following files:

- Launcher application: **dnac-esxi-launcher**
- Configuration file for single network interface controller (NIC) deployments: **config.json**
- Configuration file for dual network interface controller (NIC) deployments: **config_dual_nic.json**
- Logger configuration file: **log_config.json**
- License: **LICENSE**

Step 3 Start the CC VA Launcher in interactive mode by entering the command that's specific to your operating system:

- macOS: **./dnac-esxi-launcher**
- Microsoft Windows: **dnac-esxi-launcher.exe**

- Linux: **./dnac-esxi-launcher**

Step 4 Complete the CC VA Launcher:

a) For the host/vCenter server you want to deploy the virtual appliance on, enter its IP address, credentials, and SSL port number.

The launcher will verify connectivity with the host/vCenter server.

b) Enter the path to the Catalyst Center on ESXi OVA file.

If you're specifying a Microsoft Windows path, use "\\" as the delimiter. Your path should look similar to the following example: `C:\\Users\\dnac\\downloads\\esxi_10.ova`

c) Enter the name of the virtual machine you are going to create.

d) Choose the provisioning format the virtual disk will use, then press **Enter**.

The thick provisioned format is set by default, but both thin and thick provisioning formats are supported.

Note For NFS datastores, thick provisioning is supported only if the underlying storage vendor supports it. If not, the datastore's default provisioning format will be picked during import.

e) Choose one of the following discovery modes, then press **Enter**:

Note This step is not applicable to standalone ESXi hosts. Proceed to Step 4h.

- **Discover all the VMware Datacenters**: When selected, only the datacenters that you have access to and meet Catalyst Center on ESXi's memory, CPU reservation, and disk space requirements are listed.
- **List all available VMware Datacenters**: When selected, all available datacenters are listed.

f) Choose the datacenter you want to use, then press **Enter**.

The discovery time will vary, depending on network latency and the number of entities in the target environment (host/cluster/virtual machine/datastore).

g) If clusters or directly-attached hosts are available, you are prompted to choose the corresponding deployment target option:

- If you choose the cluster option, suitable clusters and their unreserved resources are listed. Specify the cluster you want to use and proceed to Step 4h.

  Note A warning message is displayed if the cluster you chose does not have vSphere HA enabled, as well as the cluster's Distributed Resource Scheduler (DRS) status.

- If you choose the directly-attached hosts option (or choose the cluster option and DRS is disabled), suitable hosts are listed. Specify the host you want to use and proceed to Step 4h.

  Note If DRS is enabled and a resource pool is found, you are prompted to confirm the resource pool's use in your deployment.

h) The suitable datastores that are available, based on the disk provisioning format you chose previously, are listed. Specify the datastore you want to use.

Note For NFS datastores, thick provisioning is supported only if the underlying storage vendor supports it. If not, the datastore's default provision will be picked during import.

i) Enter either **y** or **n** to specify whether you want to configure the virtual appliance's Management interface.

A list of available networks is displayed.

j) Choose the network you want to use for the appliance's Enterprise interface.

If you chose **y** in the previous step, you'll also need to choose the network you want to use for the appliance's Management interface.

k) Enter the IP address and subnet mask for the Enterprise interface:

- If you opted to configure only the Enterprise interface (by entering **n** in Step 4i), enter the IP address of the gateway to be used by the Enterprise interface.
- If you entered **y** in Step 4i, enter **y** and then configure the default gateway that the Enterprise interface will use.

Note The default gateway can be configured only for one of the appliance's interfaces. If you want to configure the default gateway on the Management interface, enter **n**.

l) Enter **y** or **n** to specify whether you want to configure static routes for the Enterprise interface.

If you enter **y**, enter the number of static routes you want to set up. Also enter each route in the following format: *<network>/<netmask>/<gateway>*.

m) If you opted to configure the appliance's Management interface (by entering **y** in Step 4i), enter its IP address and subnet mask.

n) If you entered **n** in Step 4k, enter the default gateway that the Management interface will use.

o) Enter **y** or **n** to specify whether you want to configure static routes for the Management interface.

If you enter **y**, enter the number of static routes you want to set up. Also enter each route in the following format: *<network>/<netmask>/<gateway>*.

p) Enter **y** or **n** to specify whether you want to configure a proxy server.

Note Only HTTP proxies are supported.

q) If you entered **y** in the previous step, specify whether authentication has been enabled for your proxy server by entering **y** or **n**.

r) If you entered **y** in the previous step, enter your proxy server's login credentials.

s) Enter the number of DNS servers you want to configure.

You must configure at least one server and can configure a maximum of three. If prompted, enter the IP address for the DNS servers you want to configure.

t) Enter the number of NTP servers you want to configure.

You must configure at least one server and can configure a maximum of three. If prompted, enter the IP address for the NTP servers you want to configure.

u) Specify whether you want to configure a fully qualified domain name (FQDN) by entering **y** or **n**.

If you enter **y**, enter the appropriate FQDN.

Note Except for hyphens (-), the FQDN should not contain any special characters.

v) Enter and then confirm the Maglev password. The password is used to access the shell and grant SSH access.

The password must meet the following requirements:

- Minimum length of eight characters.
- Cannot contain a tab or a line break.
- Contains characters from at least three of the following categories:
  - Uppercase letters (A–Z)
  - Lowercase letters (a–z)
  - Numbers (0–9)
  - Special characters (for example, ! or #)

A summary of the settings you just entered are displayed.

w) Start the deployment and configuration process by entering **y**.

The launcher completes the following tasks:

1. Imports the OVA file.
2. Adds the interface to the virtual machine if you have opted to configure the Management interface.
3. Applies the Catalyst Center on ESXi network configuration to the virtual machine.
4. Checks whether the **Enable Storage I/O Control and statistics collection** option has been enabled and displays a message if it hasn't.
5. Powers on the deployed virtual machine.

Note The time necessary to complete deployment depends on the available network bandwidth and datastore throughput.

Step 5 After the Catalyst Center on ESXi virtual appliance powers on, log in to the host/vCenter server you deployed and open the virtual appliance's VMWare console.

A terminal shell opens after the virtual appliance boots up, which can take up to 60 minutes.

Step 6 Log in, using the same Maglev password you entered in Step 4v.

The default username is **maglev**.

Step 7 When all of the Catalyst Center on ESXi services are up, open a supported browser and type in the IP address you entered for the Enterprise interface in Step 4k. If you configured the Management interface, enter the IP address you entered for it in Step 4m.

Step 8 When prompted by the Catalyst Center on ESXi GUI, enter the default credentials (**admin/maglev1@3**) to log in.

Configuration File Parameters

The following table describes the parameters you need to enter values for in the config.json file.

Note For optional parameters you are not using, enter an empty string ("). For example, if you don't want to specify an FQDN for the virtual appliance, its entry would look like this: `"fqdn": ""`

Category	Configuration Parameter	Description
Host/vCenter information (host_info)	ip (ip)[1]	IP address or FQDN of the vCenter or standalone ESXi host that the OVA will be imported to. **Note** You cannot specify a host that's managed by vCenter.
	SSL Port (ssl_port)[1]	Port that HTTPS is configured for on the vCenter or ESXi host. The default port is 443.
Import configuration (import_info)	OVA file path (ova_path) [1]	Directory where the Catalyst Center on ESXi OVA file was downloaded to. **Note** If you're specifying a Microsoft Windows path, use "\\" as the delimiter. Your path should look similar to the following example: `C:\\Users\\dnac\\downloads\\esxi_10.ova`
	VM Name (vm_name) [1]	Name of the VM.
	Datacenter (data_center) [2]	Name of the datacenter the virtual appliance OVA file will be imported to. This parameter is not applicable to standalone ESXi host deployments.
	Cluster Name (cluster) [3]	Name of the cluster where the virtual machine will reside.
	Resource Pool (resource_pool)[3]	Resource pool in which the imported VM should be placed. This parameter is not applicable to ESXi host deployments.
	Host Name (host_name)[2]	The ESXi host (managed by vCenter) in which the VM should be placed. This parameter is not applicable to standalone ESXi host deployments.
	Datastore (datastore)[1]	Name of the datastore where the VMDK and other supporting files should be placed.
	Disk Provision (disk_provision)[1]	The virtual disk's provisioning format. The thick provisioned format is set by default, but both thin and thick provisioning formats are supported.
	Enterprise Network (network: enterprise_network)[1]	Name of the host network that will be mapped to the virtual machine's Enterprise network.
	Management Network (network: management_network)[4]	Name of the host network that will be mapped to the virtual machine's Management network, which is used to access Catalyst Center on ESXi's GUI.(Optional)

Category	Configuration Parameter	Description
Catalyst Center on ESXi configuration information (dnac_info)	IP Address (address)[1]	IP address of the virtual appliance's Enterprise network interface.
	Subnet mask (netmask) [1]	Subnet mask for the virtual appliance's Enterprise network interface.
	Gateway (gateway)[1],[5]	IP address of the Enterprise network interface's gateway.
	Routes (routes)[5]	Static routes for the Enterprise interface. Enter routes in the following format: *<network-IP-address>/<netmask>/<gateway-IP-address>*. If you're specifying multiple routes, separate them with a comma (,).
	IP Address (address)[4]	IP address of the virtual appliance's Management interface.
	Subnet mask (netmask) [4]	Subnet mask for the virtual appliance's Management network interface.
	Gateway (gateway)[1],[5]	IP address of the Management network interface's gateway.
	Routes (routes)[5]	Static routes for the Management interface. Enter routes in the following format: *<network-IP-address>/<netmask>/<gateway-IP-address>*. If you're specifying multiple routes, separate them with a comma (,).
	DNS servers (dns_servers)[1]	DNS servers used by the virtual appliance. Specify at least one server. You can specify a maximum of three servers, separated by commas.
	HTTP Proxy (http_proxy)[6]	HTTP proxy the virtual appliance will use. When specifying the proxy, use the following format: http://*IP-address-or-FQDN*:*port-number* **Note** Keep the the proxy's username and password handy if authentication has been enabled.
	NTP server (ntp)[1]	NTP servers used by the virtual appliance. Specify at least one server. You can specify a maximum of three servers, separated by commas.
	FQDN (fqdn)[6]	Fully qualified domain name to be configured for the virtual appliance. Aside from hyphens, this name should not contain any special characters.

[1] Mandatory parameter
[2] Mandatory parameter that's applicable only to vCenter Server
[3] Optional parameter that's applicable only to vCenter, and not stand-alone ESXi hosts
[4] Mandatory parameter applicable only to dual NIC deployments
[5] Optional parameter applicable only to dual NIC deployments
[6] Optional parameter

Configure a Virtual Appliance Using the CC VA Launcher in Silent Mode

The CC VA Launcher's Silent mode allows you to deploy a Catalyst Center on ESXi virtual appliance using the settings specified in the config.json configuration file. This mode is useful when you want to integrate the launcher in your deployment automation workflow. To configure a virtual appliance using the launcher's silent mode, complete the following procedure.

Procedure

Step 1 From the location specified by Cisco, download the Catalyst Center on ESXi OVA file.

Step 2 From the same URL, download the launcher bundle (**DNAC-SW-Launcher-2.3.7.4-VA.tar.gz**) and extract it.

The bundle contains the following files:

- Launcher application: **dnac-esxi-launcher**
- Configuration file you need to update if you're only configuring the Enterprise interface: **config.json**
- Configuration file you need to update if you're configuring both the Enterprise and Management interfaces: **config_dual_nic.json**
- Logger configuration file: **log_config.json**
- License: **LICENSE**

Step 3 Navigate to the directory where the CC VA Launcher bundle files were extracted and open the configuration file in a text editor.

- For single NIC deployments, where you only want to configure the appliance's Enterprise interface, open **config.json**.
- For dual NIC deployments, where you want to configure the appliance's Enterprise and Management interfaces, open **config_dual_nic.json**.

Step 4 For the parameters provided in the configuration file, enter the values specific to your deployment.

See Configuration File Parameters, on page 102 for more information.

Note For optional parameters you are not using, enter an empty string ("""). For example, if you don't want to specify an FQDN for the virtual appliance, its entry would look like this: `"fqdn": ""`

Step 5 Run the CC VA Launcher using the values you specified in the configuration file:

a. If necessary, navigate back to the directory where the launcher bundle files were extracted.

b. Enter the command that's specific to your operating system:

- macOS: **./dnac-esxi-launcher config.json -c** *configuration-filename* **-u** *vCenter-or-host-username* **-p** *vCenter-or-host-password* **-l** *Maglev-password* **--proxy_user** *proxy-username* **--proxy_password** *proxy-password*
- Microsoft Windows: **dnac-esxi-launcher.exe config.json -c** *configuration-filename* **-u** *vCenter-or-host-username* **-p** *vCenter-or-host-password* **-l** *Maglev-password* **--proxy_user** *proxy-username* **--proxy_password** *proxy-password*
- Linux: **./dnac-esxi-launcher config.json -c** *configuration-filename* **-u** *vCenter-or-host-username* **-p** *vCenter-or-host-password* **-l** *Maglev-password* **--proxy_user** *proxy-username* **--proxy_password** *proxy-password*

Note

- If the host/vCenter server is installed with self-signed certificate, enter the following command instead to skip SSL certificate validation: **./dnac-esxi-launcher config.json -d -u** *vCenter-or-host-username* **-p** *vCenter-or-host-password* **-l** *Maglev-password* (single NIC deployment) or **./dnac-esxi-launcher config_dual_nic.json -d -u** *vCenter-or-host-username* **-p** *vCenter-or-host-password* **-l** *Maglev-password* (dual NIC deployment)
- The **--proxy_user** and **--proxy_password** parameters are optional and only need to be entered if an authentication-based proxy is being used.

The CC VA Launcher completes the following tasks after it starts:

- Verifies connectivity with the host/vCenter server.
- Validates the target environment and configuration parameters.
- Displays a configuration summary after successful validation.
- Imports the OVA file.
- If you opted to configure the Management interface, the launcher adds this interface to the imported virtual machine.
- Applies the Catalyst Center on ESXi network configuration to the virtual machine.
- Checks whether the **Enable Storage I/O Control and statistics collection** option has been enabled and displays a message if it hasn't.
- Powers on the deployed virtual machine.

The deployment time will vary, depending on the available network bandwidth and target datastore's throughput.

Step 6 After the virtual appliance powers on, enter the host/vCenter server's credentials to open the appliance's VMware console.

It can take up to an hour for the a terminal shell to open.

Step 7 Log in, using **maglev** as the username and the password you specified in Step 5.

Step 8 After all of the Catalyst Center on ESXi services come up, use a supported browser to open the IP address you specified for the Enterprise interface in the configuration file.

Step 9 Log in, using **admin** as the username and **maglev1@3** as the password.

Complete the Quick Start Workflow

After you have deployed and configured a Catalyst Center on ESXi virtual appliance, you can log in to its GUI. Use a compatible, HTTPS-enabled browser when accessing Catalyst Center on ESXi.

When you log in for the first time as the admin superuser (with the username `admin` and the SUPER-ADMIN-ROLE assigned), the Quick Start workflow automatically starts. Complete this workflow to discover the devices that Catalyst Center on ESXi will manage and enable the collection of telemetry from those devices.

Before you begin

To log in to Catalyst Center on ESXi and complete the Quick Start workflow, you will need:

- If you completed the Advanced Install configuration wizard, the *admin* superuser username and password that you specified.

- The information described in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide's* "Required First-Time Setup Information" topic.

Procedure

Step 1 Do one of the following:

- If you completed either of the Maglev Configuration wizards, access the Catalyst Center on ESXi GUI by using **`HTTPS://`** and the IP address of the Catalyst Center on ESXi GUI that was displayed at the end of the configuration process.
- If you completed either of the browser-based configuration wizards, click **Open Catalyst Center Virtual Appliance** on the wizard's last page.

One of the following messages appears (depending on the browser you are using):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

Step 2 Ignore the message and click **Advanced**.

One of the following messages appears:

- Google Chrome:

```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted
 by your computer's
 operating system. This may be caused by a misconfiguration or an attacker intercepting your
connection.
```

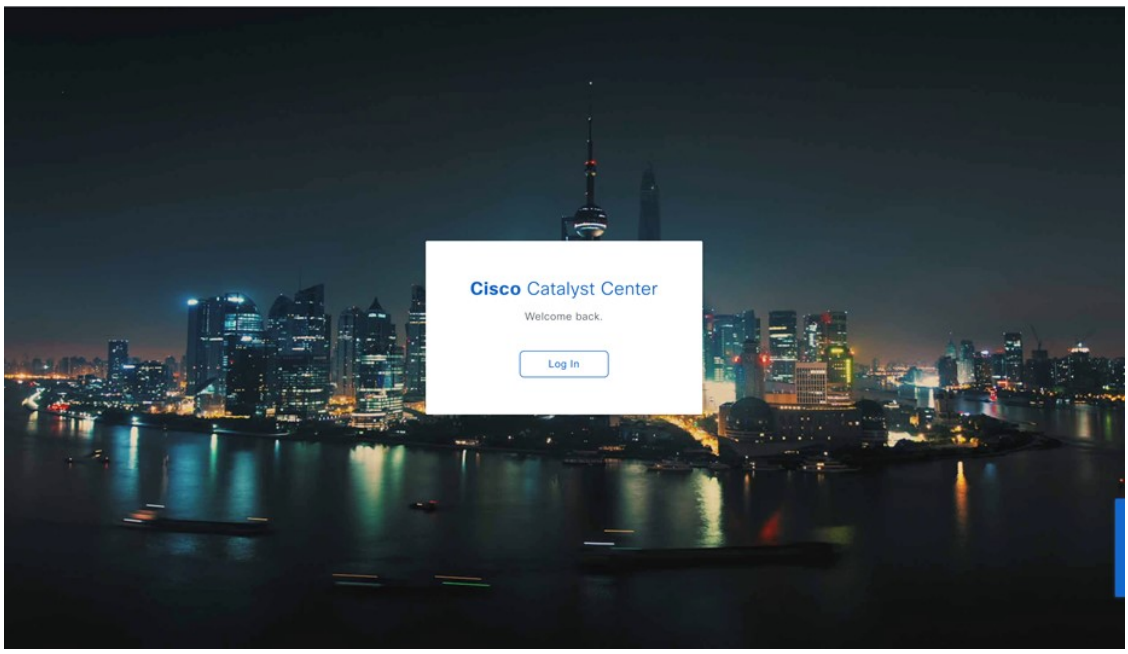
- Mozilla Firefox:

```
Someone could be trying to impersonate the site and you should not continue.
Websites prove their identity via certificates.
Firefox does not trust GUI-IP-address because its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate
certificates.
```

These messages appear because the controller uses a self-signed certificate. For information on how Catalyst Center on ESXi uses certificates, see the "Certificate and Private Key Support" section in the *Cisco Catalyst Center Administrator Guide*.

Step 3 Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to** *GUI-IP-address* **(unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.



Step 4 Click **Log In**.

The Catalyst Center on ESXi login screen appears.

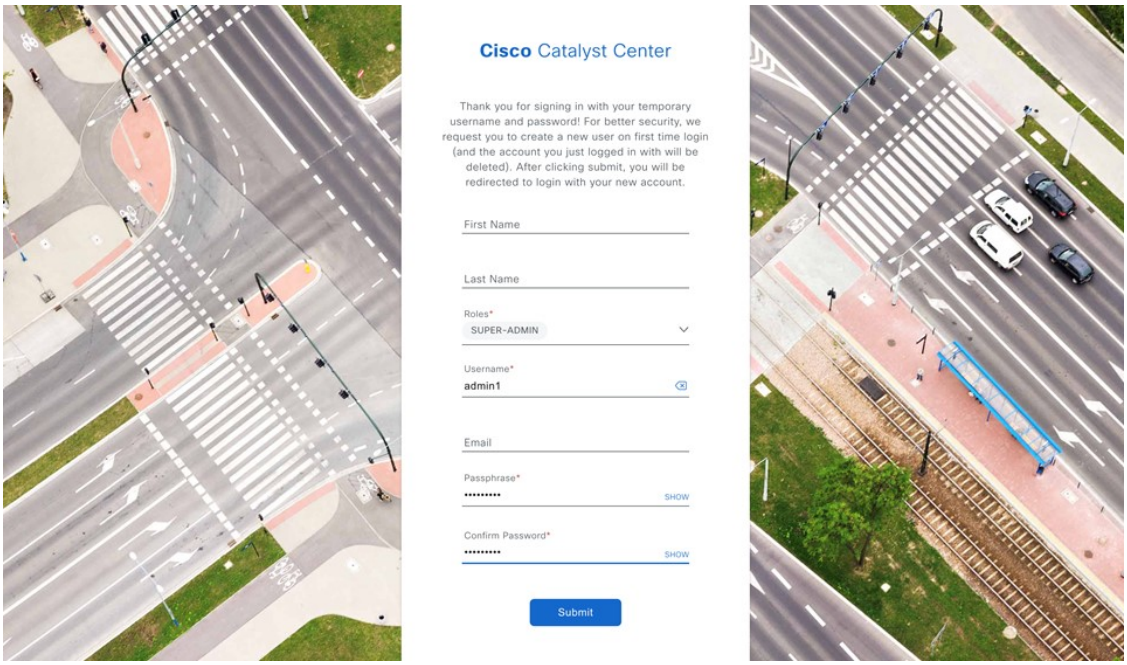
Step 5 Do one of the following and then click **Login**:

- If you completed either of the Maglev configuration wizards or the browser-based Install configuration wizard, enter the admin's username (**admin**) and password (**maglev1@3**).
- If you completed the browser-based Advanced Install configuration wizard, enter the admin's username (**admin**) and password that you set when you configured your Catalyst Center on ESXi appliance.

In the next screen, you are prompted to configure a new admin user (as the default credentials used to log in for the first time will be deleted).

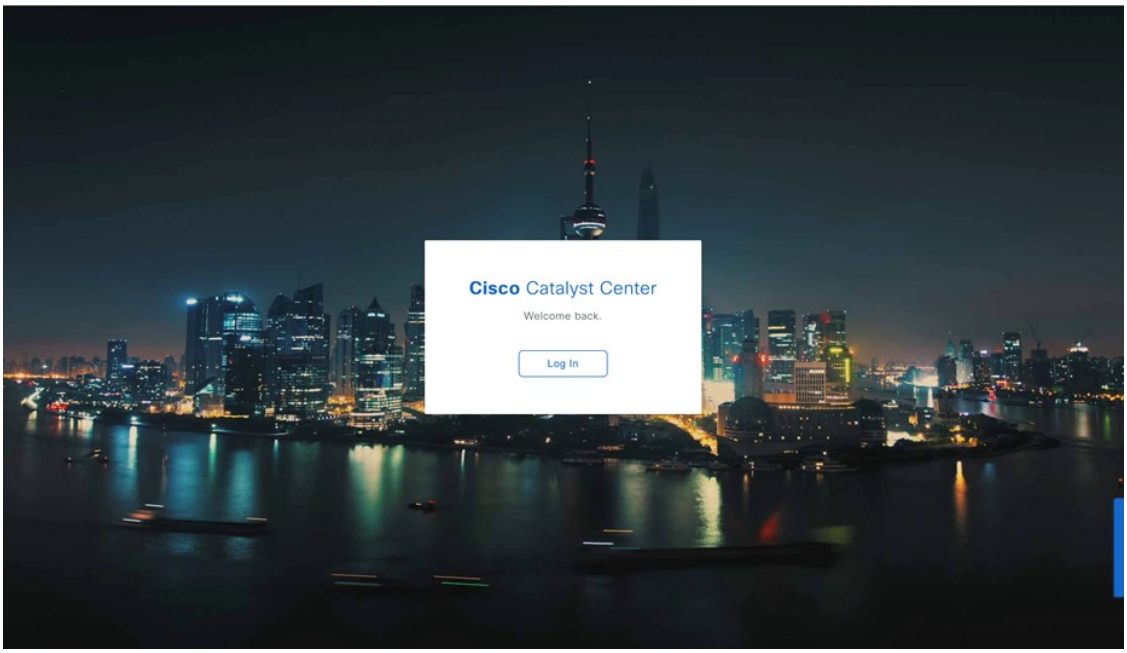
Step 6 Do the following in the resulting dialog box, then click **Submit**.

- In the **Roles** drop-down list, ensure that the `SUPER-ADMIN` user role is selected.
- Enter the new admin user's username.
- Enter and then confirm the new admin user's password.

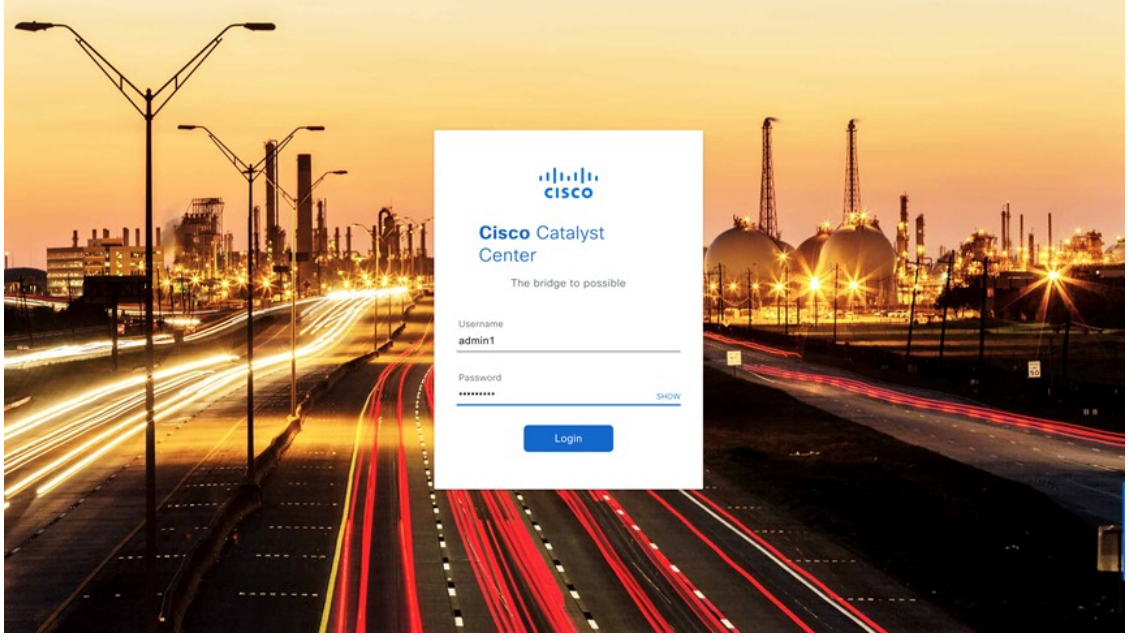


Step 7 Click **Log In**.

The Catalyst Center on ESXi login screen appears.



Step 8 Enter the username and password you configured for the new admin user, then click **Login**.



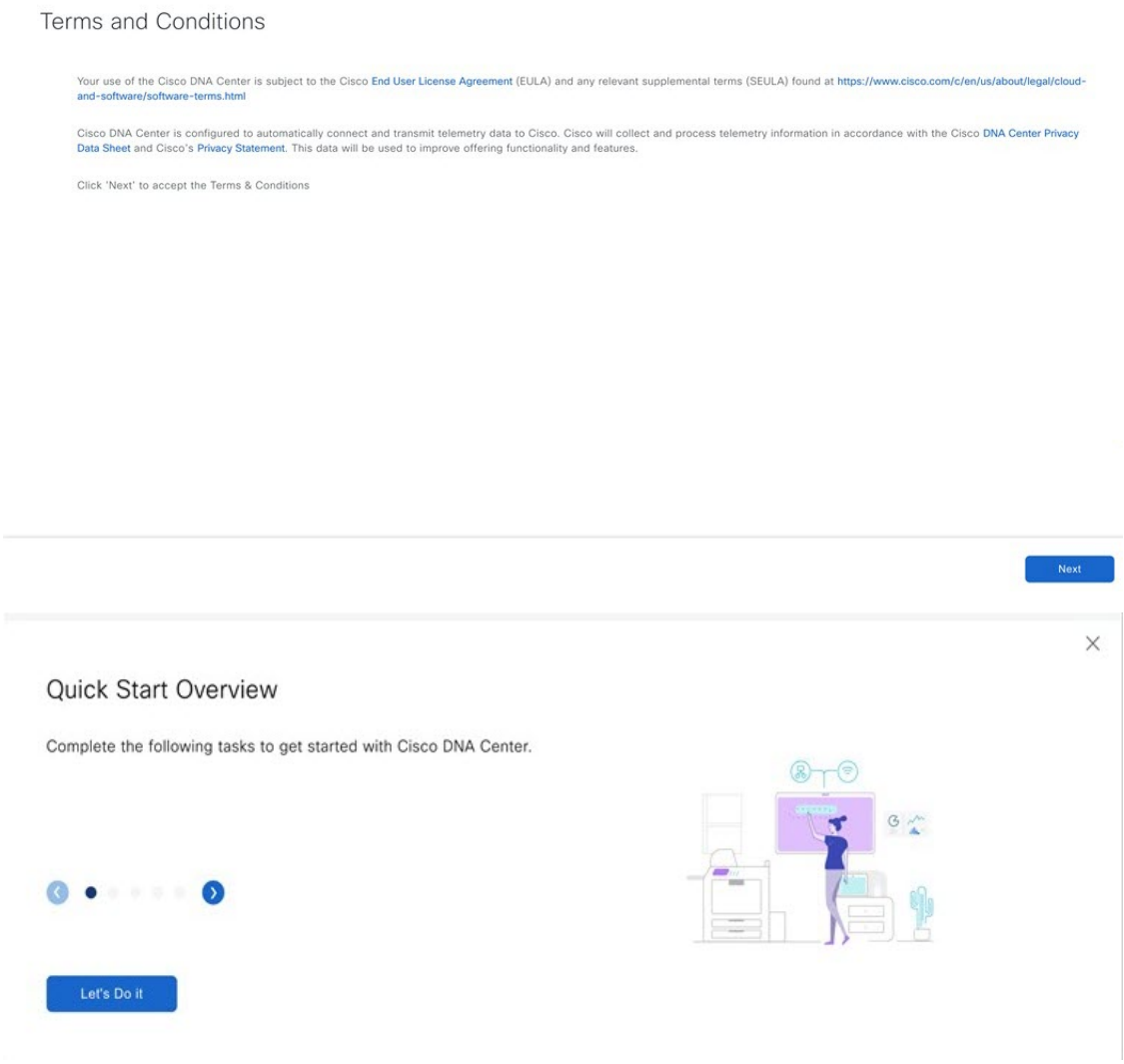
Step 9 Enter your cisco.com username and password (which are used to register software downloads and receive system communications) and then click **Next**.

Note If you don't want to enter these credentials at this time, click **Skip** instead.

The **Terms & Conditions** screen opens, providing links to the software End User License Agreement (EULA) and any supplemental terms that are currently available.

Step 10 After reviewing these documents, click **Next** to accept the EULA.

The **Quick Start Overview** slider opens. Click > to view a description of the tasks that the Quick Start workflow will help you complete in order to start using Catalyst Center on ESXi.



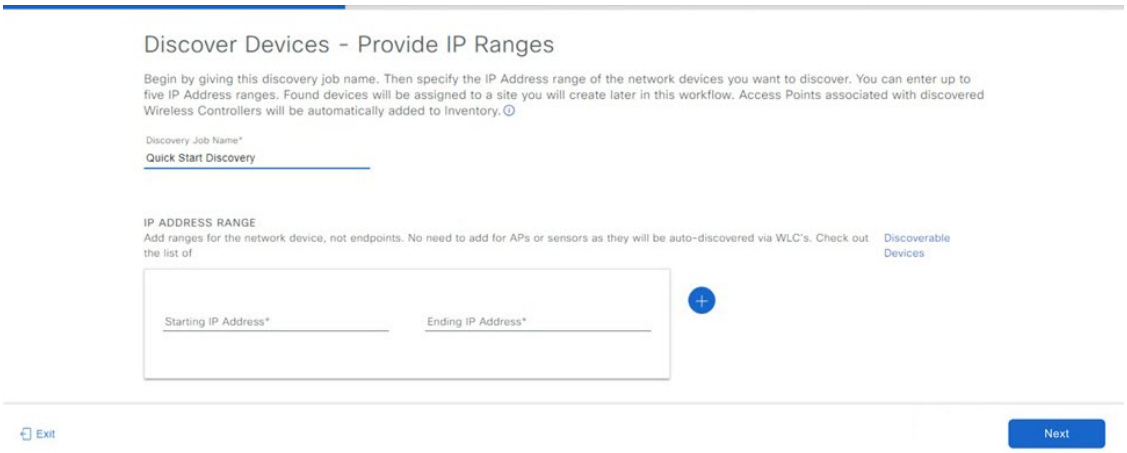
Step 11 Complete the Quick Start workflow:

a) Click **Let's Do it**.

b) In the **Discover Devices: Provide IP Ranges** page, enter the following information and then click **Next**:

- The name for the device discovery job.
- The IP address ranges of the devices you want to discover. Click + to enter additional ranges.
- Specify whether you want to designate your appliance's loopback address as its preferred management IP address. For more information, see the "Preferred Management IP Address" topic in the *Cisco Catalyst Center User Guide*.

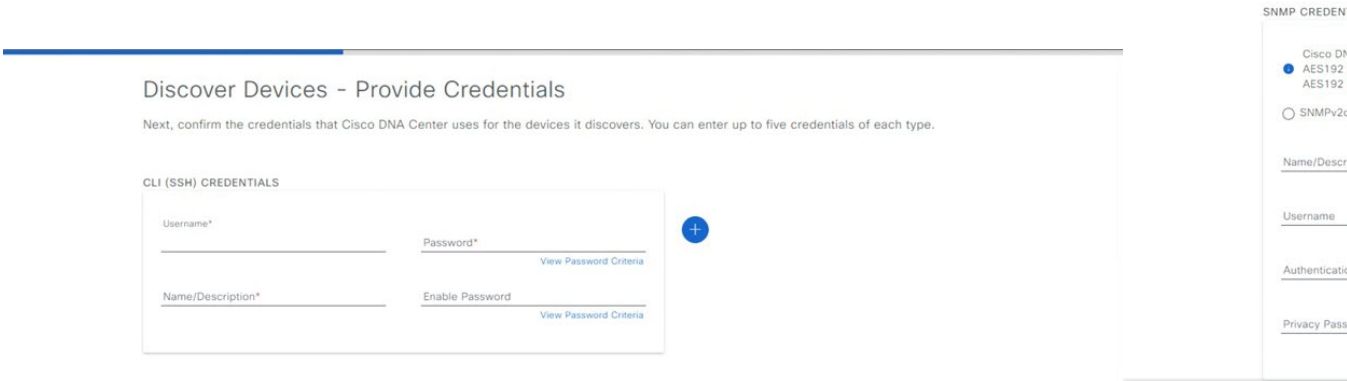
c) In the **Discover Devices: Provide Credentials** screen, enter the information described in the following table for the type of credentials you want to configure and then click **Next**:



GUI Components	Description
CLI (SSH) Credentials	
Username field	Username used to log in to the CLI of the devices in your network.
Password field	Password used to log in to the CLI of the devices in your network. The password you enter must be at least eight characters long.
Name/Description field	Name or description of the CLI credentials.
Enable Password field	Password used to enable a higher privilege level in the CLI. Configure this password only if your network devices require it.
SNMP Credentials	
SNMPv2c radio button	Click to use SNMPv2c credentials.
SNMPv3 radio button	Click to use SNMPv3 credentials.
SNMP Credentials: SNMPv2c	
SNMPv2c Type drop-down list	Choose either read or write community strings when SNMPv2c credentials are being used.
Name/Description field	Name or description of the SNMPv2c read or write community string.
Community String field	Read-only community string password used only to view SNMP information on the device.
SNMP Credentials: SNMPv3	
Name/Description field	Name or description of the SNMPv3 credentials.
Username field	Username associated with the SNMPv3 credentials.

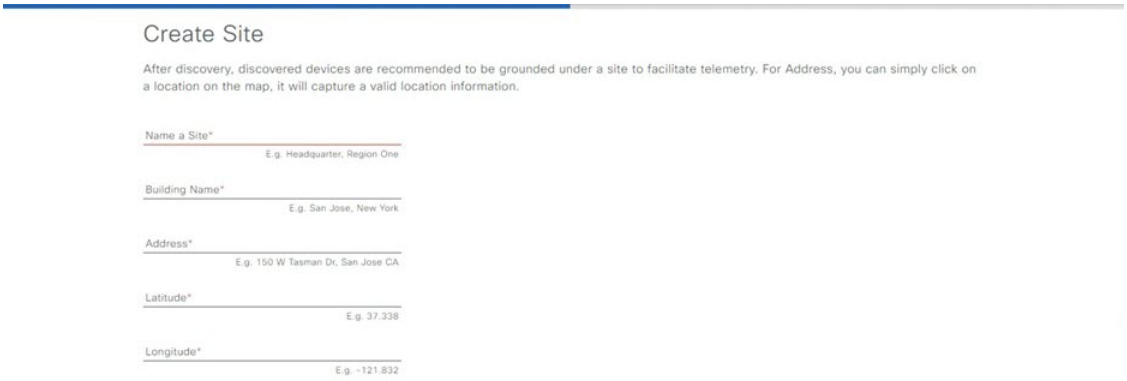
GUI Components	Description
Mode field	Security level that SNMP messages require: • **No Authentication, No Privacy** (noAuthnoPriv): Does not provide authentication or encryption. • **Authentication, No Privacy** (authNoPriv): Provides authentication, but does not provide encryption. • **Authentication and Privacy** (authPriv): Provides both authentication and encryption.
Authentication Password field	Password required to gain access to information from devices that use SNMPv3. The password must be at least eight characters in length. Note the following points: • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center on ESXi. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Authentication Type field	Hash-based Message Authentication Code (HMAC) type used when either **Authentication and Privacy** or **Authentication, No Privacy** is set as the authentication mode: • **SHA**: HMAC-SHA authentication. • **MD5**: HMAC-MD5 authentication.
Privacy Type field	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Choose one of the following privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **AES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **AES256**: 256-bit CBC mode AES for encryption on Cisco devices. **Note** • Privacy types AES192 and AES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

GUI Components	Description
Privacy Password field	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices supported with AES128, AES192, and AES256 encryption standards. Passwords (or passphrases) must be at least eight characters long. Note the following points: • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center on ESXi. • Passwords are encrypted for security reasons and are not displayed in the configuration.
NETCONF	
Port field	The NETCONF port that Catalyst Center on ESXi should use in order to discover wireless controllers that run Cisco IOS-XE.

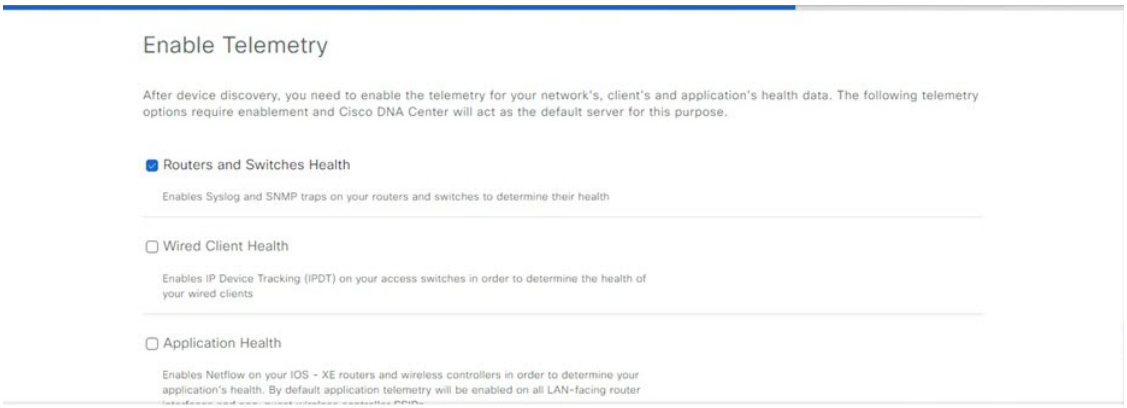


d) In the **Create Site** screen, group the devices you are going to discover into one site in order to facilitate telemetry and then click **Next**.

You can enter the site's information manually or click the location you want to use in the provided map.



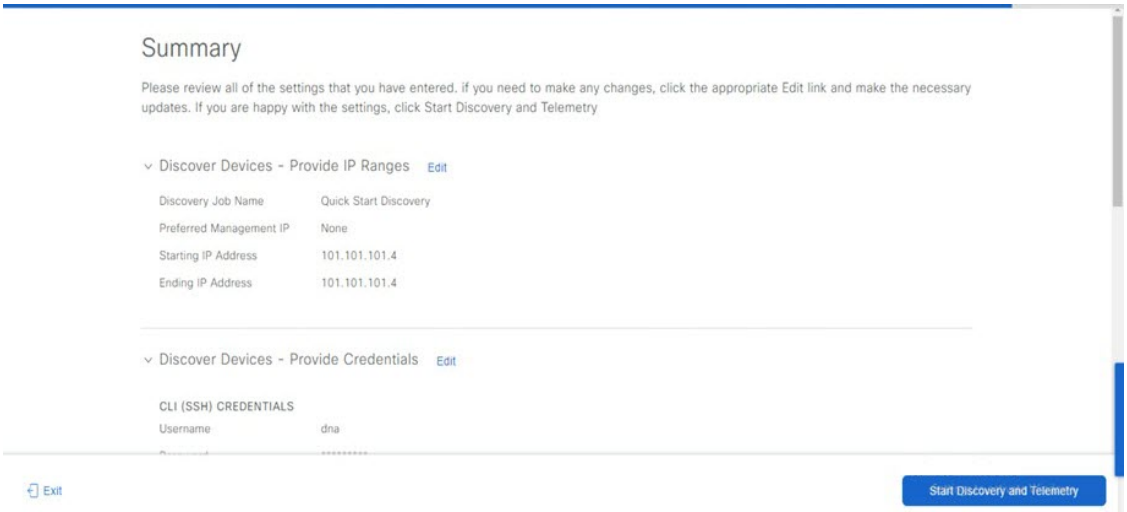
e) In the **Enable Telemetry** screen, check the network components that you want Catalyst Center on ESXi to collect telemetry for and then click **Next**.

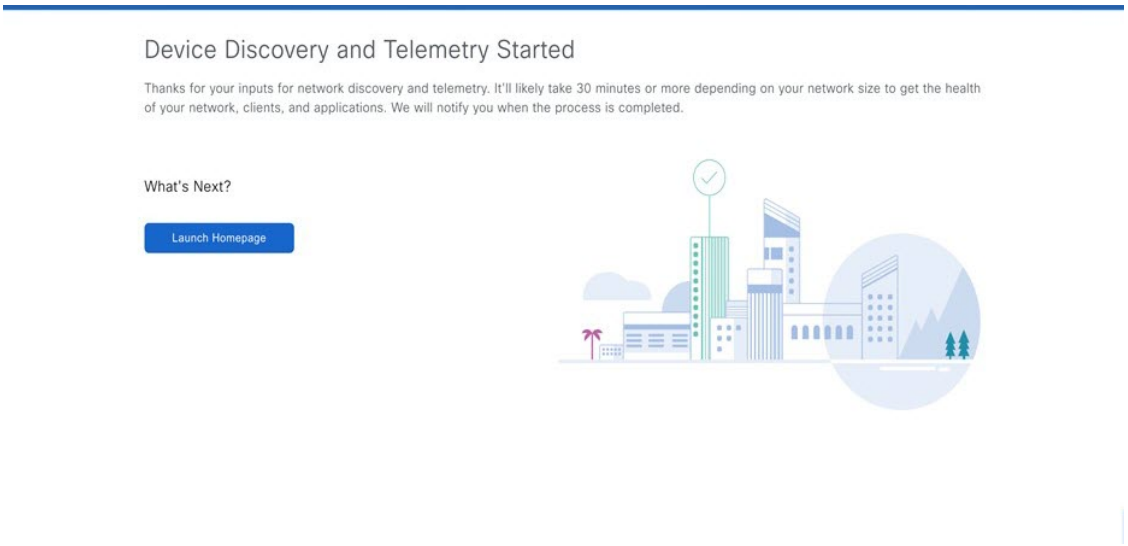


f) In the **Summary** screen, review the settings that you have entered and then do one of the following:

- If you want to make changes, click the appropriate **Edit** link to open the relevant screen.
- If you're happy with the settings, click **Start Discovery and Telemetry**. Catalyst Center on ESXi validates your settings to ensure that they will not result in any issues. After validation is complete, the screen updates.

  Catalyst Center on ESXi begins the process of discovering your network's devices and enabling telemetry for the network components you selected. The process will take a minimum of 30 minutes (more for larger networks).

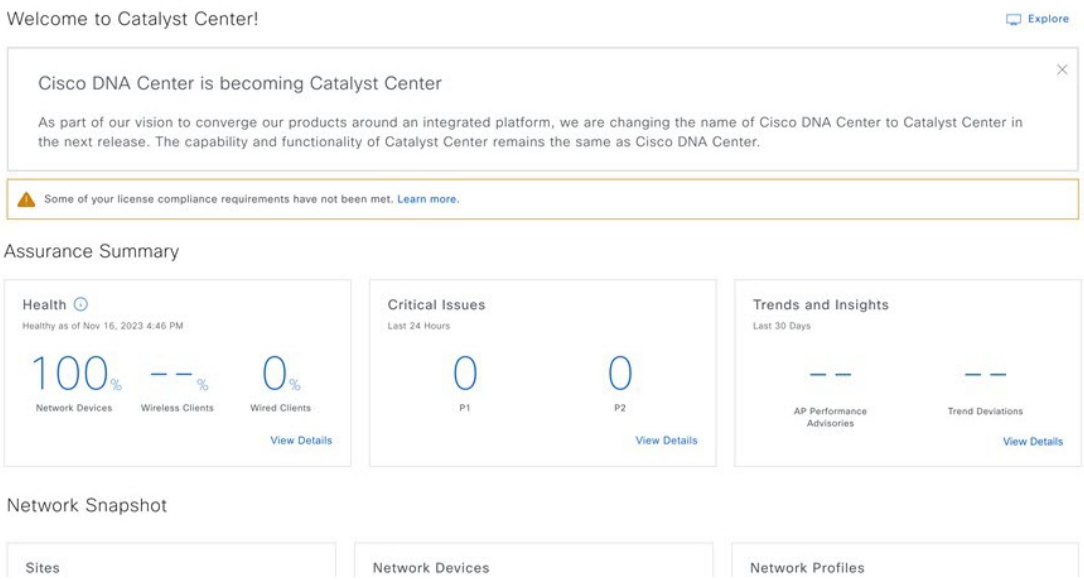




g) Click **Launch Homepage** to open the Catalyst Center on ESXi homepage.

From here, you can monitor the progress of device discovery and telemetry enablement. While these tasks are completing, do one or more of the following:

- To open the **Discoveries** page and confirm that the devices in your network have been discovered, click the menu icon and choose **Tools** > **Discovery**.
- To verify that the credentials you entered previously have been configured for your site, click the menu icon and choose **Design** > **Network Settings**. Then click the **Device Credentials** tab.
- To view any tasks (such as a weekly scan of the network for security advisories) that Catalyst Center on ESXi has already scheduled to run, click the menu icon and choose **Activities**. Then click the **Tasks** tab.
- To access guided workflows that will help you set up and maintain your network, click the menu icon and choose **Workflows**.



Postdeployment Configurations

After deploying a virtual appliance, you'll need to complete the following postdeployment tasks to run the appliance.

Enable VM Restart Priority

If VMware vSphere HA is enabled in your environment, complete the following procedure to ensure that the virtual appliance's VM is prioritized to power on first during an HA failover.

Procedure

Step 1 In the vSphere Client's navigation pane, click the HA cluster.

Step 2 Click the **Configure** tab.

Step 3 Choose **Configuration** > **VM Overides** and then click **Add**.

Step 4 Click the virtual machine you want to apply overrides to and then click **OK**.

Step 5 In the **vSphere HA** area's **VM Restart Priority** field, do the following:

a. Check the **Override** check box.

b. From the drop-down list, choose **High**.

Step 6 Click **Finish**.

Configure Authentication and Policy Servers

Catalyst Center uses AAA servers for user authentication and Cisco ISE for both user authentication and access control. Use this procedure to configure AAA servers, including Cisco ISE.

Before you begin

If you are using Cisco ISE to perform both policy and AAA functions, make sure that Catalyst Center and Cisco ISE are integrated.

If you are using another product (not Cisco ISE) to perform AAA functions, make sure to do the following:

- Register Catalyst Center with the AAA server, including defining the shared secret on both the AAA server and Catalyst Center.
- Define an attribute name for Catalyst Center on the AAA server.
- For a Catalyst Center multihost cluster configuration, define all individual host IP addresses and the virtual IP address for the multihost cluster on the AAA server.

Before you configure Cisco ISE, confirm that:

- You have deployed Cisco ISE on your network. For information on supported Cisco ISE versions, see the Cisco Catalyst Center Compatibility Matrix. For information on installing Cisco ISE, see the Cisco Identity Services Engine Install and Upgrade guides.
- If you have a standalone Cisco ISE deployment, you must integrate Catalyst Center with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.

Note Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Catalyst Center releases earlier than 2.2.1.x do not support more than two pxGrid nodes.

- If you have a distributed Cisco ISE deployment:

  You must integrate Catalyst Center with the primary policy administration node (PAN), and enable ERS on the PAN.

  Note We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the Policy Service Nodes (PSNs).

  You must enable the pxGrid service on one of the Cisco ISE nodes within the distributed deployment. Although you can choose to do so, you do not have to enable pxGrid on the PAN. You can enable pxGrid on any Cisco ISE node in your distributed deployment.

  The PSNs that you configure in Cisco ISE to handle TrustSec or SD Access content and Protected Access Credentials (PACs) must also be defined in **Work Centers** > **Trustsec** > **Trustsec Servers** > **Trustsec AAA Servers**. For more information, see the *Cisco Identity Services Engine Administrator Guide*.

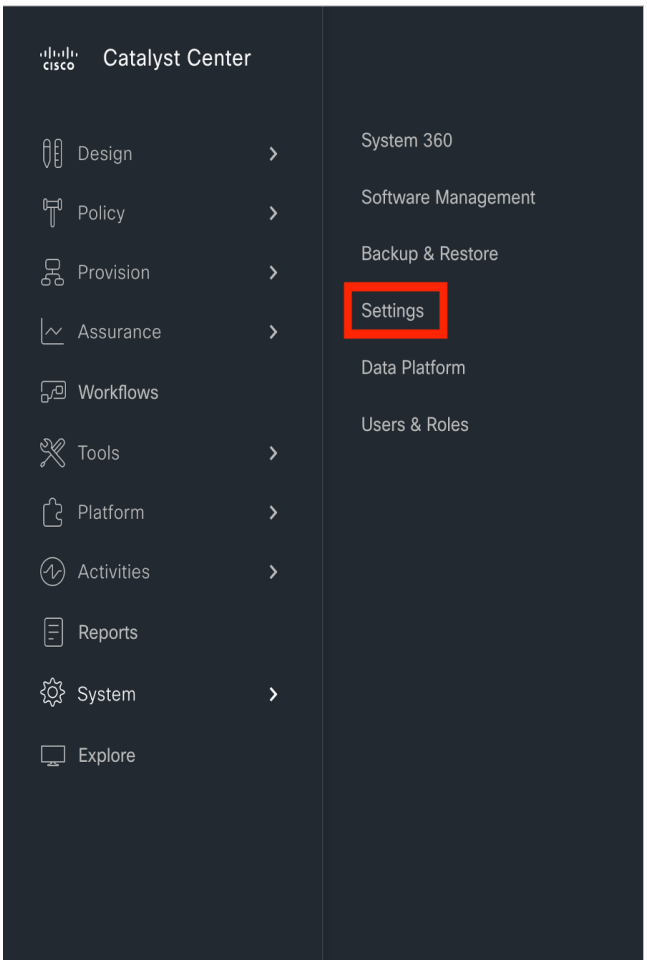
- You must enable communication between Catalyst Center and Cisco ISE on the following ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Catalyst Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or the fully qualified domain name (FQDN) in either the certificate subject name or the Subject Alternative Name (SAN).
- The Catalyst Center system certificate must list both the Catalyst Center appliance IP address and FQDN in the SAN field.

  Note For Cisco ISE 2.4 Patch 13, 2.6 Patch 7, and 2.7 Patch 3, if you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying those patches. This is because the older versions of that certificate have the Netscape Cert Type extension specified as the SSL server, which now fails (because a client certificate is required).

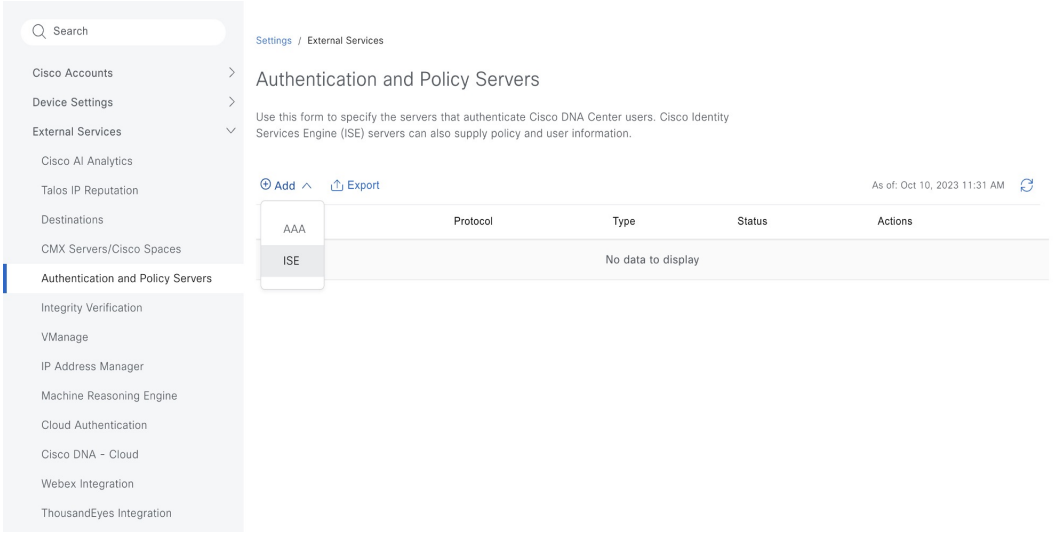
  This issue doesn't occur in Cisco ISE 3.0 and later. For more information, see the Cisco ISE Release Notes.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**.

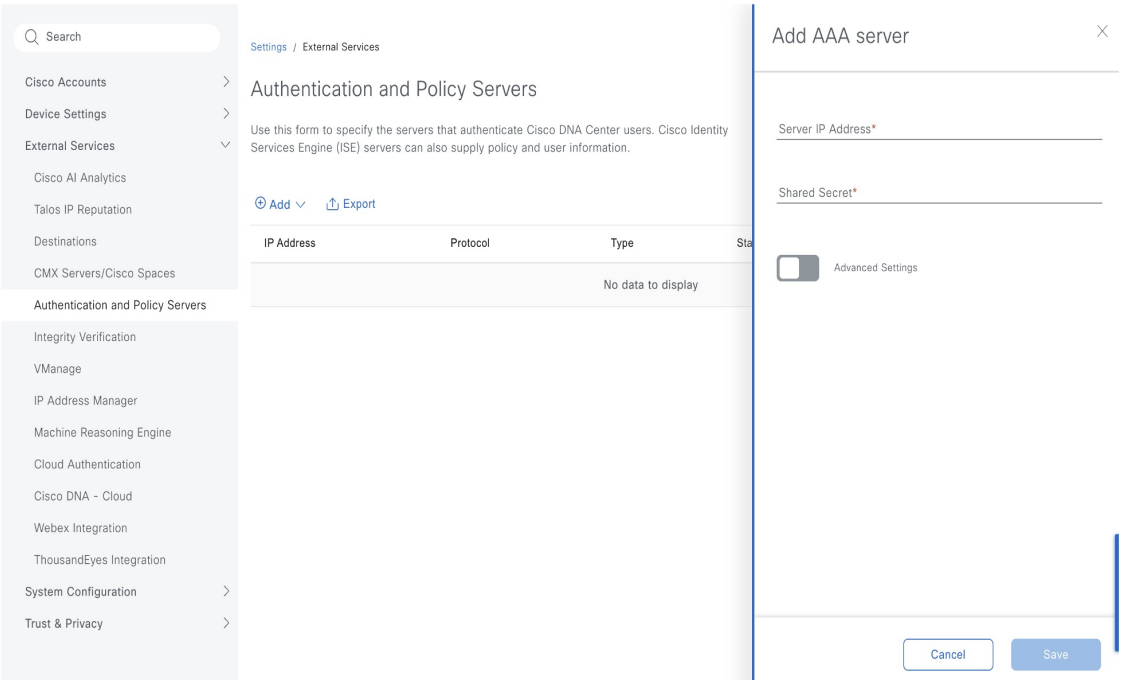


Step 2 From the **Add** drop-down list, choose **AAA** or **ISE**.



Step 3 To configure the primary AAA server, enter the following information:

- **Server IP Address**: IP address of the AAA server.
- **Shared Secret**: Key for device authentications. The shared secret must contain from 4 to 100 characters. It cannot contain a space, question mark (?), or less-than angle bracket (<).



Step 4 To configure a Cisco ISE server, enter the following details:

- **Server IP Address**: IP address of the Cisco ISE server.
- **Shared Secret**: Key for device authentications. The shared secret must contain from 4 to 100 characters. It cannot contain a space, question mark (?), or less-than angle bracket (<).
- **Username**: Username that is used to log in to Cisco ISE via HTTPS.
- **Password**: Password for the Cisco ISE HTTPS username.

  Note The username and password must be an ISE admin account that belongs to the Super Admin.

- **FQDN**: Fully qualified domain name (FQDN) of the Cisco ISE server.

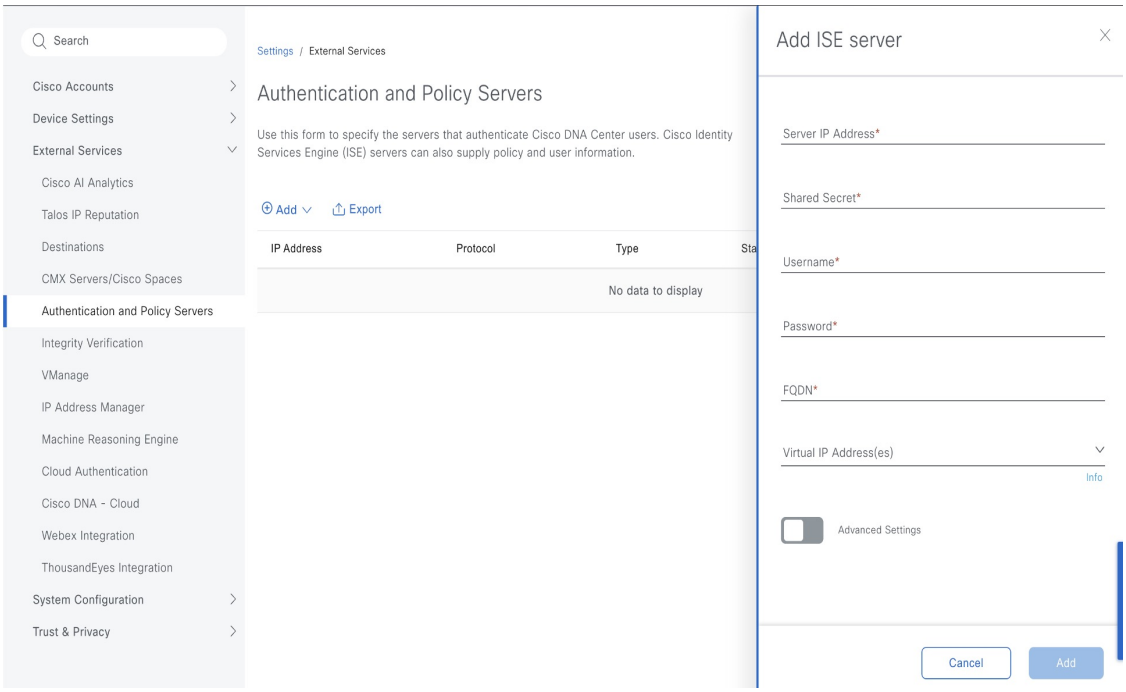
  Note
  - We recommend that you copy the FQDN that is defined in Cisco ISE (**Administration** > **Deployment** > **Deployment Nodes** > **List**) and paste it directly into this field.
  - The FQDN that you enter must match the FQDN, Common Name (CN), or Subject Alternative Name (SAN) defined in the Cisco ISE certificate.

  The FQDN consists of two parts, a hostname and the domain name, in the following format:

  hostname.domainname.com

  For example, the FQDN for a Cisco ISE server can be ise.cisco.com.

- **Virtual IP Address(es)**: Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.



Step 5 Click **Advanced Settings** and configure the settings:

- **Connect to pxGrid**: Check this check box to enable a pxGrid connection.

  If you want to use the Catalyst Center system certificate as the pxGrid client certificate (sent to Cisco ISE to authenticate the Catalyst Center system as a pxGrid client), check the **Use Catalyst Center Certificate for pxGrid** check box. You can use this option if all the certificates that are used in your operating environments must be generated by the same Certificate Authority (CA). If this option is disabled, Catalyst Center will send a request to Cisco ISE to generate a pxGrid client certificate for the system to use.

  When you enable this option, ensure that:

  - The Catalyst Center certificate is generated by the same CA as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).
  - The Certificate Extended Key Use (EKU) field includes "Client Authentication."

- **Protocol**: **TACACS** and **RADIUS** (the default). You can select both protocols.

  Attention If you do not enable TACACS for a Cisco ISE server here, you cannot configure the Cisco ISE server as a TACACS server under **Design** > **Network Settings** > **Servers** when configuring a AAA server for network device authentication.

- **Authentication Port**: UDP port used to relay authentication messages to the AAA server. The default UDP port used for authentication is 1812.
- **Accounting Port**: UDP port used to relay important events to the AAA server. The default is UDP port 1812.

- **Port**: TCP port used to communicate with the TACACS server. The default TCP port used for TACACS is 49.
- **Retries**: Number of times that Catalyst Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
- **Timeout**: The time period for which the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

Note

After the required information is provided, Cisco ISE is integrated with Catalyst Center in two phases. It takes several minutes for the integration to complete. The phase-wise integration status is shown in the **Authentication and Policy Servers** window and **System 360** window.

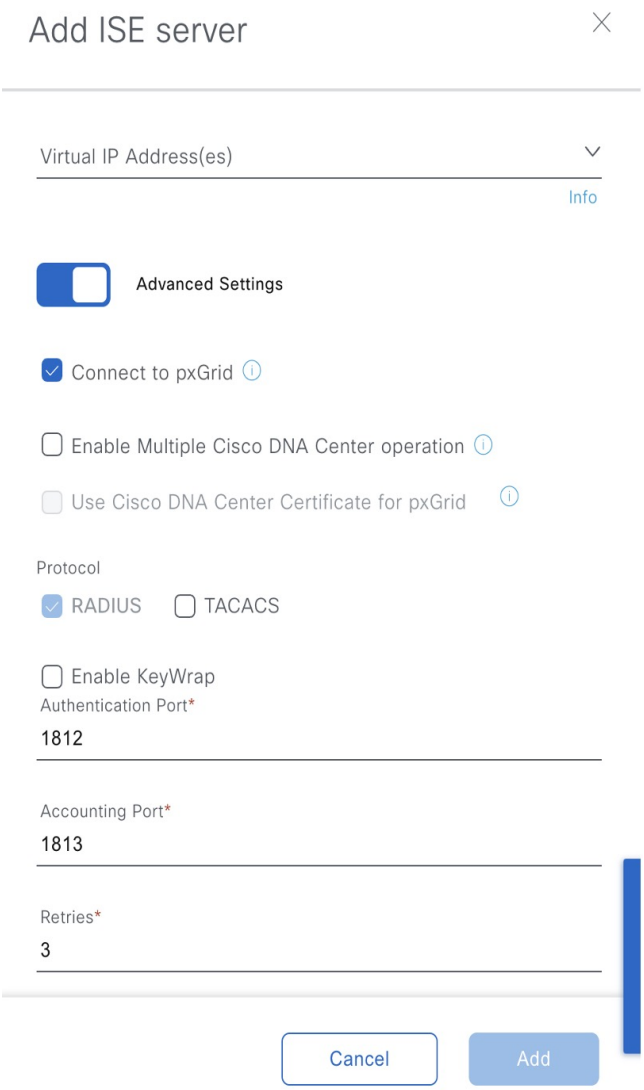
Cisco ISE server registration phase:

- **Authentication and Policy Servers** window: "In Progress"
- **System 360** window: "Primary Available"

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** window: "Active"
- **System 360** window: "Primary Available" and "pxGrid Available"

If the status of the configured Cisco ISE server is shown as "FAILED" due to a password change, click **Retry**, and update the password to resynchronize the Cisco ISE connectivity.



Step 6 Click **Add**.

Step 7 To add a secondary server, repeat the preceding steps.

Step 8 To view the Cisco ISE integration status of a device, do the following:

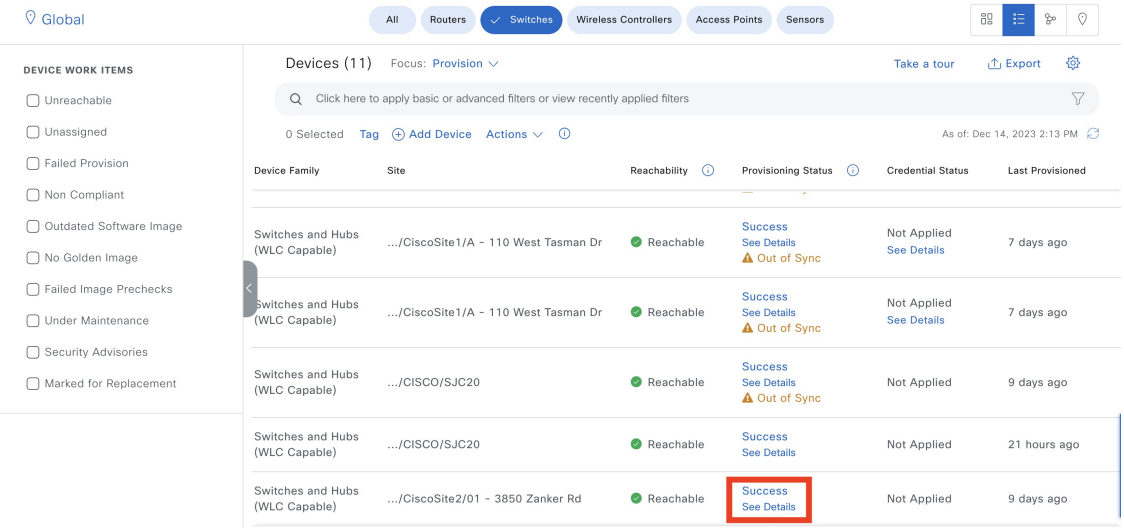
a. From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The **Inventory** window displays the device information.

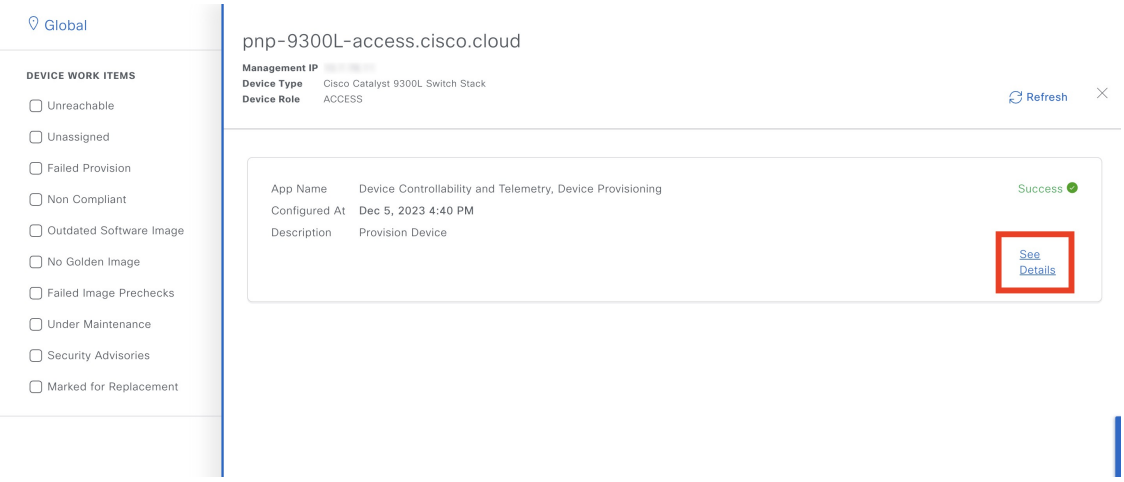
b. From the **Focus** drop-down menu, choose **Provision**.

c. In the **Devices** table, the **Provisioning Status** column displays information about the provisioning status of your device (**Success**, **Failed**, or **Not Provisioned**).

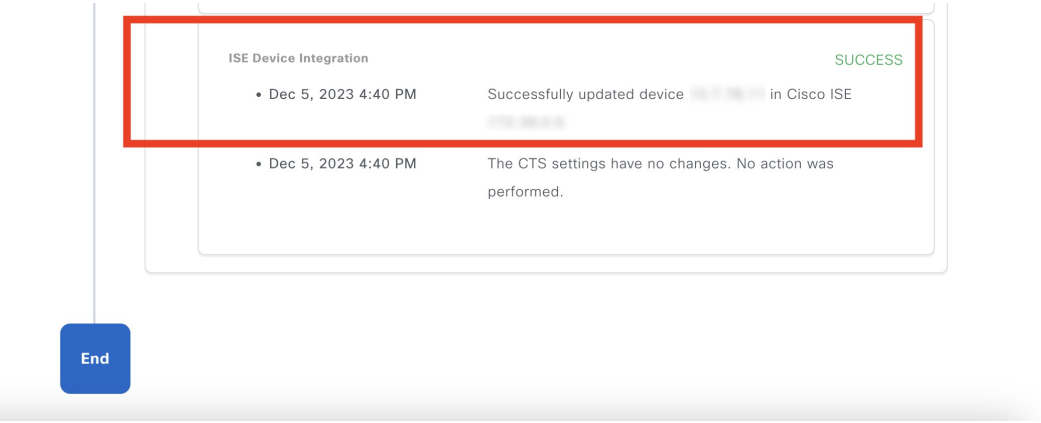
Click **See Details** to open a slide-in pane with additional information.



d. In the slide-in pane that is displayed, click **See Details**.



e. Scroll down to the **ISE Device Integration** tile to view detailed information about the integration status of the device.



High Availability

VMware vSphere High Availability (HA) provides high availability for Catalyst Center on ESXi by linking the virtual machines and their hosts in the same vSphere cluster. vSphere HA requires shared storage to function. If a host failure occurs, the virtual machines restart on alternate hosts. vSphere HA responds to the failure based on its configuration, and vSphere HA detects the failure at the following levels:

- Host level
- Virtual machine (VM) level
- Application level

In the current release, Catalyst Center only supports high availability for host-level failures.

Configure VMware vSphere HA for Host-Level Failures

To configure vSphere HA for host-level failures, complete the following procedure.

Before you begin

For the Catalyst Center virtual machine to take over from the failed hosts, at least two hosts must have the unreserved CPU/Memory resources described in the *Cisco Catalyst Center on ESXi Release Notes*.

Note Enable **HA Admission Control** with the appropriate configuration to ensure that the Catalyst Center virtual machine has sufficient resources to take over for the failed host. The configuration should allow the virtual machine to be restarted on another host without any impact to the system. If the necessary resources are not reserved, the virtual machine restarted on the failover host may fail due to resource shortage.

Procedure

Step 1 Log in to the vSphere Client.

Step 2 Choose the appropriate Catalyst Center cluster in the device menu.

Step 3 To configure the cluster, choose **Configure** > **Services** > **vSphere Availability**.

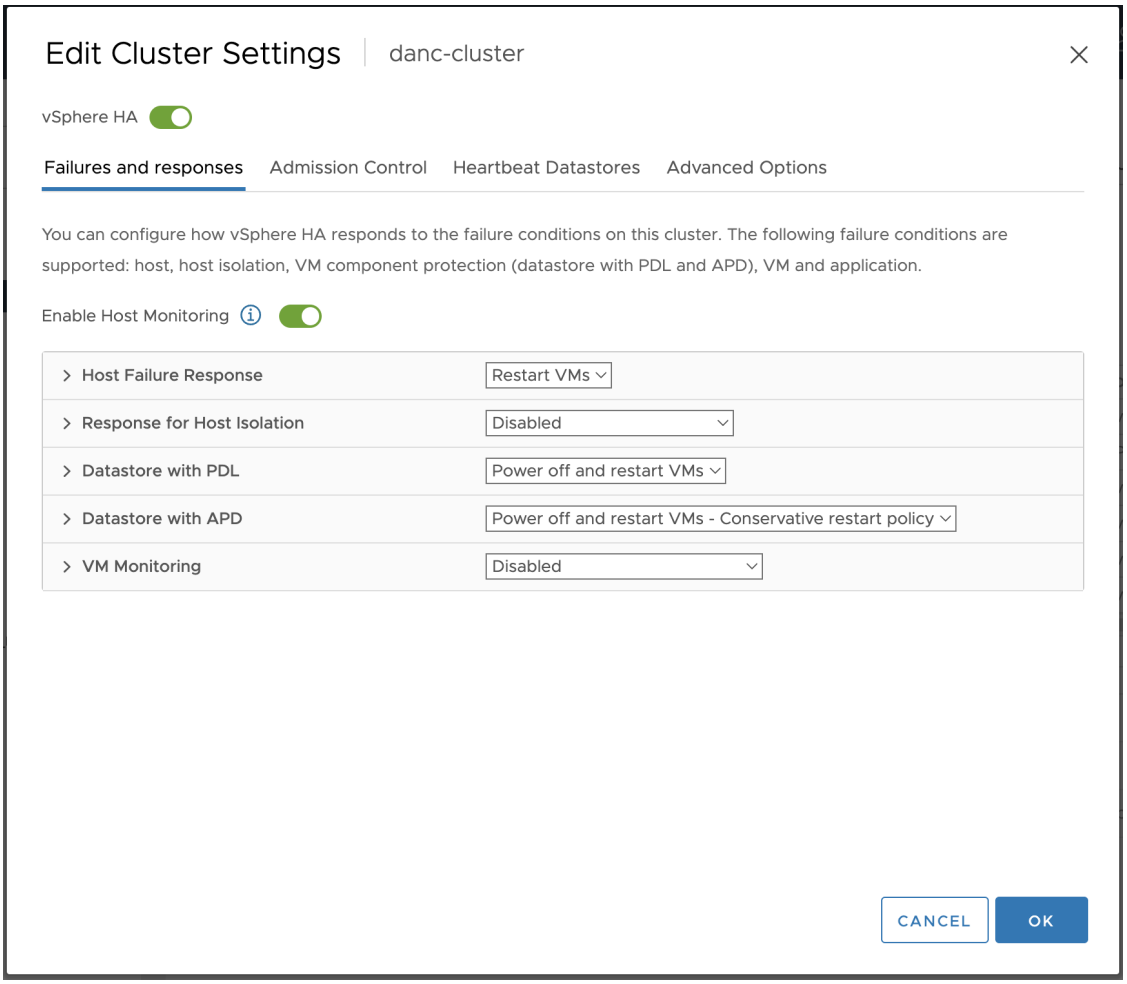
Step 4 From the top-right corner, click **Edit**.

Step 5 Click the toggle button to enable **vSphere HA**.

Step 6 Choose **Failures and responses** and configure the following settings:

a) Click the toggle button to enable **Host Monitoring**.

b) Go to the **Host Failure Response** drop-down list and choose **Restart VMs**.



Step 7 Click **OK**.

Configure Catalyst Center on ESXi Virtual Machine for Priority Restart

For the Catalyst Center on ESXi virtual machine to have priority restart upon host failure, complete the following procedure.

Procedure

Step 1 Log in to the vSphere Client.

Step 2 Choose the appropriate Catalyst Center on ESXi cluster in the device menu.

Step 3 To configure the cluster, choose **Configure** > **VM Overrides** > **ADD**.

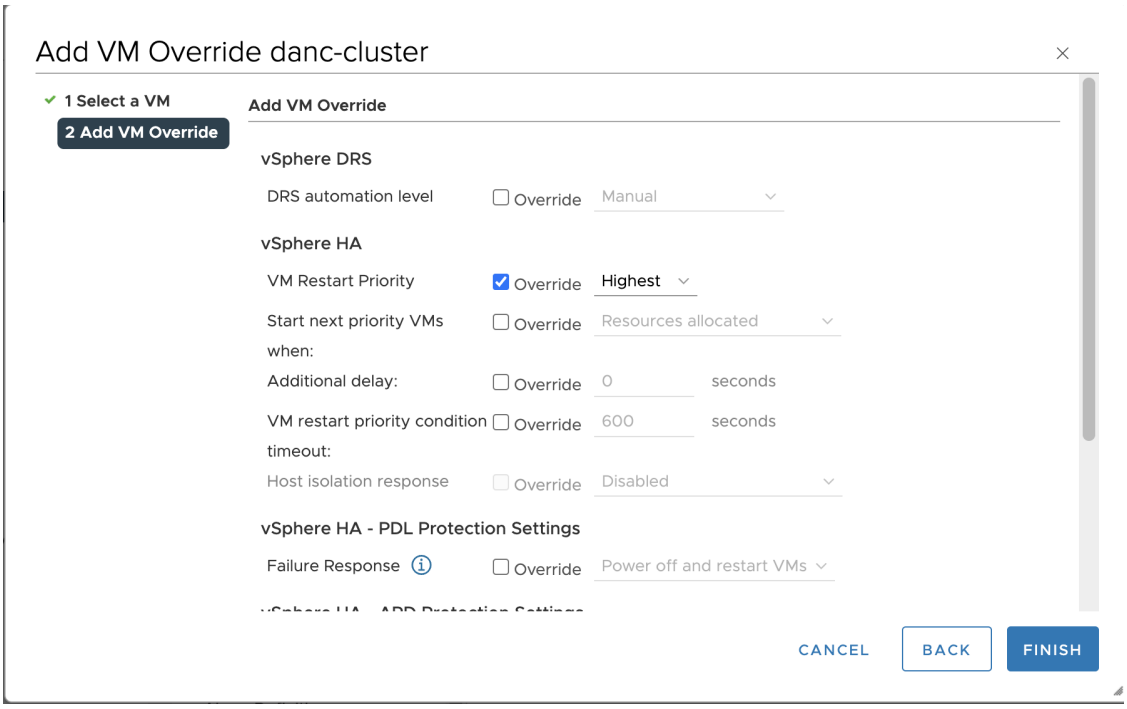
Step 4 In the **Select a VM** window, choose the deployed Catalyst Center on ESXi virtual machine.

Step 5 Click **OK**.

Step 6 In the **Add VM Override** window, go to **vSphere HA** > **VM Restart Priority** and configure the following settings:

a) Check the **Override** check box.

b) From the drop-down list, choose **Highest**.



Step 7 Click **FINISH**.

VMware vSphere Product Documentation

Catalyst Center on ESXi supports high availability through VMware vSphere HA functionality. For information about VMware vSphere's implementation and requirements for creating and using a vSphere HA cluster, see the following VMware vSphere Product Documentation:

- VMware High Availability Product Datasheet (PDF)
- VMware Infrastructure: Automating High Availability (HA) Services with VMware HA (PDF)
- How vSphere HA Works (HTML)
- vSphere HA Checklist (HTML)

Backup and Restore

You can use the backup and restore functions to create the backup files and to restore to the same or different virtual appliance (if required for your network configuration).

Automation and Assurance data are unified to use a single data storage device. The data can be stored on a physical disk that is attached to the virtual machine or on a remote Network File System (NFS) server.

Backup

You can back up both automation and Assurance data.

Automation data consists of Catalyst Center databases, credentials, file systems, and files. The automation backup is always a full backup.

Assurance data consists of network assurance and analytics data. The first backup of Assurance data is a full backup. After that, backups are incremental.

Note Do not modify the backup files. If you do, you might not be able to restore the backup files to Catalyst Center on ESXi.

Catalyst Center on ESXi creates the backup files and posts them to a physical disk or an NFS server.

You can add multiple physical disks for backup. If the previous backup disk runs out of disk space, you can use the other added disks for backup. For information on how to add a physical disk, see Add a Physical Disk for Backup and Restore, on page 133. You must change the disk in the **System** > **Settings** > **Backup Configuration** window, and save changes for the new disk to be used as a backup location. For information on how to change the physical disk, see Configure the Location to Store Backup Files, on page 139.

You can also add multiple NFS servers for backup. For information on how to add an NFS server, see Add the NFS Server, on page 137. You must change the NFS server in the **System** > **Settings** > **Backup Configuration** window, and save changes for the new NFS server to be used as a backup location. For information on how to change the NFS server, see Configure the Location to Store Backup Files, on page 139.

Note Only a single backup can be performed at a time. Performing multiple backups at once is not supported.

When a backup is being performed, you cannot delete the files that have been uploaded to the backup server, and changes that you make to these files might not be captured by the backup process.

We recommend the following:

- Perform a daily backup to maintain a current version of your database and files.
- Perform a backup after making changes to your configuration, for example, when changing or creating a new policy on a device.
- Perform a backup only during a low-impact or maintenance period.

You can schedule weekly backups on a specific day of the week and time.

Restore

You can restore backup files from the physical disk or NFS server using Catalyst Center on ESXi.

Catalyst Center on ESXi supports cross-version backup and restore; that is, you can create a backup on one version of Catalyst Center on ESXi and restore it to another version of Catalyst Center on ESXi. For example, a backup on Catalyst Center on ESXi 2.3.7.0-75530 version can be restored to Catalyst Center on ESXi 2.3.7.3-75176 version. The same applies to the later releases of Catalyst Center on ESXi.

Note A backup created on a virtual machine can only be restored on a virtual machine with the same or later software version.

When you restore the backup files, Catalyst Center on ESXi removes and replaces the existing database and files with the backup database and files. While a restore is being performed, Catalyst Center on ESXi is unavailable.

You can restore the backup files of a failed or faulty virtual appliance. For more information, see Restore Data from a Physical Disk for a Faulty Virtual Appliance, on page 147 and Restore Data from an NFS Server for a Faulty Virtual Appliance, on page 153.

Also, you can restore a backup to a Catalyst Center on ESXi appliance with a different IP address.

Note After a backup and restore of Catalyst Center on ESXi, you must access the **Integration Settings** window and update (if necessary) the **Callback URL Host Name** or **IP Address**.

Backup and Restore Event Notifications

You can receive a notification whenever a backup or restore event takes place. To configure and subscribe to these notifications, complete the steps described in the "Work with Event Notifications" topic of the *Cisco Catalyst Center Platform User Guide*. When completing this procedure, ensure that you select and subscribe to the SYSTEM-BACKUP and SYSTEM-RESTORE events.

Operation	Event
Backup	The process to create a backup file for your system has started.
	A backup file could not be created for your system. • This event typically happens because the necessary disk space is not available on remote storage. • You encountered connectivity issues or latency while creating a backup file on your system.
Restore	The process to restore a backup file has started.
	The restoration of a backup file failed. • This event typically happens because the backup file has become corrupted. • You encountered connectivity issues or latency while creating a backup file from your system.

NFS Backup Server Requirements

To support data backups on the NFS server, the server must be a Linux-based NFS server that meets the following requirements:

- Support NFS v4 and NFS v3. (To verify this support, from the server, enter **nfsstat -s**.)
- Have read and write permissions on the NFS export directory.
- Have a stable network connection between Catalyst Center on ESXi and the NFS server.
- Have sufficient network speed between Catalyst Center on ESXi and the NFS server.

Note You cannot use an NFS-mounted directory as the backup server. A cascaded NFS mount adds a layer of latency and is therefore not supported.

Requirements for Multiple Catalyst Center on ESXi Deployments

If your network includes multiple Catalyst Center clusters, the following example configuration shows how to name your NFS server backup directory structure:

Resource	Example Configuration
Catalyst Center on ESXi clusters	**1.** *cluster1* **2.** *cluster2*
Backup server hosting automation and Assurance backups	The example directory is `/data/`, which has ample space to host both types of backups.

NFS export configuration	The content of the `/etc/exports` file:
	`/data/cluster1 *(rw,sync,no_subtree_check,all_squash)`
	`/data/cluster2 *(rw,sync,no_subtree_check,all_squash)`

Backup Physical Disk Nomenclature

To use a physical disk for backup, you must add a physical disk to the virtual machine. To easily identify the physical disks for backups, UUID is used.

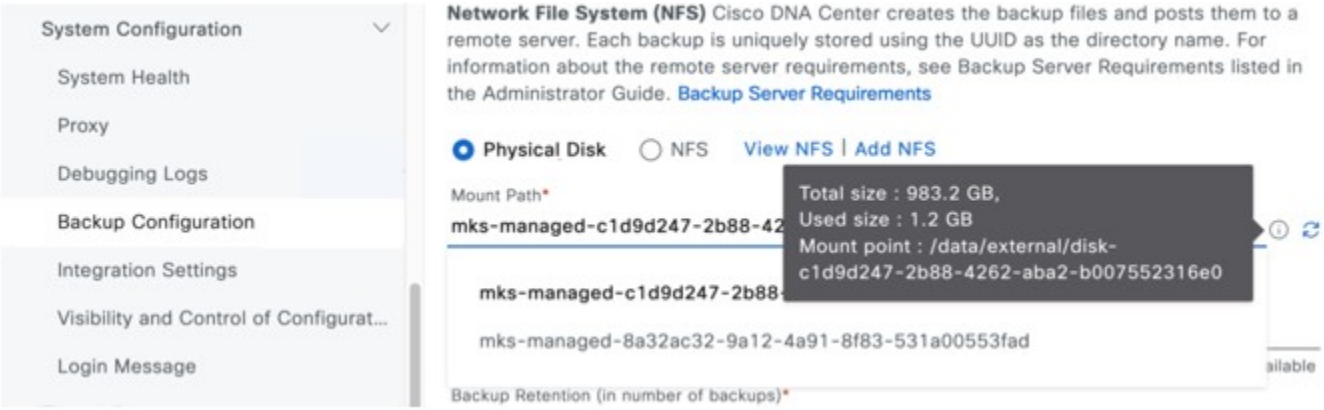
UUID is a unique identifier that is associated with the disk, which does not change across reboots. A disk that is removed and added to a different cluster will have the same UUID, as long as it is not formatted again.

The disk is explicitly labeled as `mks-managed`.

You can view the physical disks available for backup in the **System** > **Settings** > **Backup Configuration** window, under the **Mount Path** drop-down list.

Hover over the **i** icon to view the physical disk nomenclature, which is shown in the following format:

```
/data/external/disk-<uuid>
```



Backup Storage Requirements

Catalyst Center on ESXi stores backup copies of Assurance and automation data on a physical disk that is attached to the virtual machine or a remote NFS server. You must allocate enough external storage for your backups to cover the required retention. We recommend the following storage.

Virtual Appliance	Assurance Data Storage (14 Days Incremental)	Automation Data Storage (Daily Full)	Physical Disk/NFS Server (Assurance and Automation) Storage
DN-SW-APL	1.75 TB	50 GB	1.75 TB + 50 GB

Additional notes:

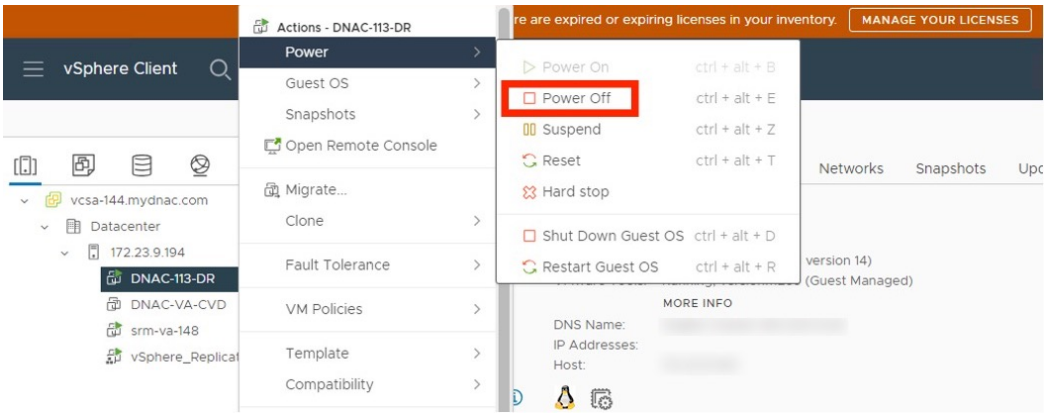
- The preceding table assumes fully loaded virtual appliance configurations that support the maximum number of access points and network devices for each appliance.
- The automation backup sizing is estimated for one daily backup. If you want to retain backups for additional days, multiply the required storage by the additional number of days. For example, if you have a DN-SW-APL virtual appliance and you want to store five copies of automation data backups generated once each day, the total storage required is 5 * 50 GB = 250 GB.
- The total backup time varies depending on your daily data load and the amount of historical data that you want to retain.
- The write path to Catalyst Center depends on the network throughput from Catalyst Center to the NFS server. The NFS server must have a throughput of at least 100 MB/sec.
- As with any other IT service, monitoring NFS performance is required to ensure optimal performance.

Add a Physical Disk for Backup and Restore

Use this procedure to add a physical disk that can be used for backup and restore operations.

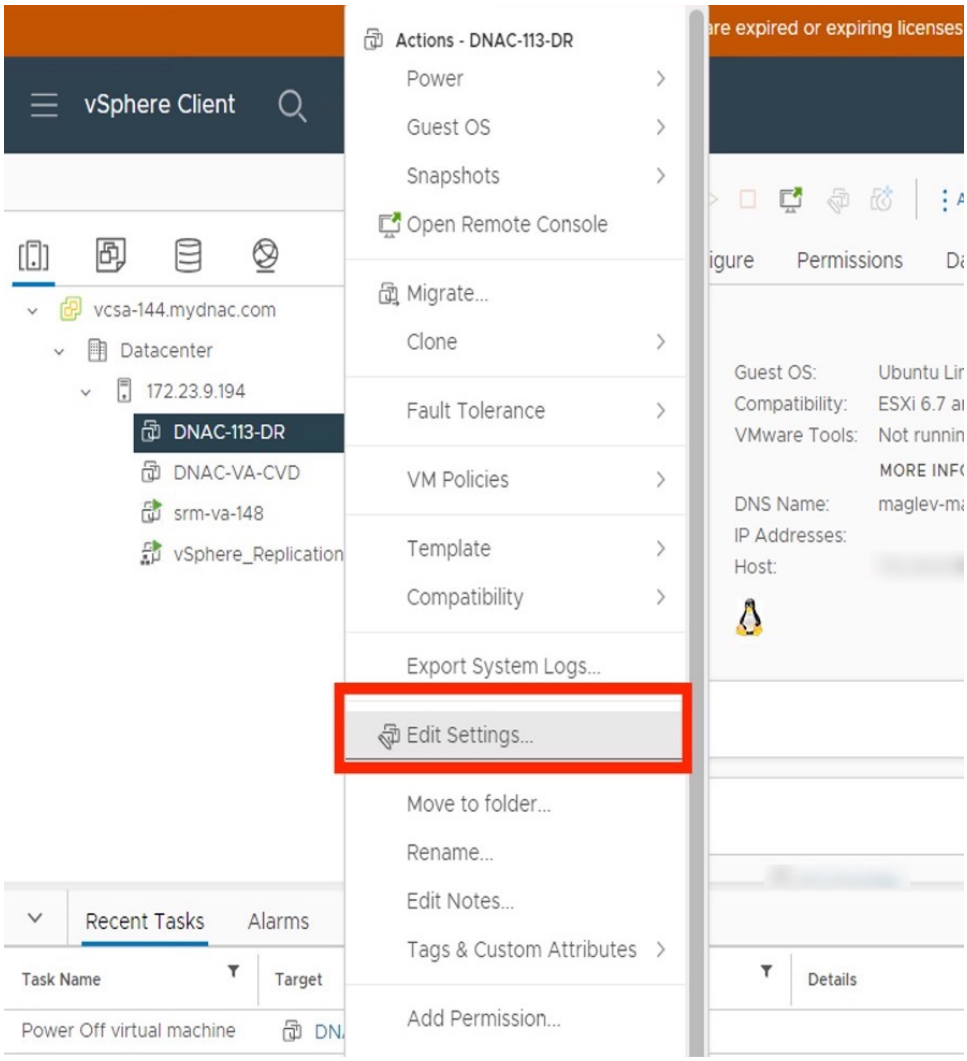
Procedure

Step 1 If your appliance is running on the machine that's hosting Catalyst Center on ESXi, power off the appliance's virtual machine.

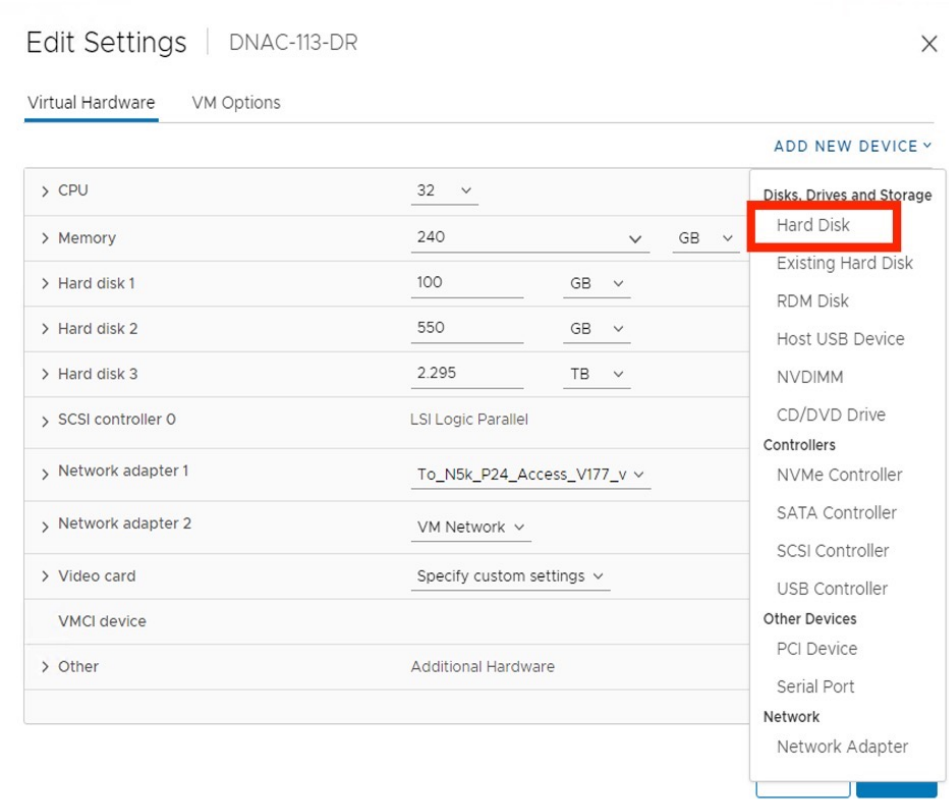


Step 2 Log in to VMware vSphere.

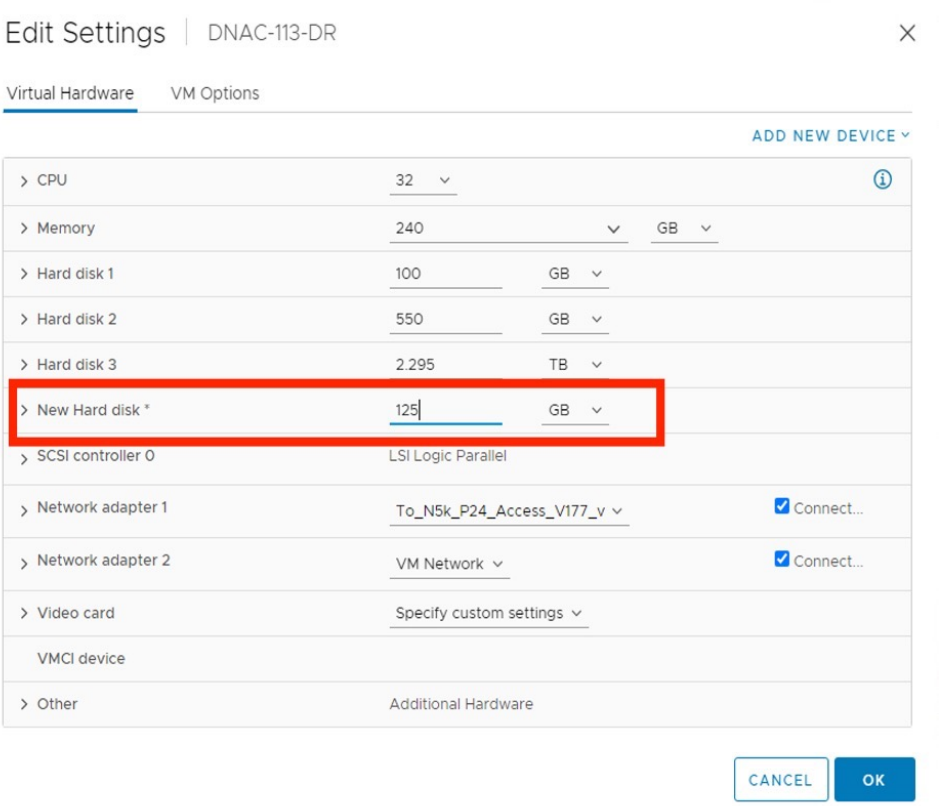
Step 3 From the vSphere client's left pane, right-click the ESXi host and then choose **Edit Settings**.



Step 4 In the **Edit Settings** dialog box, click **Add New Device** and then choose **Hard Disk**.



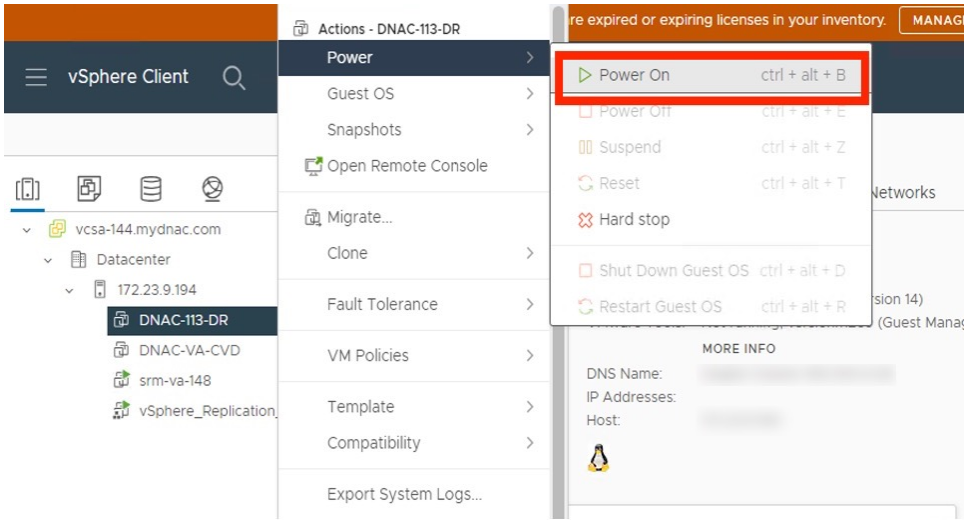
Step 5 In the **New Hard disk** field, enter the desired storage size.



Note For information on the recommended storage space for backup, see Backup Storage Requirements, on page 132.

Step 6 Click **OK**.

Step 7 Power on the appliance's virtual machine.



What to do next

You can now configure the added physical disk for backup. For information on how to configure the physical disk, see Configure the Location to Store Backup Files, on page 139.

Add the NFS Server

Catalyst Center allows you to add multiple Network File System (NFS) servers for backup purposes. Use this procedure to add an NFS server that can be used for the backup operation.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Backup Configuration**.

Step 2 Click the **Add NFS** link.

Step 3 In the **Add NFS** slide-in pane, do the following:

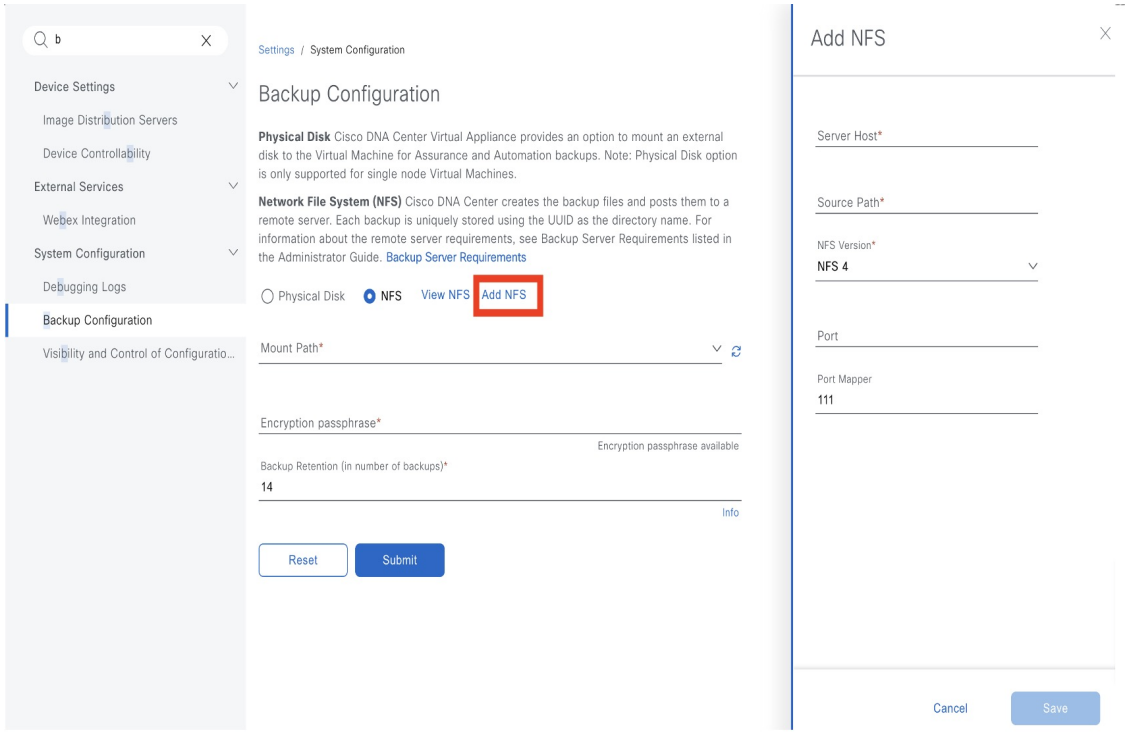
a) Enter the **Server Host** and **Source Path** in the respective fields.

b) Choose **NFS Version** from the drop-down list.

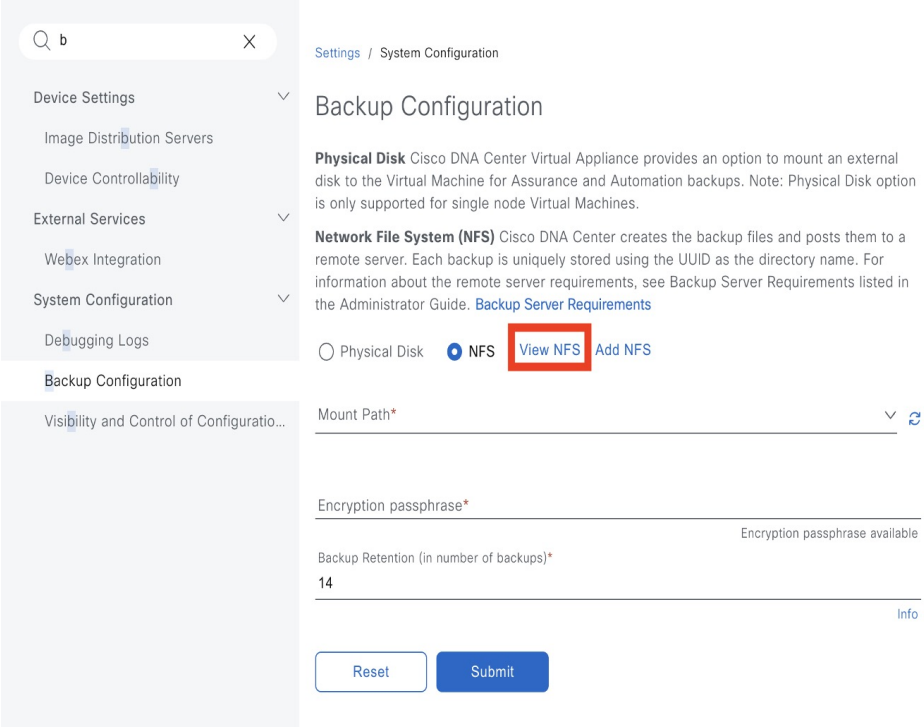
c) The **Port** is added by default. You can leave the field empty.

d) (Optional) Enter the **Port Mapper** number.

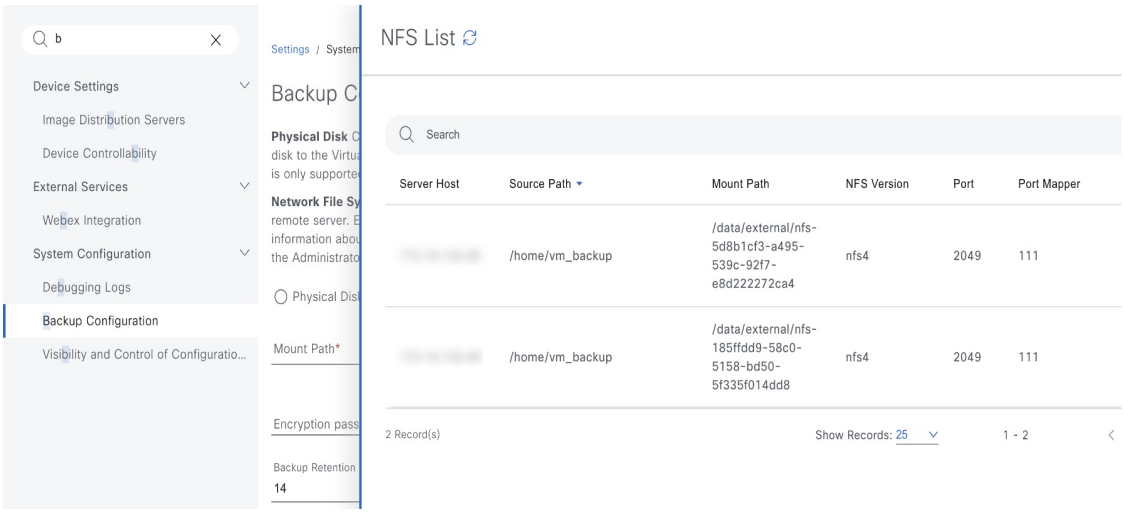
e) Click **Save**.



Step 4 Click **View NFS** to view the available NFS servers.

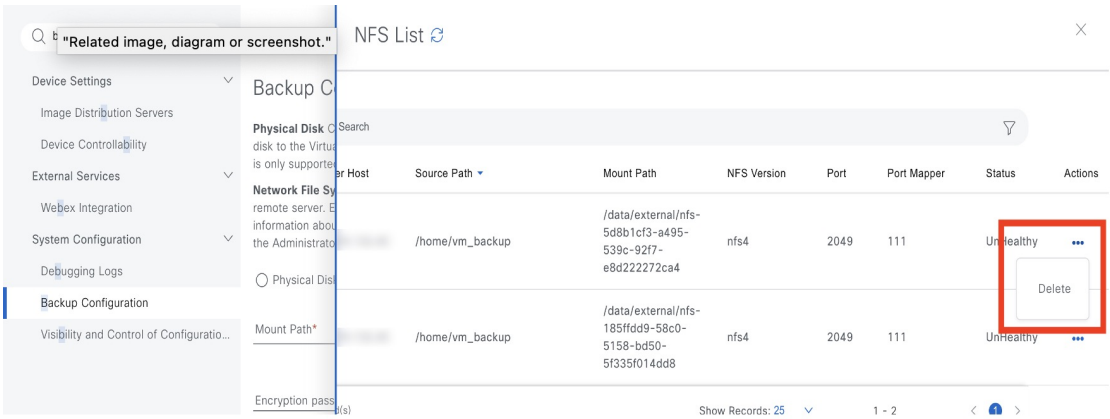


The **NFS** slide-in pane displays the list of NFS servers, along with details.



Step 5 In the **NFS** slide-in pane, click the ellipsis under **Actions** to **Delete** the NFS server.

Note You can delete the NFS server only when there is no backup job in progress.



What to do next

Configure the added NFS server for backup. For more information, see Configure the Location to Store Backup Files, on page 139.

Configure the Location to Store Backup Files

Catalyst Center allows you to configure backups for automation and Assurance data.

Use this procedure to configure the storage location for backup files.

Before you begin

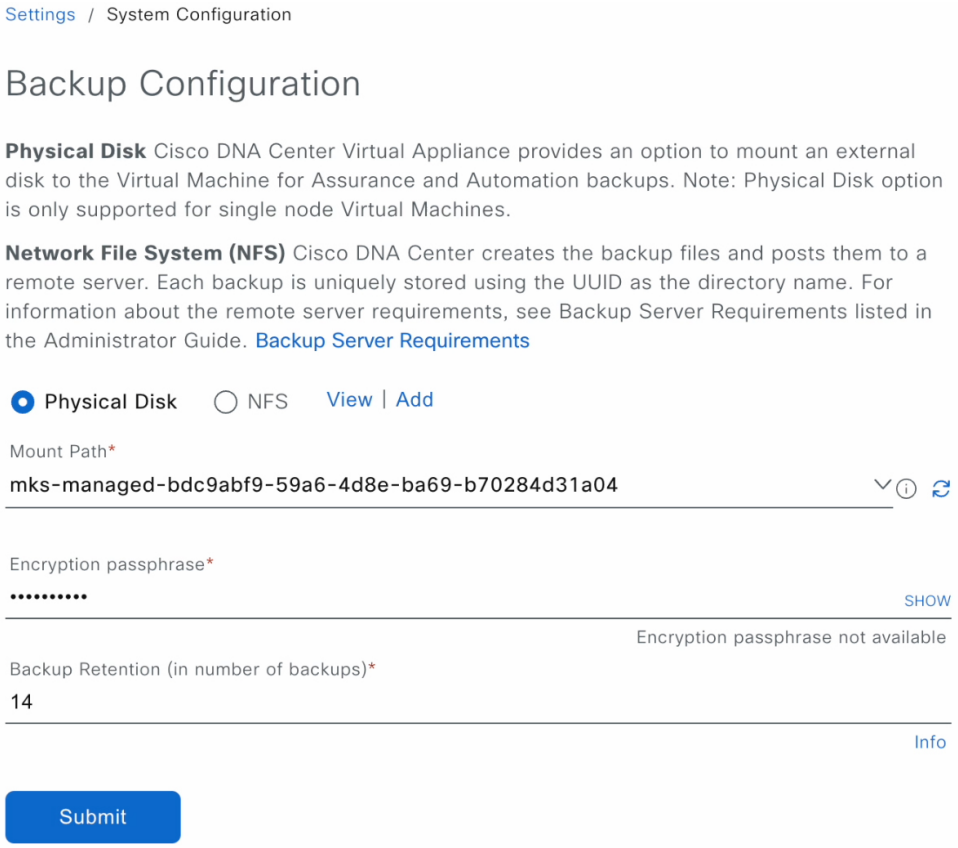
Make sure that the following requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in NFS Backup Server Requirements, on page 131.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

You can choose a physical disk or NFS server as your backup location.



Step 2 **Physical Disk**: Catalyst Center provides an option to mount an external disk to the virtual machine, to store a backup copy of Assurance and automation data. To configure a physical disk, click the **Physical Disk** radio button and define the following settings:

Note The physical disk option is only supported for single-node virtual machines.

Field	Description
Mount Path	Location of the external disk.
Encryption Passphrase	Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials. This passphrase is required, and you will be prompted to enter this passphrase when restoring the backup files. Without this passphrase, backup files are not restored.
Backup Retention	Number of backups for which the data is retained. Data older than the specified number of backups is deleted.

Step 3 **NFS**: Catalyst Center creates the backup files and posts them to a remote NFS server. For information about the remote server requirements, see NFS Backup Server Requirements, on page 131. To configure an NFS backup server, click the **NFS** radio button and define the following settings:

Field	Description
Mount Path	Location of the remote server.
Encryption Passphrase	Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials. This passphrase is required, and you will be prompted to enter this passphrase when restoring the backup files. Without this passphrase, backup files are not restored.
Backup Retention	Number of backups for which the data is retained. Data older than the specified number of backups is deleted.

Step 4 Click **Submit**.

After the request is submitted, you can view the configured physical disk or NFS server under **System** > **Backup & Restore**.

Create a Backup

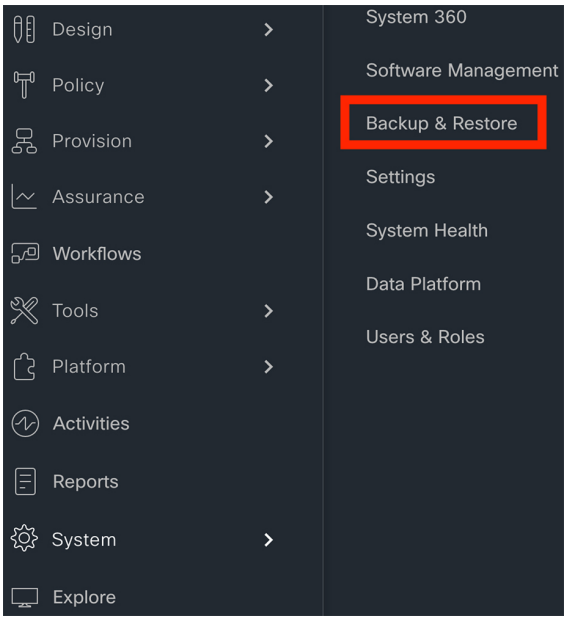
Use this procedure to create a backup of your virtual appliance.

Before you begin

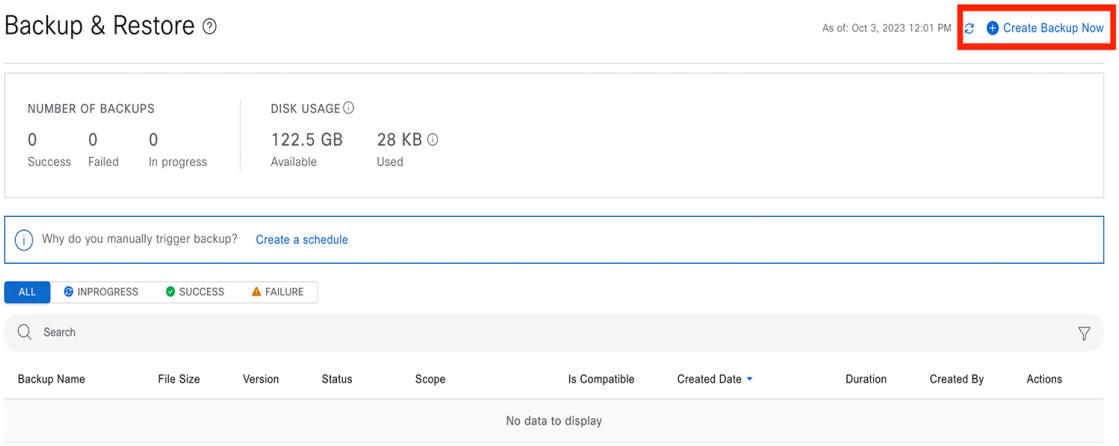
You must configure the backup location. For more information, see Configure the Location to Store Backup Files, on page 139.

Procedure

Step 1 From the Catalyst Center on ESXi menu, choose **System** > **Backup & Restore**.

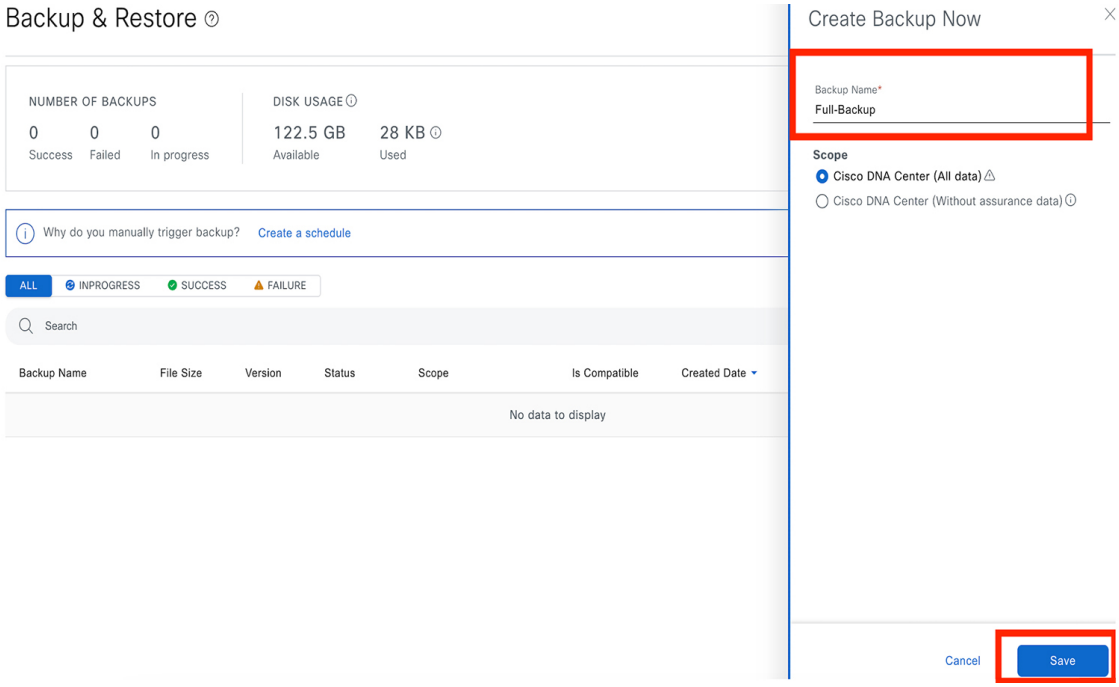


Step 2 Click **Create Backup Now**.

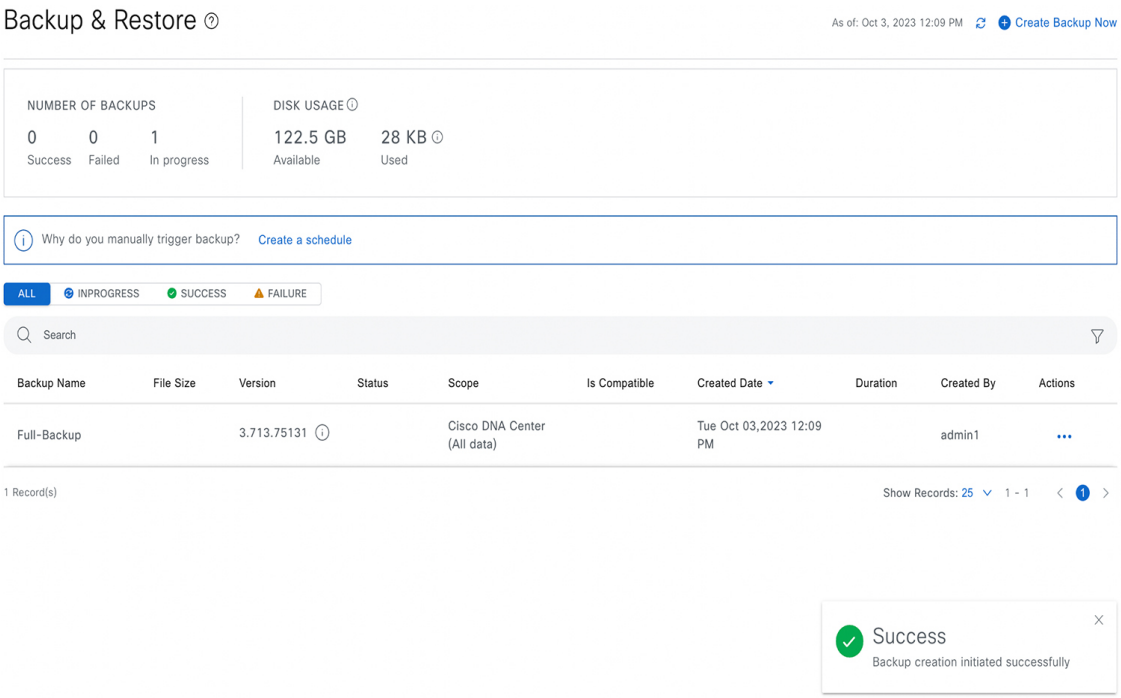


The **Create Backup Now** slide-in pane opens.

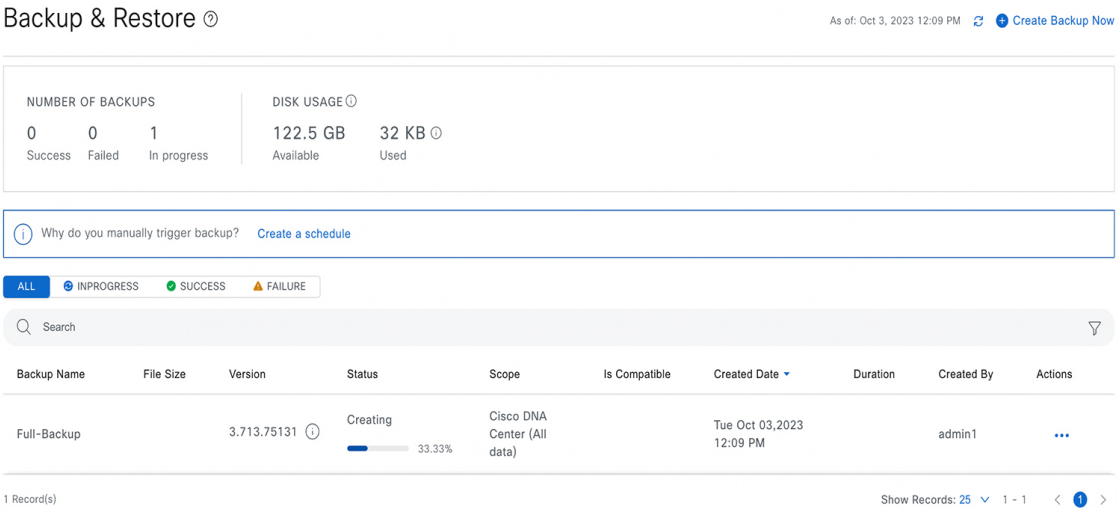
Step 3 Enter a unique name for the backup, then click **Save**.



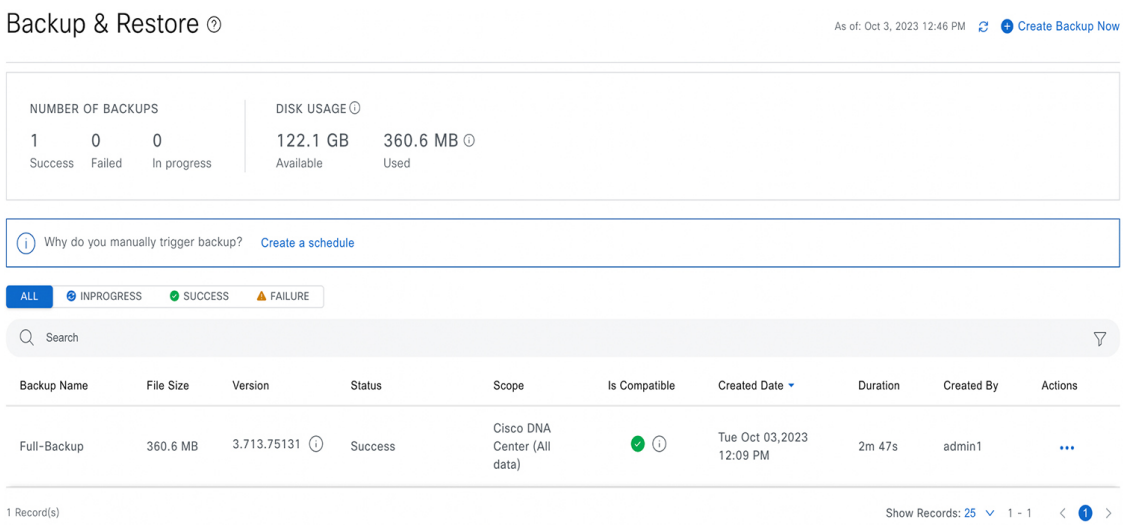
Catalyst Center on ESXi begins the backup process. An entry for the backup is added to the **Backup & Restore** window's table.



To view details regarding the backup's status, click the ellipsis, and then choose **View Status**.



When the backup is complete, its status changes from `Creating` to `Success`.



Restore Data from Backups

Use this procedure to restore backup data from your virtual appliance. To restore backup data from a failed or faulty virtual appliance, see Restore Data from a Physical Disk for a Faulty Virtual Appliance, on page 147.

Caution The Catalyst Center restore process restores only the database and files. The restore process does not restore your network state or any changes that were made since the last backup, including any new or updated network policies, passwords, certificates, or trustpool bundles.

Before you begin

Make sure that the following requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- You have backups from which to restore data.

When you restore data, Catalyst Center on ESXi enters maintenance mode, and is unavailable until the restore process is completed. Make sure you restore data at a time when Catalyst Center on ESXi can be unavailable.

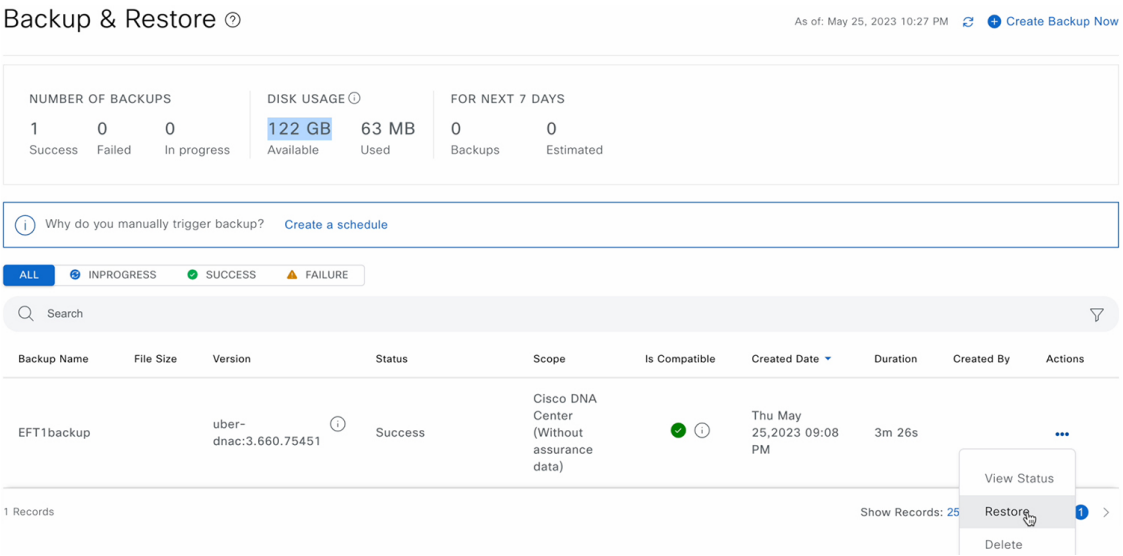
Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Backup & Restore**.

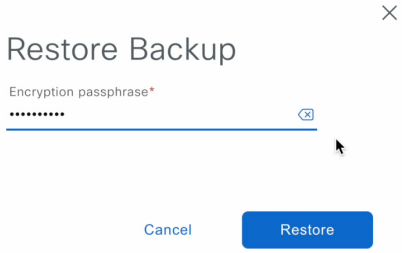
If you have created a backup, it appears in the **Backup & Restore** window.

Step 2 In the **Backup Name** column, locate the backup that you want to restore.

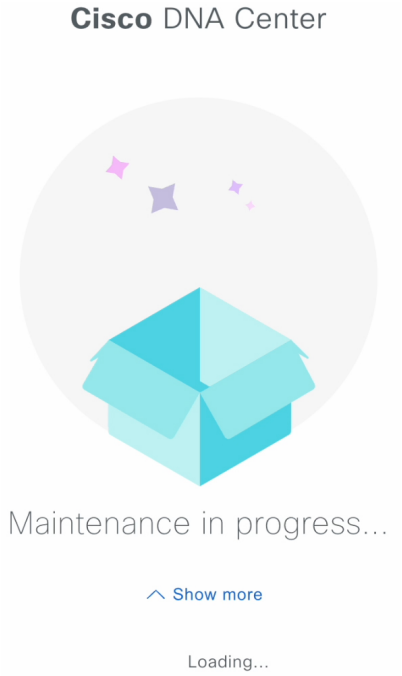
Step 3 In the **Actions** column, click the ellipsis and choose **Restore**.



Step 4 In the **Restore Backup** dialog box, enter the **Encryption Passphrase** that you used while configuring the backup location and click **Restore**.

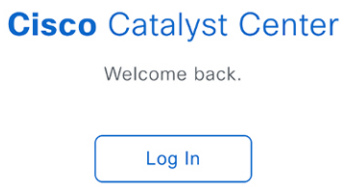


The appliance goes into maintenance mode and starts the restore process.

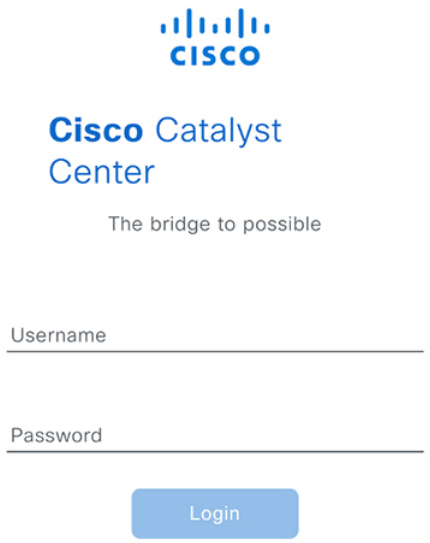


When the restore operation is complete, its status in the **Backup & Restore** window table changes to `Success`.

Step 5 After the restore operation completes, click **Log In** to log back in to Catalyst Center on ESXi.



Step 6 Enter the admin user's username and password, then click **Login**.



Restore Data from a Physical Disk for a Faulty Virtual Appliance

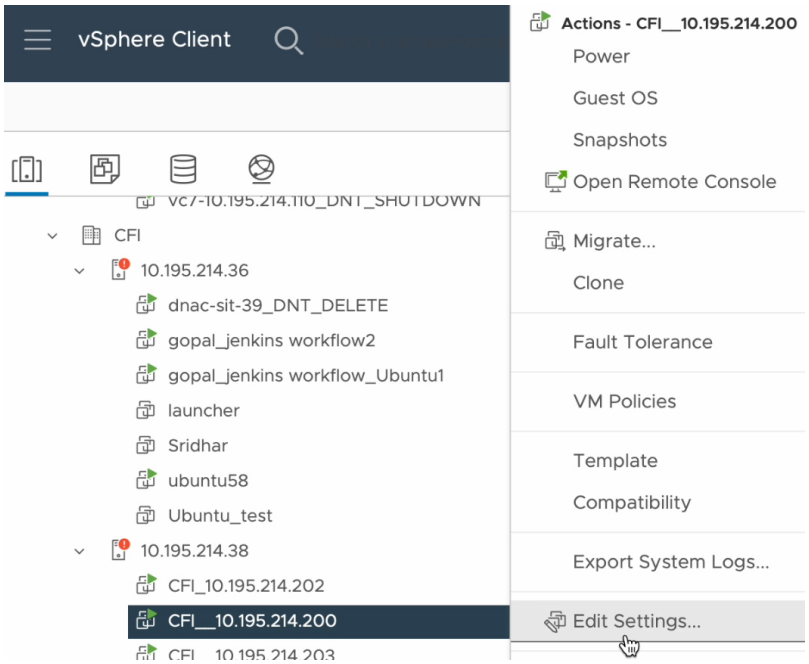
Use this procedure to restore data from a physical disk for a virtual appliance that has failed or is faulty.

Procedure

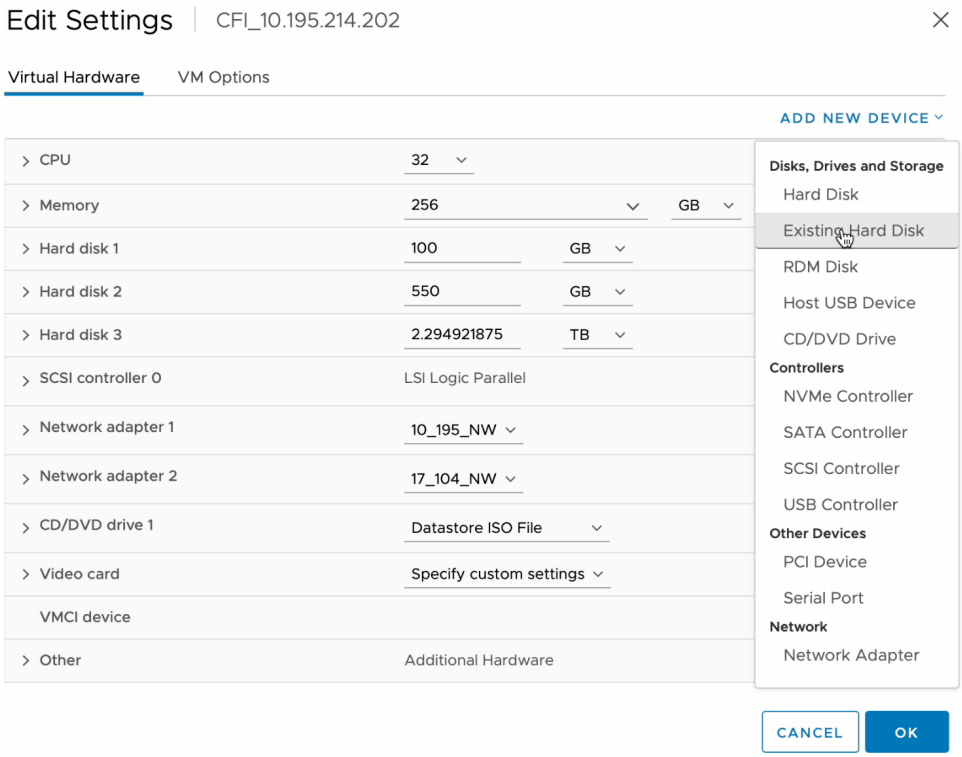
Step 1 For your new virtual appliance, do the following to configure Catalyst Center on ESXi to use the storage disk that you configured for the faulty virtual appliance:

a. Power OFF the appliance's virtual machine.

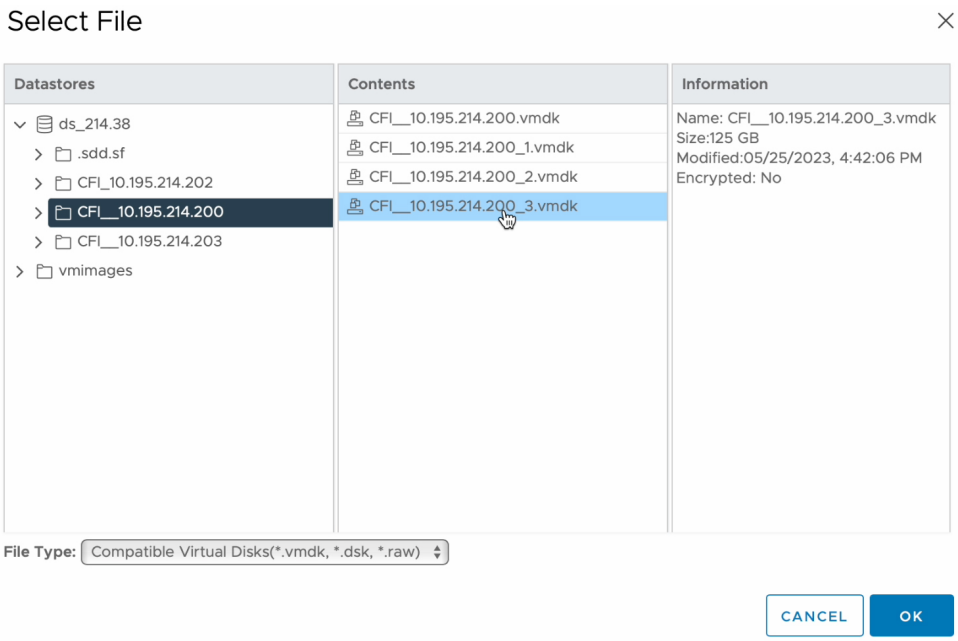
b. Open a vSphere Client, right-click the Catalyst Center on ESXi virtual machine in the left pane, and then choose **Edit Settings**.



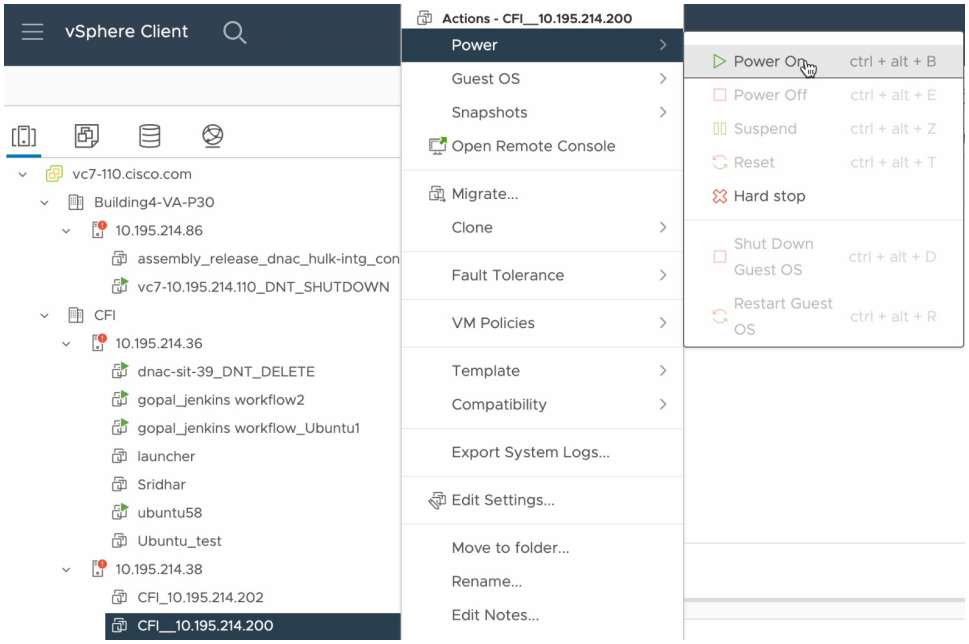
c. In the **Edit Settings** dialog box, click **Add New Device** and then choose **Existing Hard Disk**.



d. In the **Select File** dialog box, click your ESXi host, click the storage disk (.vmdk) that was created, and then click **OK**.



e. Power on the appliance's virtual machine.



It takes approximately 45 minutes for all the services to restart.

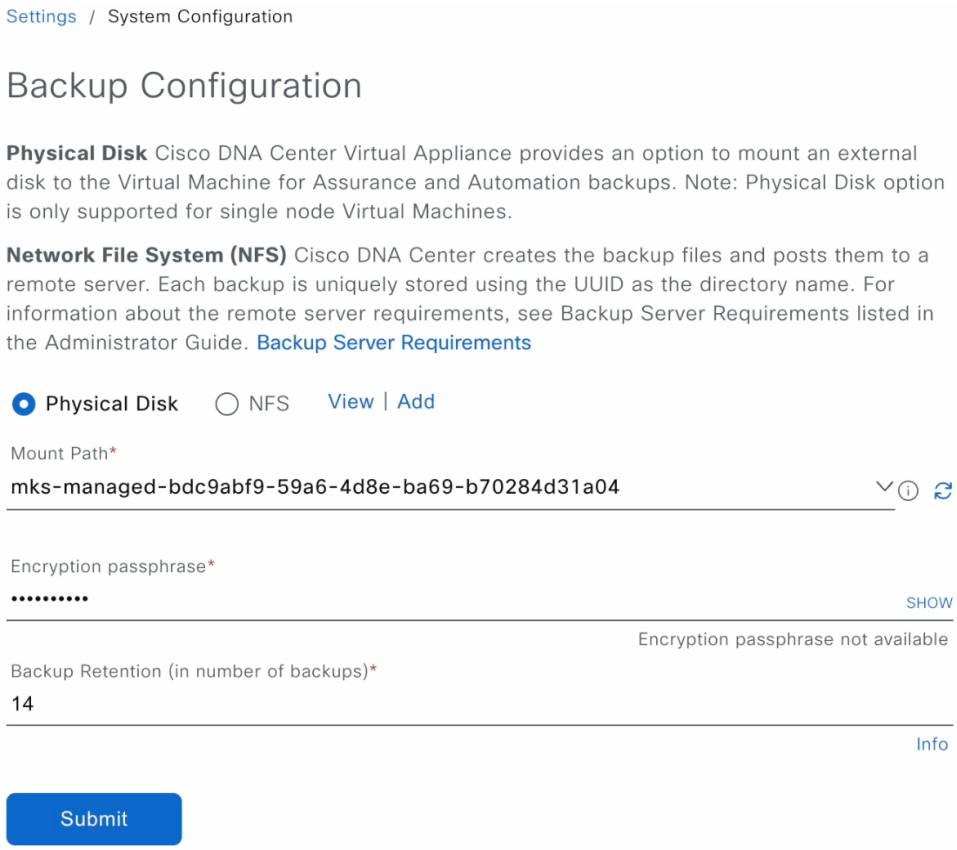
Note After the virtual machine comes back up, run the **magctl appstack status** command to confirm that the services are running.

Step 2 To configure the storage location for the backup, do the following:

a) From the Catalyst Center on ESXi menu, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

b) Click the **Physical Disk** radio button.

c) Choose the physical disk from the **Mount Path** drop-down list.



d) Enter the passphrase that will be used to encrypt the security-sensitive components of the backup (such as certificates and credentials).

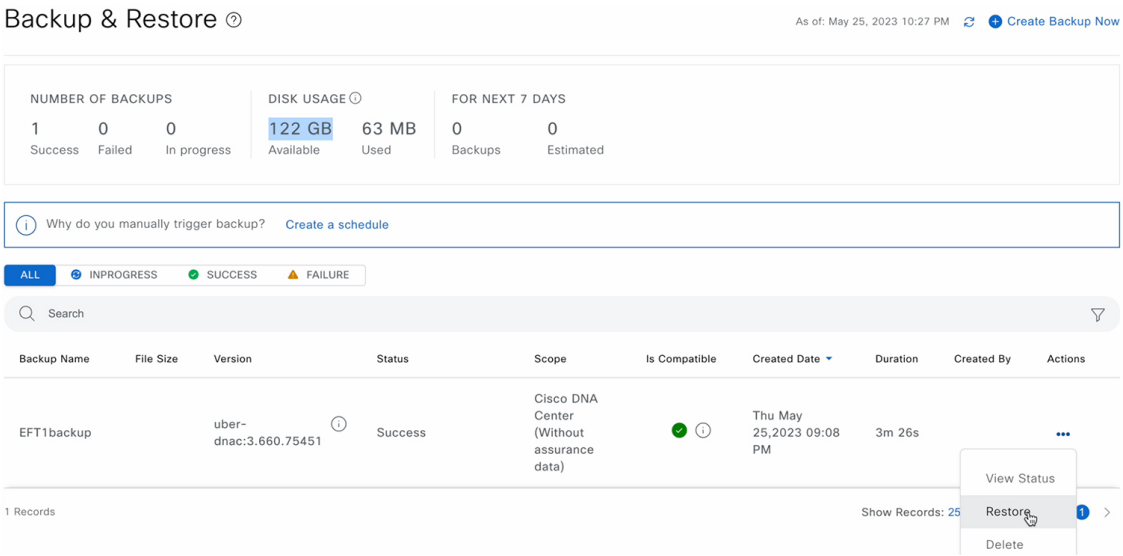
Important Make sure that you don't lose this passphrase. You'll need to enter it later in the succeeding steps and won't be able to restore the backup you're about to create without it.

e) Set how long backup files are kept before they are deleted.

f) Click **Submit**.

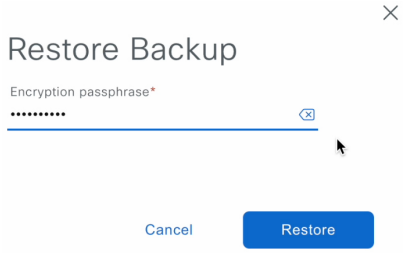
Step 3 To restore the backup, do the following:

a) From the Catalyst Center on ESXi menu, choose **System** > **Backup & Restore**.

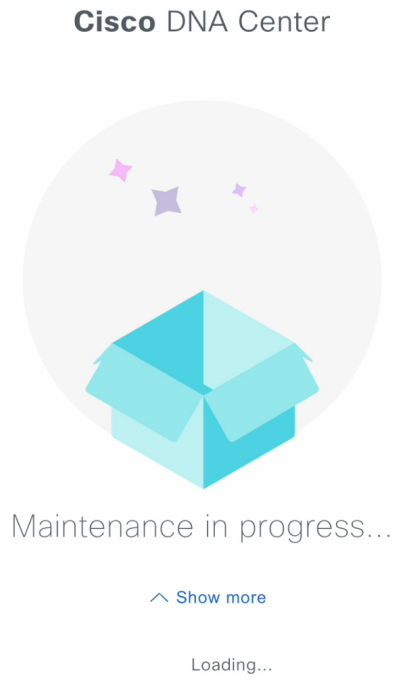


b) Locate the backup in the **Backup & Restore** window's table, click the ellipsis under **Actions** column, and choose **Restore**.

c) Enter the same encryption passphrase that you entered in the preceding step, and click **Restore**.

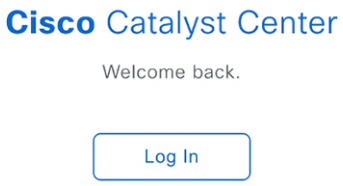


The appliance goes into maintenance mode and starts the restore process.

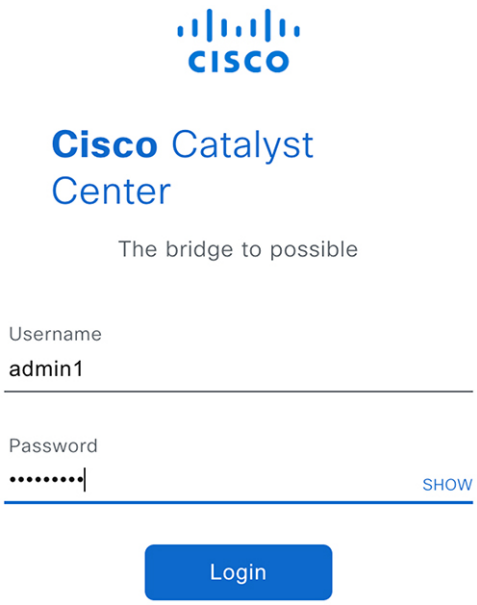


When the restore operation is complete, its status in the **Backup & Restore** window's table changes to `Success`.

d) After the restore operation completes, click **Log In** to log back in to Catalyst Center on ESXi.



e) Enter the admin user's username and password, then click **Login**.



Restore Data from an NFS Server for a Faulty Virtual Appliance

Use this procedure to restore data from an NFS server for a virtual appliance that has failed or is faulty.

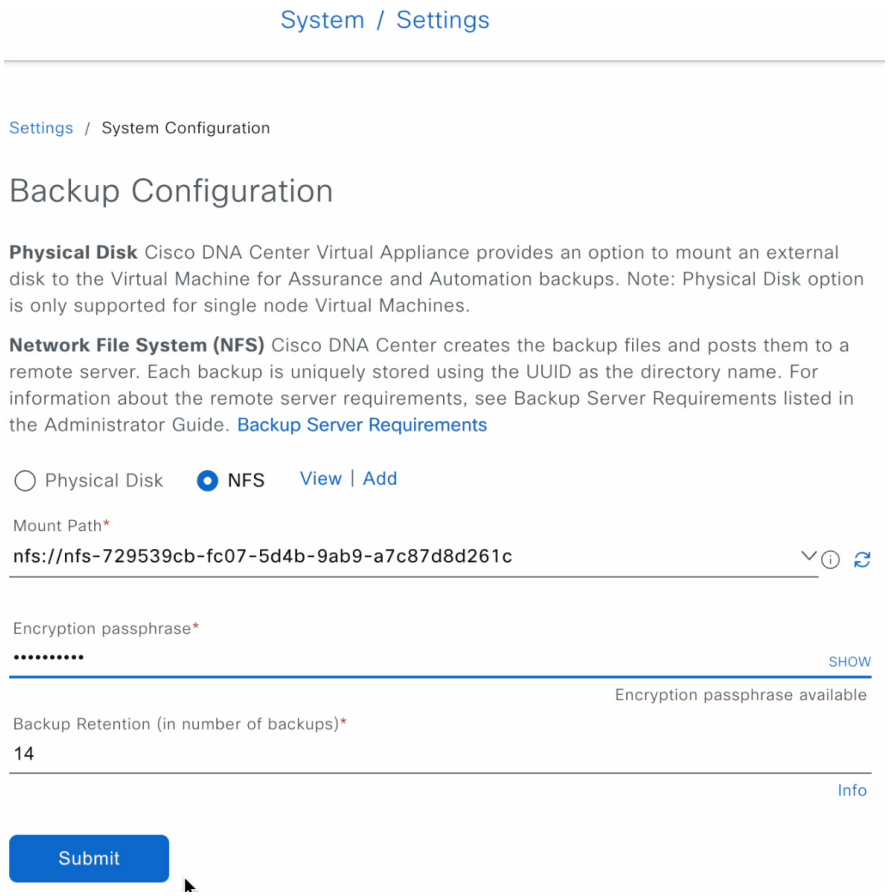
Procedure

Step 1 For your new virtual appliance, do the following to configure Catalyst Center on ESXi to use the NFS server that you configured for the faulty virtual appliance:

a) From the Catalyst Center on ESXi menu, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

b) Click the **NFS** radio button.

c) Choose the NFS server from the **Mount Path** drop-down list.



d) Enter the passphrase that will be used to encrypt the security-sensitive components of the backup (such as certificates and credentials).

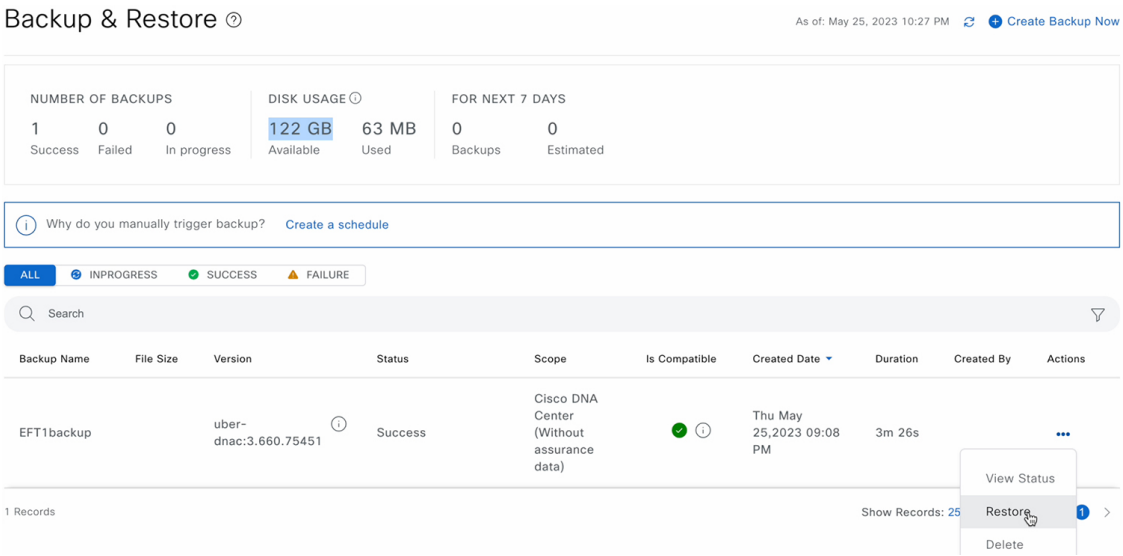
Important Make sure that you don't lose this passphrase. You'll need to enter it later in the succeeding steps and won't be able to restore the backup you're about to create without it.

e) Set how long backup files are kept before they are deleted.

f) Click **Submit**.

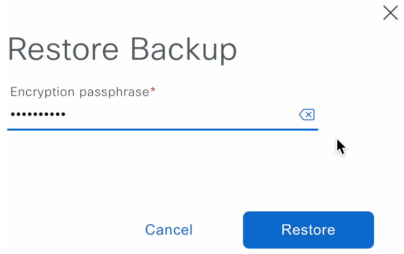
Step 2 To restore the backup, do the following:

a) From the Catalyst Center on ESXi menu, choose **System** > **Backup & Restore**.

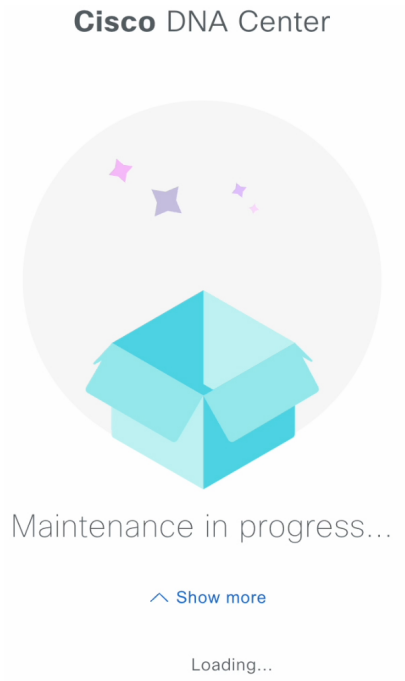


b) Locate the backup in the **Backup & Restore** window's table, click the ellipsis under **Actions** column, and choose **Restore**.

c) Enter the same encryption passphrase that you entered in the preceding step, and click **Restore**.

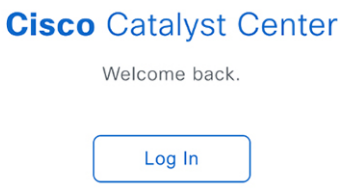


The appliance goes into maintenance mode and starts the restore process.

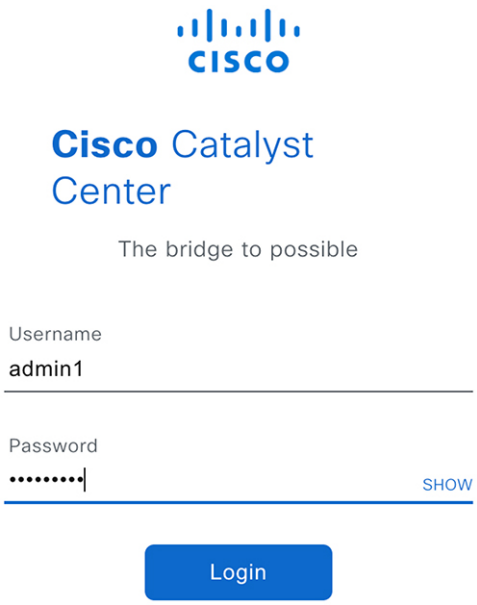


When the restore operation is complete, its status in the **Backup & Restore** window's table changes to `Success`.

d) After the restore operation completes, click **Log In** to log back in to Catalyst Center on ESXi.



e) Enter the admin user's username and password, then click **Login**.



Schedule Data Backup

You can schedule recurring backups and define the day of the week and the time of day when they will occur.

Before you begin

Make sure that the following requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in NFS Backup Server Requirements, on page 131.
- Backup servers have been configured in Catalyst Center. For more information, see Configure the Location to Store Backup Files, on page 139.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Backup & Restore**.
The **Backup & Restore** window is displayed.

Step 2 Click the **Create a Schedule** link.

Note You can schedule a new backup only when there is no backup job in progress.

Step 3 In the **Create Schedule** slide-in pane, do the following:

a. In the **Backup Name** field, enter a unique name for the backup.

b. Choose a schedule option:

- **Schedule Daily**: To schedule the backup job daily, choose the time of the day when you want the backup to occur.

- **Schedule Weekly**: To schedule the backup job weekly, choose the days of the week and time of the day when you want the backup to occur.

c. Define the scope of the backup:

- **Cisco DNA Center (All data)**: This option allows the system administrator to create a backup for automation, Assurance, and system-specific sets.
- **Cisco DNA Center (without Assurance data)**: This option allows the administrator to create a backup for automation and system-specific sets.

d. Click **Save**.

The **Backup & Restore** window displays a banner message that shows the day and time for which the backup is scheduled.

Step 4 (Optional) Click the ellipsis at the end of the banner message to do the following:

a. Click **Edit** to edit the schedule.

b. Click **Upcoming Schedules** to make any changes to the upcoming schedules. If you don't want the backup to occur on a scheduled date and time, in the **Upcoming Schedules** slide-in pane, click the toggle button to disable a particular schedule.

c. Click **Delete** to delete the schedule.

Step 5 After the backup starts, it appears in the **Backup & Restore** window. To view the list of steps executed, click the ellipsis under **Actions** and choose **View Status**.

You can also view the backup status under the **Status** column.

Step 6 In the **Backup & Restore** window, click the **In Progress**, **Success**, or **Failure** tab to filter the list of backups to show only those tasks with a status of In Progress, Success, or Failure.

During the backup process, Catalyst Center creates the backup database and files. The backup files are saved to the specified location. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. The status of the backup job changes from **In Progress** to **Success** when the process is finished.

Note If the backup process fails, there is no impact to the appliance or its database. The most common reason for a failed backup is insufficient disk space. If your backup process fails, make sure that there is sufficient disk space on the remote server and attempt another backup.

View the Status of the Backup and Restore

You can view the success or failure status of backup and restore operations.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Backup & Restore**.
The **Backup & Restore** window is displayed.

Step 2 Under **Actions** for a specific backup, click the ellipsis and choose **View Status**.
The **Task Details** window shows the status and other details.

Manage Applications

Catalyst Center provides many of its functions as individual applications, packaged separately from the core infrastructure. This enables you to install and run the applications that you want and uninstall those you are not using, depending on your preferences.

The number and type of application packages shown in the **Software Management** window vary depending on your Catalyst Center version and your Catalyst Center licensing level. All the application packages that are available to you are shown, whether or not they are currently installed.

Some applications are so basic that they are required on nearly every Catalyst Center deployment. For a description of a package, click the **Currently Installed Applications** link and place your cursor over its name.

Each Catalyst Center application package consists of service bundles, metadata files, and scripts.

Note Perform all application management procedures from the Catalyst Center GUI. Although you can perform many of these procedures using the CLI (after logging in to the shell), we do not recommend this. In particular, if you use the CLI to deploy or upgrade packages, you must ensure that no **deploy** or **upgrade** command is entered unless the results of the **maglev package status** command show all the packages as NOT_DEPLOYED, DEPLOYED, or DEPLOYMENT_ERROR. Any other state indicates that the corresponding activity is in progress, and parallel deployments or upgrades are not supported.

Download the Latest System Version

The **Software Management** window indicates the latest Catalyst Center version available.

Complete the following procedure to download the packages for the latest system version.

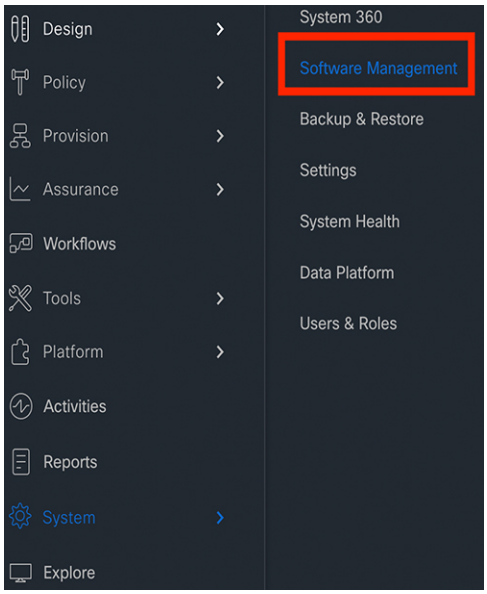
Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

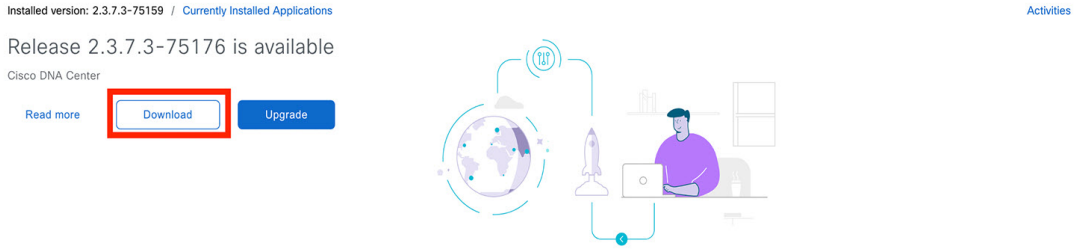
Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

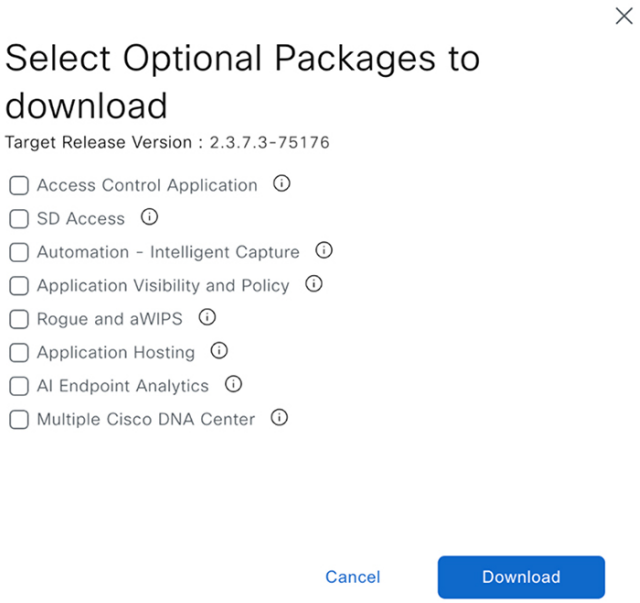
Note At this point, Catalyst Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window doesn’t display a system update that's currently available.



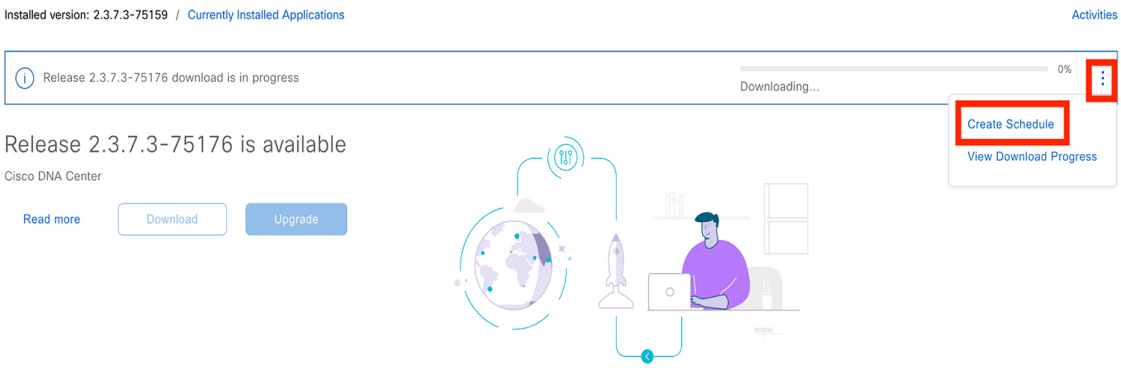
Step 2 If the window indicates that a system update is available, click **Download** to download the system update.



Step 3 Check the check box for the optional packages you want to install, then click **Download**.

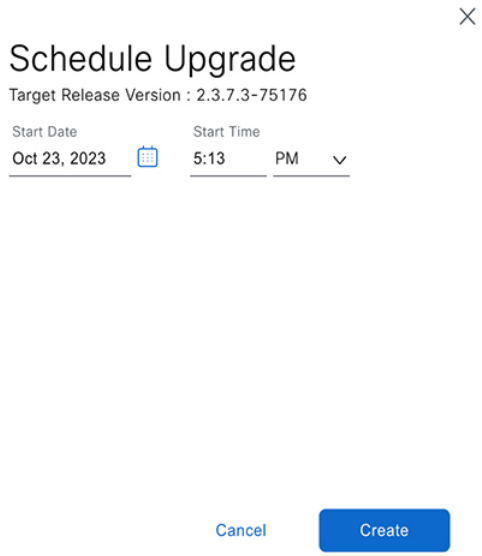


A download progress bar is displayed at the top of the **Software Management** window.

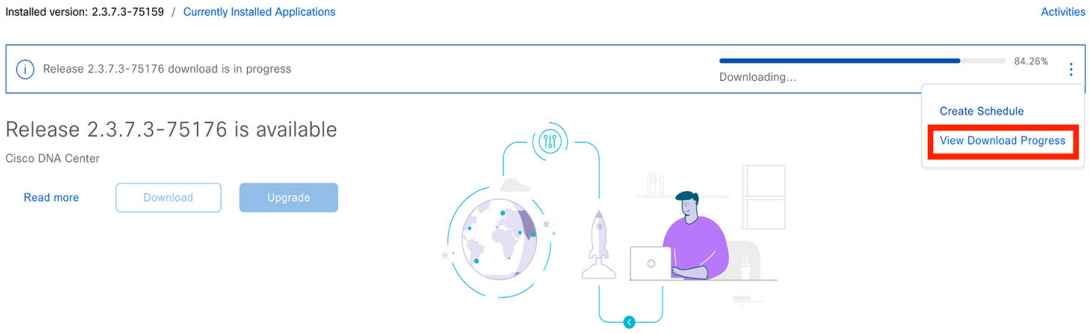


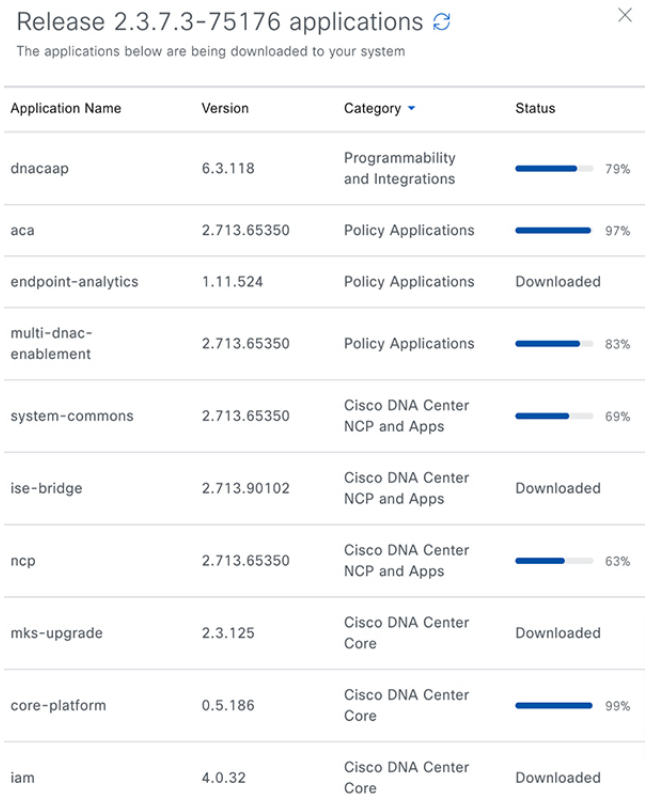
Step 4 Hover your cursor over the ellipsis to the right of the progress bar to access the following options:

- **Create Schedule**: Choose this option to schedule the date and time an upgrade should take place. Schedule the upgrade, then click **Create**.



- **View Download Progress**: Choose this option to view the progress of the packages that are being downloaded.





Upgrade to the Latest System Version

The **Software Management** window indicates the latest Catalyst Center version available.

Complete the following procedure to upgrade to the latest system version.

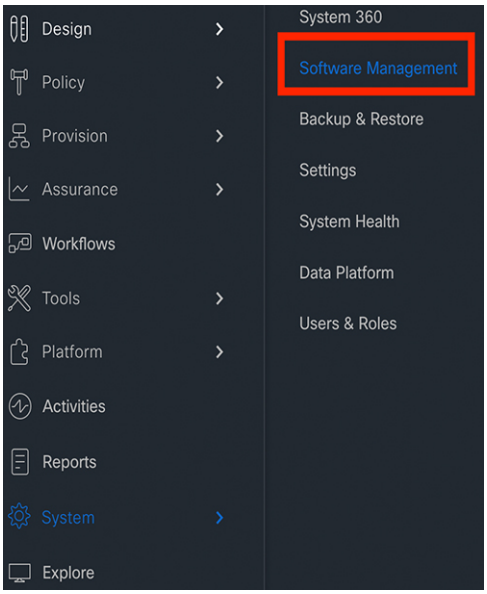
Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

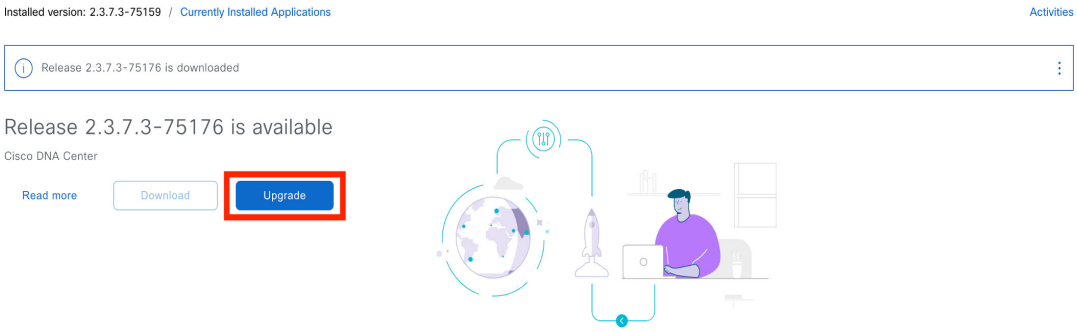
Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Note At this point, Catalyst Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window doesn’t display a system update that's currently available.

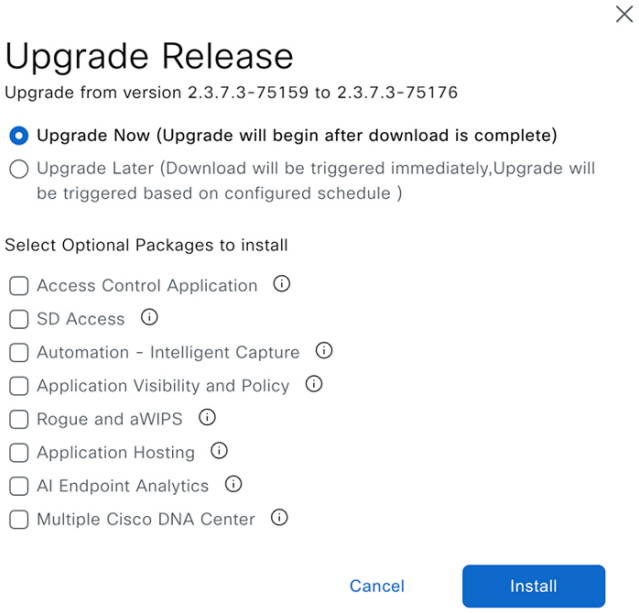


Step 2 If the window indicates that a system update is available, click **Upgrade**.



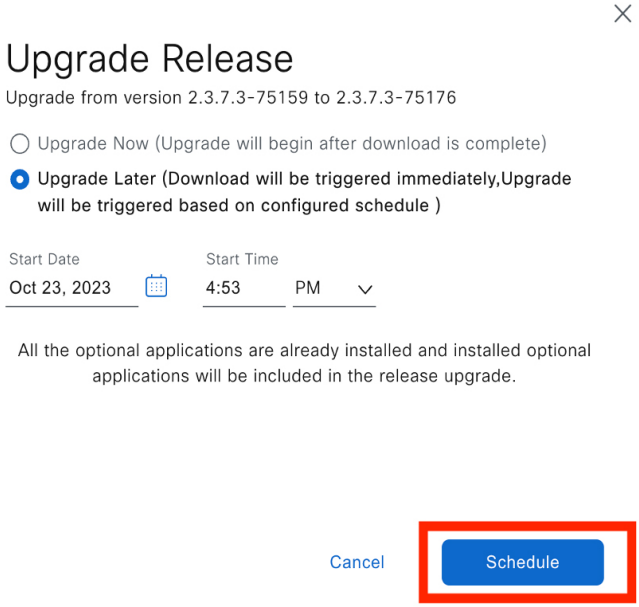
Step 3 Do one of the following in the **Upgrade Release** dialog box:

- Click the **Upgrade Now** radio button, check the check boxes for the optional packages you want to upgrade, and then click **Install**.



The packages for the latest release are downloaded. After the download completes, the upgrade begins automatically.

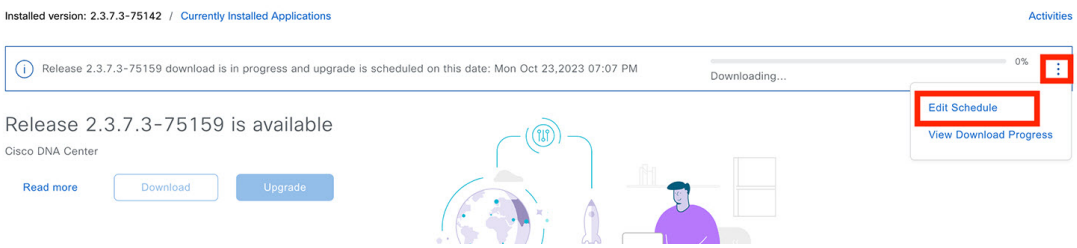
- Click the **Upgrade Later** radio button, set the date and time you want the upgrade to begin, and then click **Schedule**.



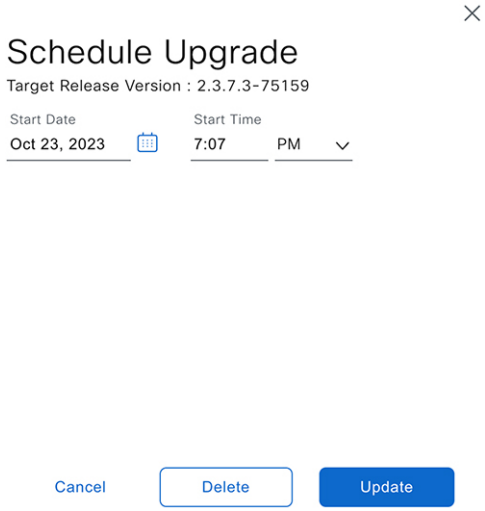
The download of packages for the latest release starts immediately. A progress bar is displayed at the top of the **Software Management** window.

Step 4 Hover your cursor over the ellipsis to the right of the progress bar to access the following options:

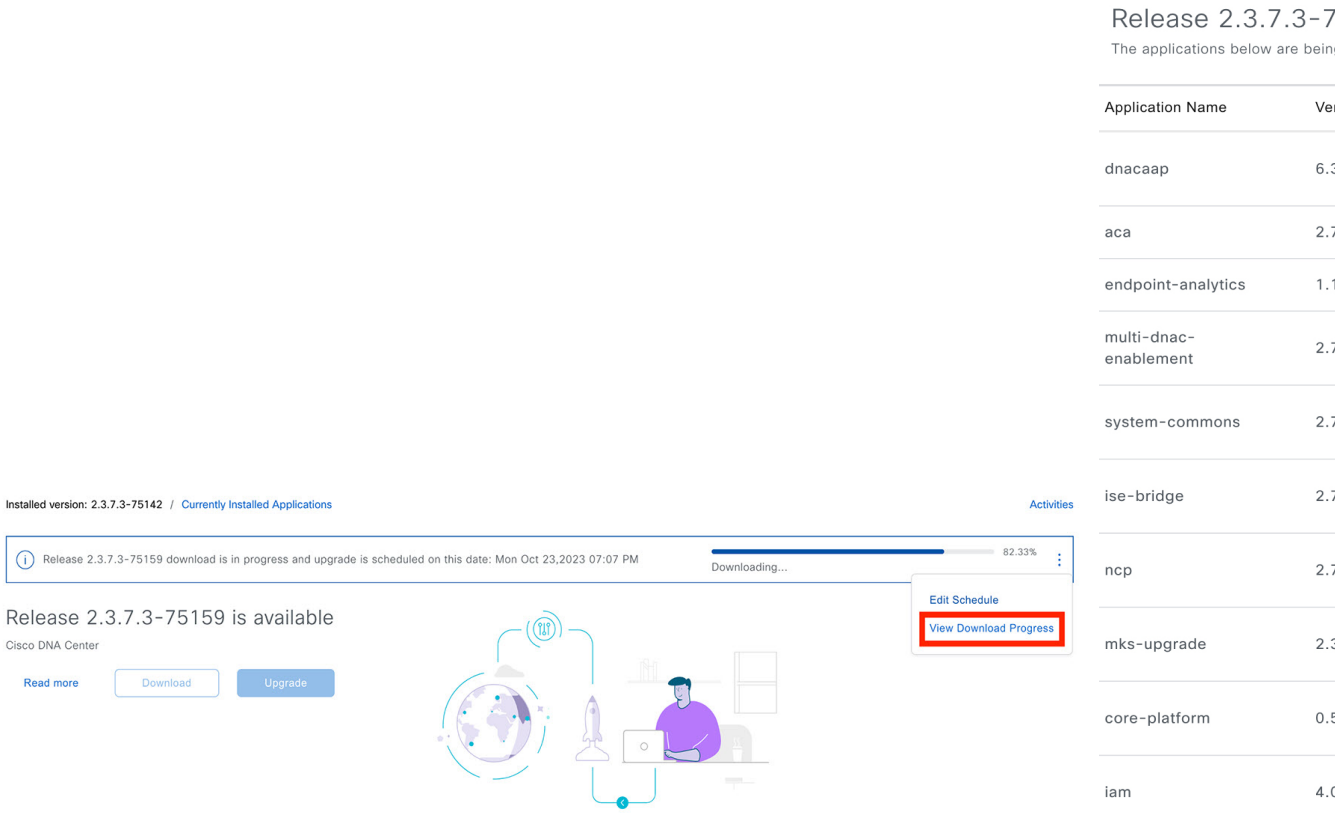
- To configure another start date and time for the upgrade, click **Edit Schedule**.



In the **Schedule Upgrade** dialog box, set the new start date and time, then click **Update**.



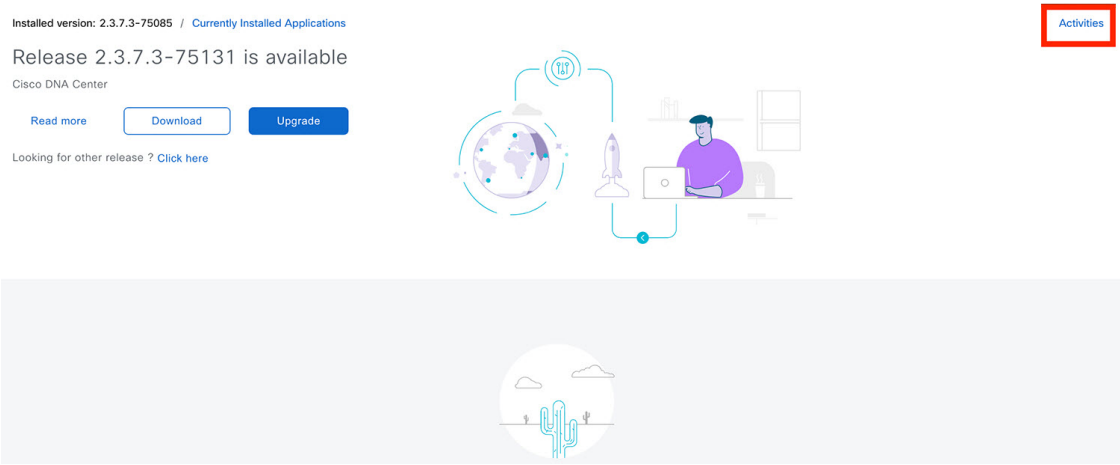
- To view the progress of the packages that are being downloaded, click **View Download Progress**.



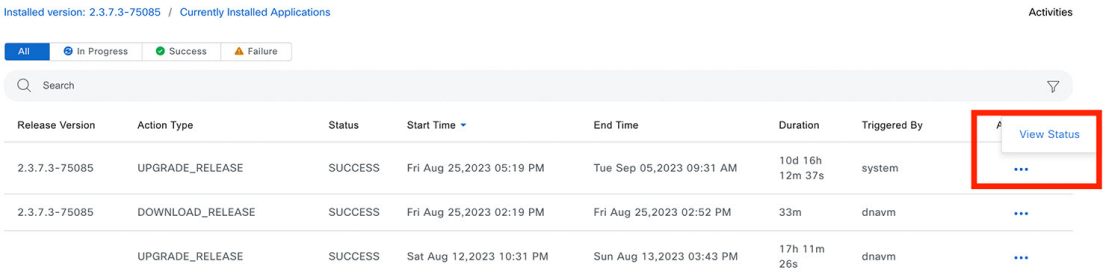
Note Catalyst Center enters Maintenance mode during the upgrade, and remains unavailable while the system update takes place. After the update completes, log back in to Catalyst Center.

After the system upgrade is complete, a message at the top of the window indicates that your system is up to date.

Step 5 In the **Software Management** window, click **Activities** to view a list of changes made to the system. You can view the system upgrade or download details, the applications installed or uninstalled, and a timestamp of the activity.



Step 6 Under the **Actions** column, click the ellipsis to view the tasks that occurred during the execution of the activity.



Download and Install the Latest System Version in Air Gap Mode

The system upgrade is completed by connecting to the internet and using the online update process. However, in some cases, the upgrade is maintained strictly within internal networks (that is, within an air-gapped environment). This upgrade may be necessary to support additional security or regulatory requirements.

Note With the Air Gap mode enabled, you can do the following:

- Communicate with only private IP subnets.
- Add IP address ranges to pass through the air-gapped environment by using the provided API.
- Switch between Air Gap mode and Cloud mode.

Before you begin

Air Gap mode must be enabled on the cluster. For information about how to enable Air Gap mode, see the *Cisco Catalyst Center Air Gap Deployment Guide*.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Step 2 Access the air gap directory on the restricted shell and copy the air gap tarball from the predetermined location using the following SCP command:

```
scp -P 2222 <airgap tar file> maglev@<cluster_ip>:airgap/
```

If it is a three-node cluster, you can copy the file to any node.

Step 3 In the top-right corner of the **Software Management** window, click **Scan** to view the latest available software release.

Step 4 To download the files and schedule the upgrade for a later time, do the following:

a) Click **PreLoad**.

b) In the **Schedule Upgrade** dialog box, schedule the system upgrade and click **PreLoad**.

On the successful submission, a banner message at the top of the window displays the scheduled date and time of the system upgrade.

c) Click the ellipsis at the end of the banner message to edit or delete the scheduled system upgrade. You can also choose to upgrade the schedule immediately.

Step 5 To download the latest version and upgrade the system immediately, do the following:

a) Click **Upgrade**.

b) In the dialog box, from the listed available package applications, check the check box next to application to install the application.

c) Click **Install**.

Note Catalyst Center enters maintenance mode during the upgrade and remains unavailable while the system update takes place.

After the system upgrade is complete, a message at the top of the window indicates that your system is up to date.

Note

- If the system can connect to the external cloud when the air gap mode is enabled, use the following command to verify the network policy:

```
sudo calicoctl get gnp allow-outbound-external -o yaml
```

- Use the following command to verify if ALM has network mode as air gap:

```
kubectl get pods -n maglev-control-plane alm-agent-8469679dfb-nvkxk -o yaml | grep -A1
 NETWORK_MODE
```

Note The above command can only be run from a full shell (_shell and consent token).

- Use the following command to get the scan status and logs:

```
kubectl get pods -n maglev-control-plane | grep ef-airgap-seed
```

- Use the following command to get the preload status and logs:

```
kubectl get pods -n maglev-control-plane | grep ef-airgap-scan
```

Download and Install Application Updates

Catalyst Center treats individual applications as separate from the core infrastructure. Specifically, individual packages for applications can be installed to run on Catalyst Center.

Packages for applications may take time to install and deploy. Therefore, install the packages during a maintenance period for your network.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

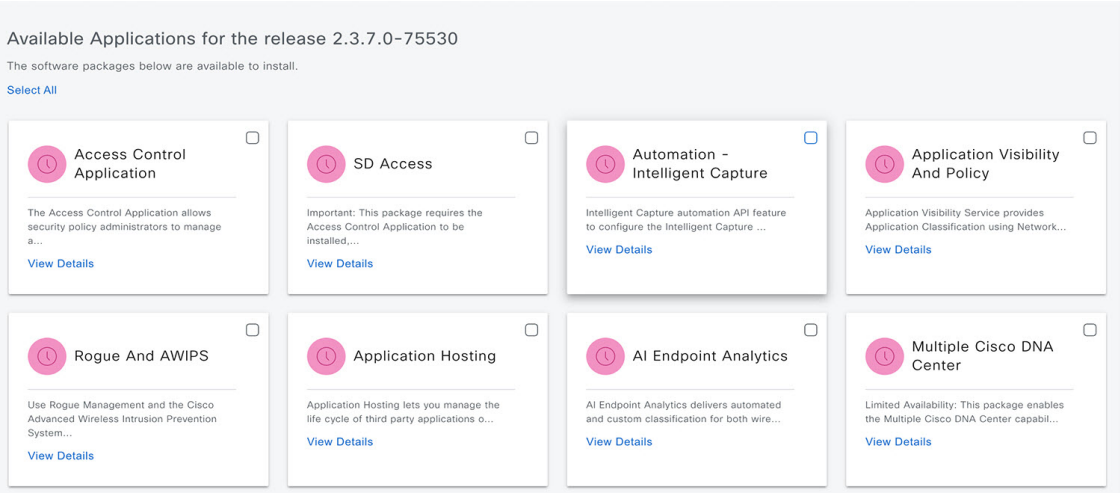
Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Note At this point, Catalyst Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window doesn't display the application updates that are currently available.

Step 2 If any application updates are available, they are displayed at the bottom of the window. Do one of the following:

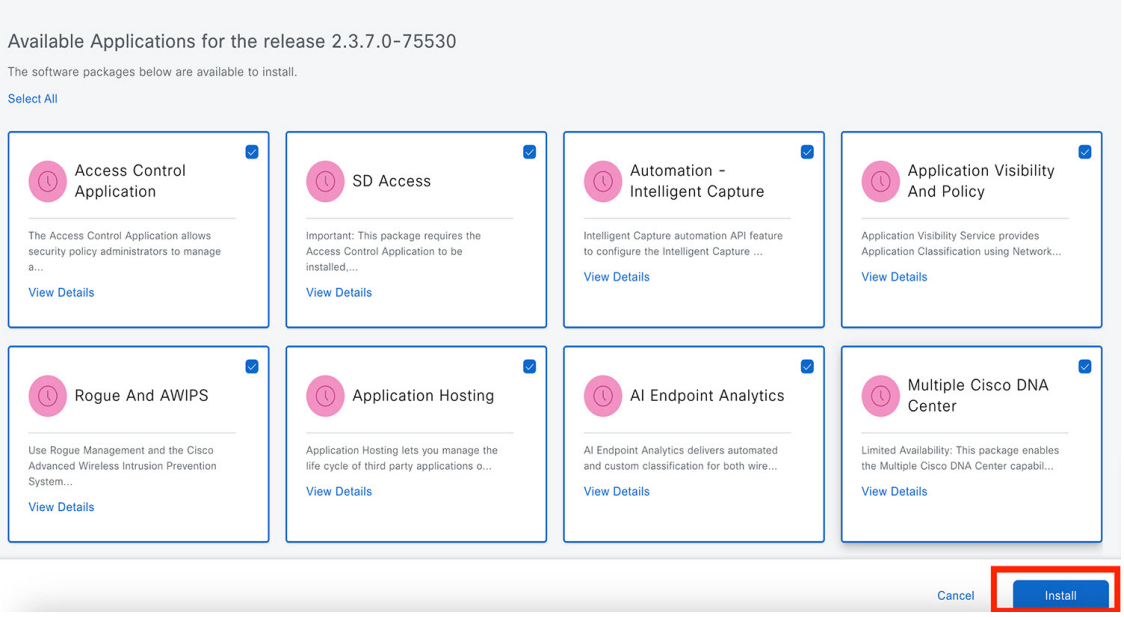
a. To install all the available application updates, click the **Select All** link.

b. To install individual application updates, check the appropriate check boxes.



Step 3 Click **Install**.

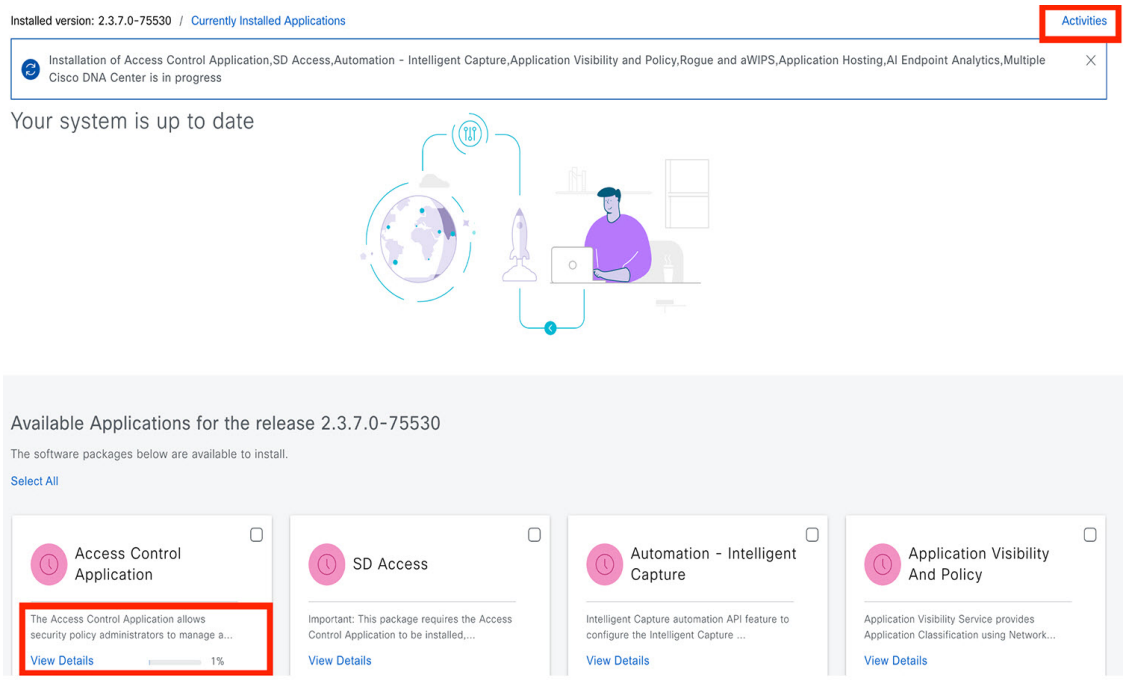
Note During installation, dependencies are checked and installed automatically.



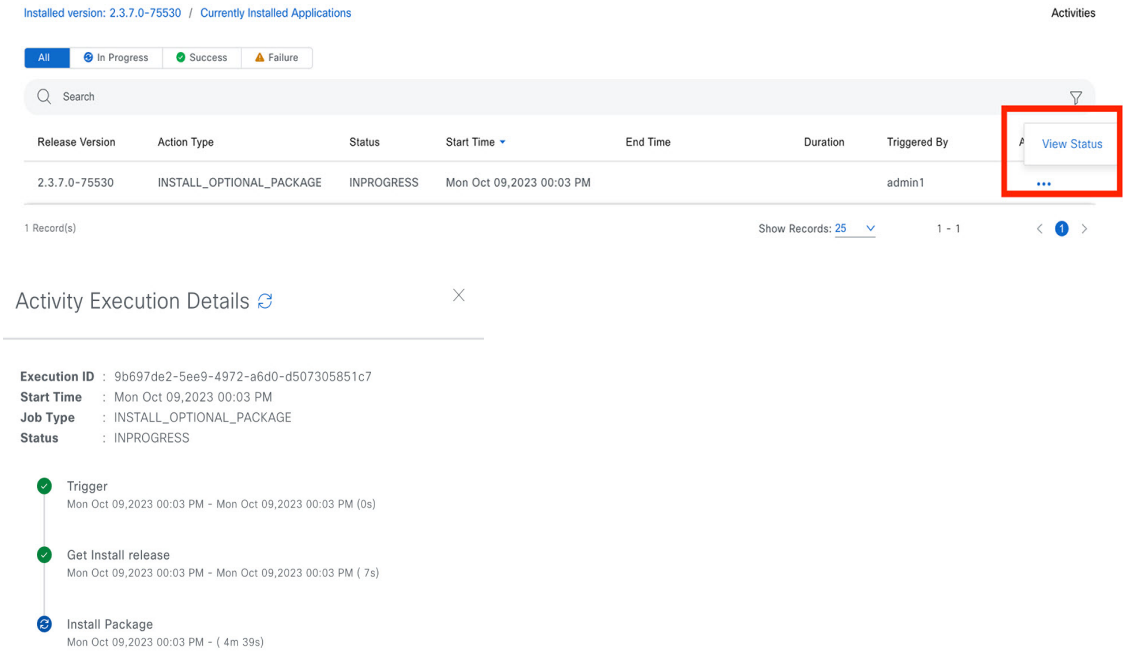
The window displays a progress bar for each application that's being updated.

Step 4 Click the **Currently Installed Applications** link and confirm that the applications you selected have been updated.

Step 5 In the **Software Management** window, click **Activities** to view a list of changes made to the system. You can view the system upgrade or download details, the applications installed or uninstalled, and a timestamp of the activity.



Step 6 Under the **Actions** column, click the ellipsis to view the tasks that occurred during the execution of the activity.



Uninstall an Application

Catalyst Center treats individual applications as separate from the core infrastructure. Specifically, individual packages for applications can be uninstalled from Catalyst Center.

You can uninstall only packages for applications that are not system critical.

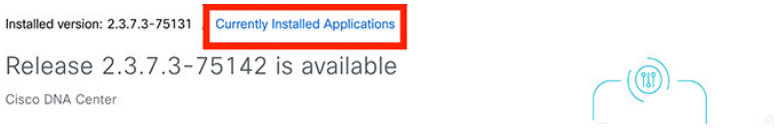
Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

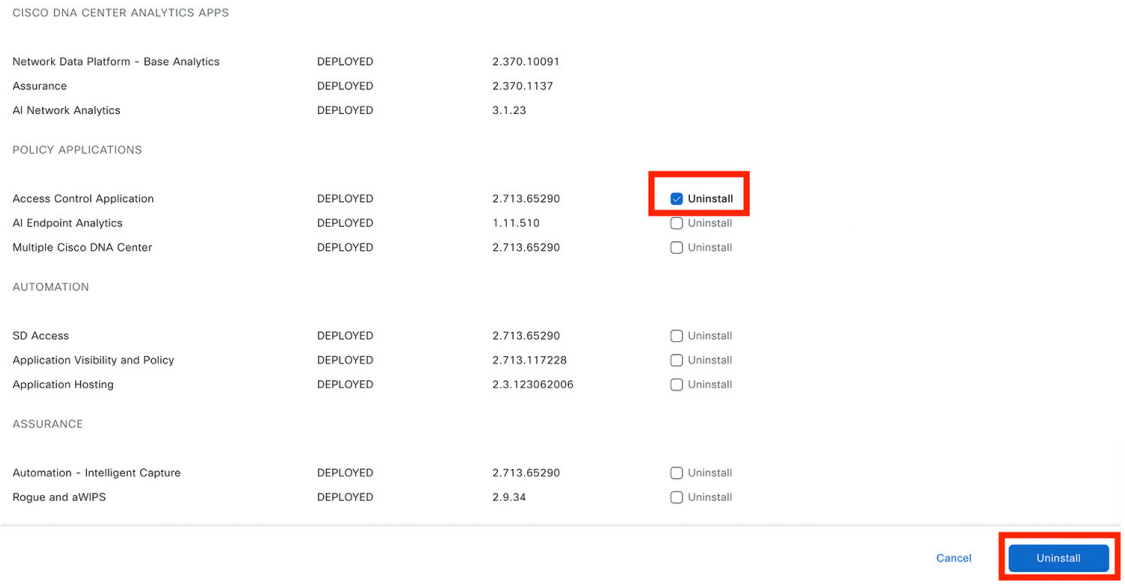
Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Step 2 Click the **Currently Installed Applications** link to view all the applications that are installed on your Catalyst Center appliance.



Step 3 Check the package you want to remove and click **Uninstall**.

Note
- You can uninstall multiple packages simultaneously.
- You can uninstall only the optional packages.



Catalyst Center displays a message after the application has been removed.

Manage Users

A user profile defines the login, password, and role (permissions) of a user.

You can configure both internal and external profiles for users. Internal user profiles reside in Catalyst Center, and external user profiles reside on an external AAA server.

A default user profile with SUPER-ADMIN-ROLE permissions is created when you install Catalyst Center.

About User Roles

Users are assigned user roles that specify the functions that they are permitted to perform:

- **Administrator (SUPER-ADMIN-ROLE)**: Users with this role have full access to all of the Catalyst Center functions. They can create other user profiles with various roles, including those with the SUPER-ADMIN-ROLE.
- **Network Administrator (NETWORK-ADMIN-ROLE)**: Users with this role have full access to all of the network-related Catalyst Center functions. However, they do not have access to system-related functions, such as backup and restore.
- **Observer (OBSERVER-ROLE)**: Users with this role have view-only access to the Catalyst Center functions. Users with an observer role cannot access any functions that configure or control Catalyst Center or the devices it manages.

Create an Internal User

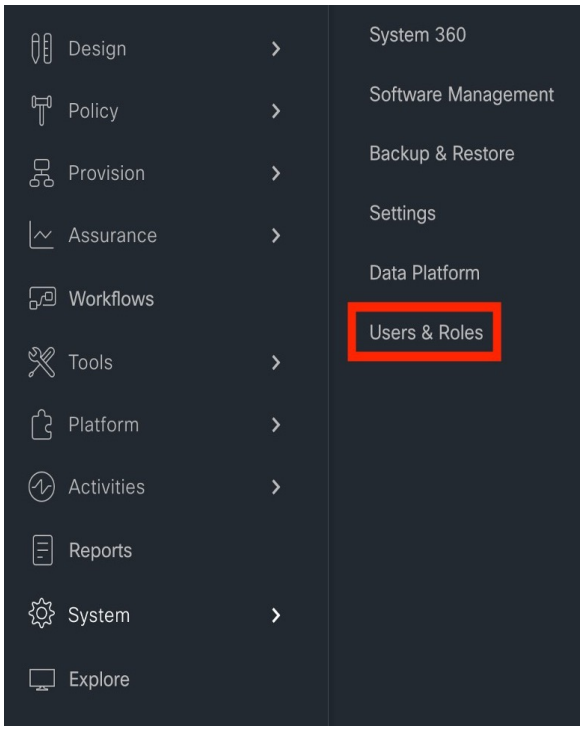
You can create a user and assign this user a role.

Before you begin

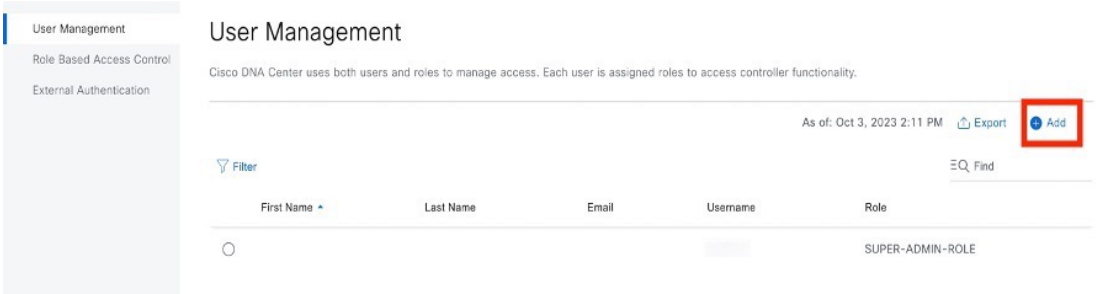
Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **User Management**.

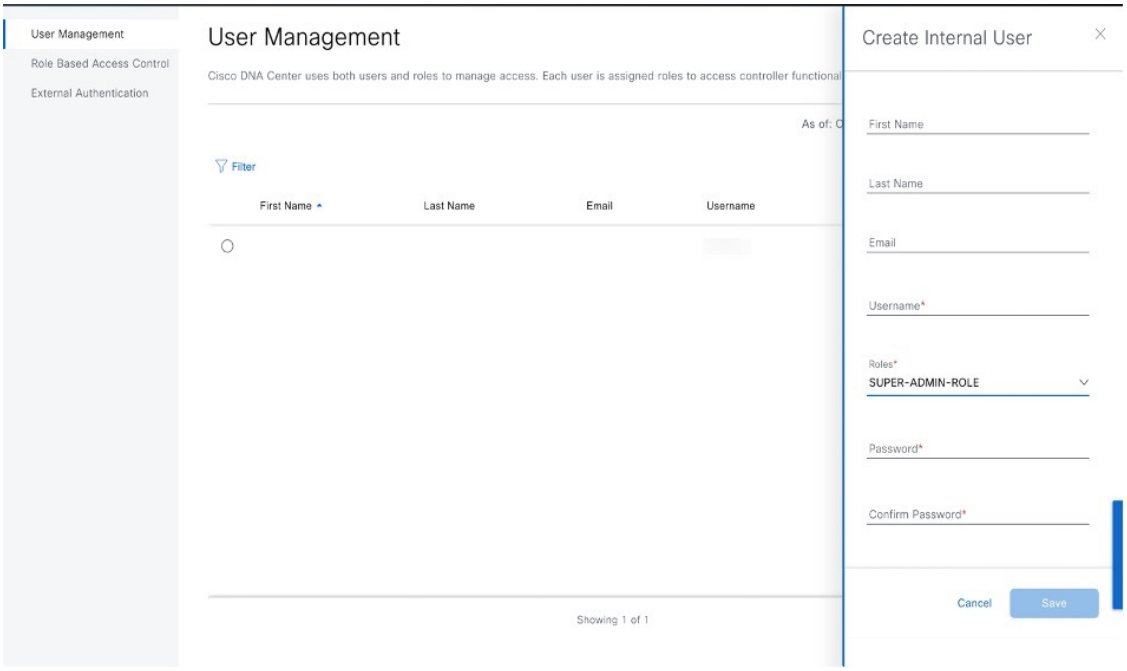


Step 2 Click **Add**.

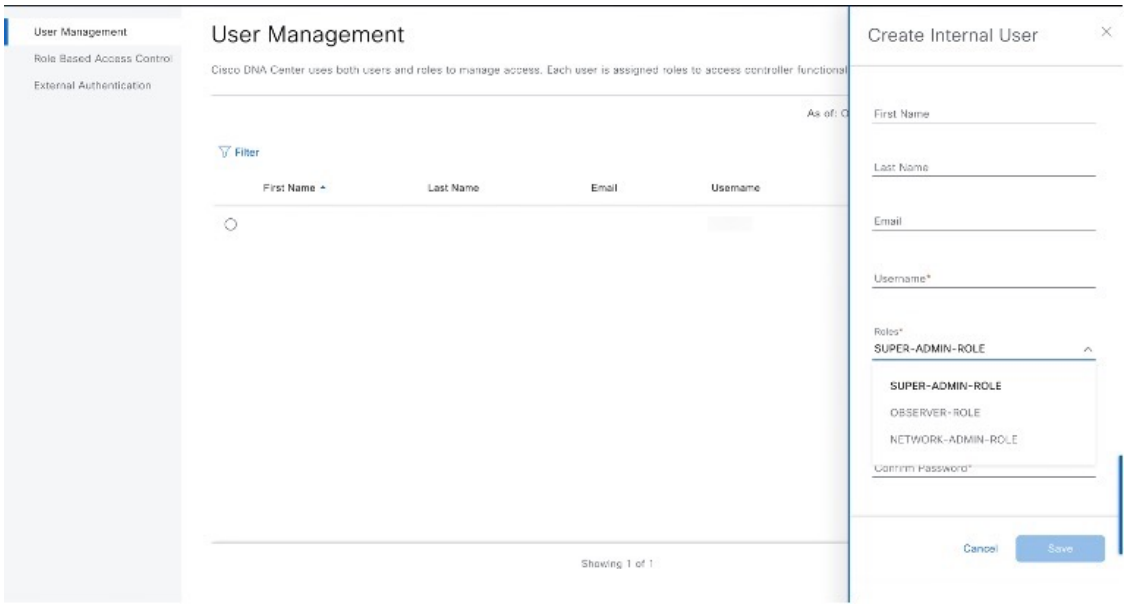


Step 3 Enter a first name, last name, email address, and username for the new user.

The email address must meet the requirements for the standard Apache EmailValidator class.



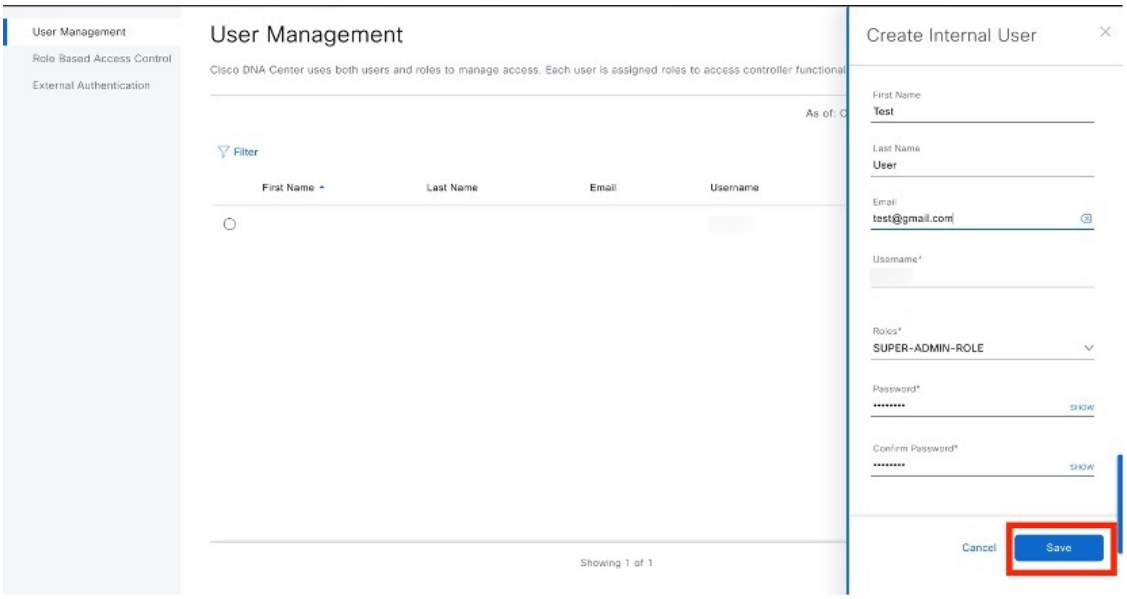
Step 4 Under **Role List**, choose one of the following roles: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.



Step 5 Enter a password and confirm it. The password must contain:

- At least eight characters
- A character from at least three of the following categories:
  - Lowercase letter
  - Uppercase letter
  - Number
  - Special character

Step 6 Click **Save**.



Edit a User

You can edit some user properties (but not the username).

Before you begin

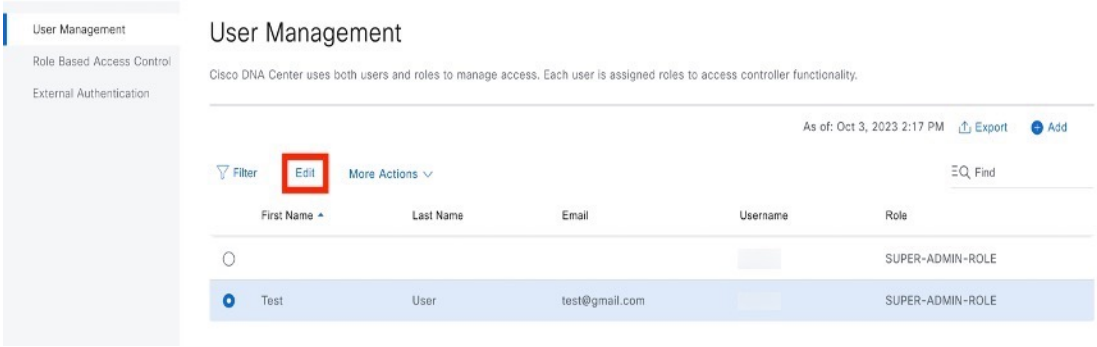
Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to edit.

Step 3 Click **Edit**.



Step 4 Edit the first or last name or email address, if needed.

Step 5 Under **Role List**, choose a new role, if needed: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.

Step 6 Click **Save**.

Delete a User

Before you begin

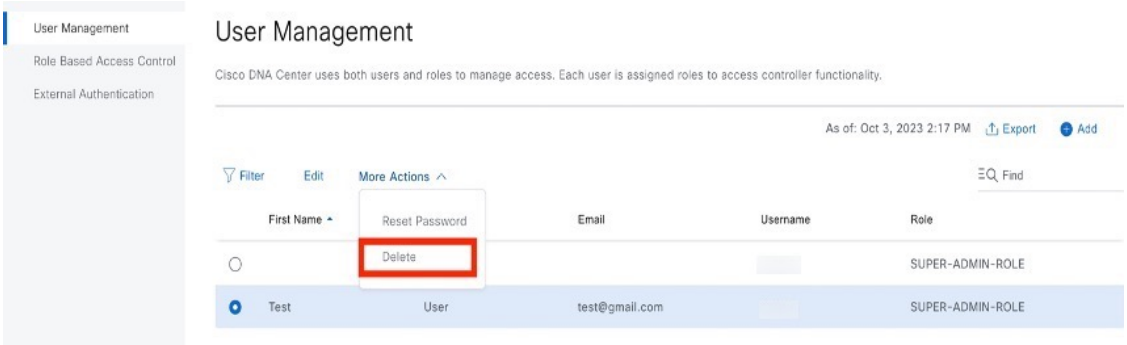
Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to delete.

Step 3 Click **Delete**.



Step 4 At the confirmation prompt, click **Continue**.

Reset a User Password

You can reset another user's password.

For security reasons, passwords are not displayed to any user, not even to the users with administrator privileges.

Before you begin

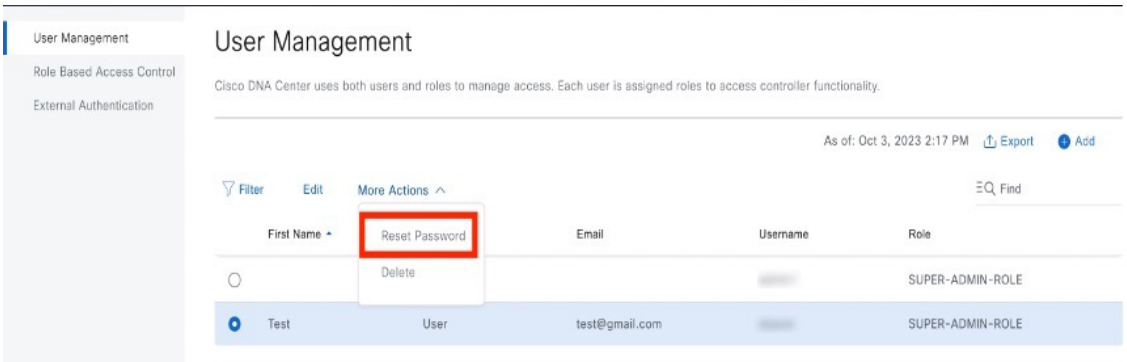
Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user whose password you want to reset.

Step 3 From the **More Actions** drop-down list, click **Reset Password**.



Step 4 Enter a new password and confirm it. The new password must contain:

- At least eight characters
- A character from at least three of the following categories:
  - Lowercase letter
  - Uppercase letter
  - Number
  - Special character

Step 5 Click **Save**.

Change Your Own User Password

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **Change Password**.

Step 2 Enter information in the required fields.

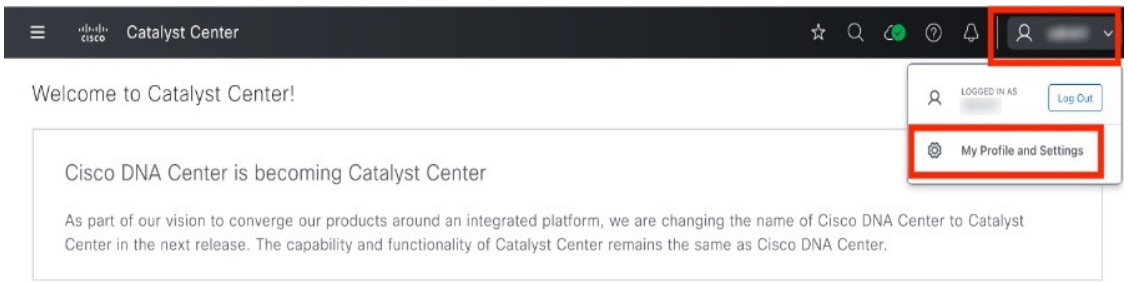
Step 3 Click **Update**.

Change Your Own User Password Without Admin Permission

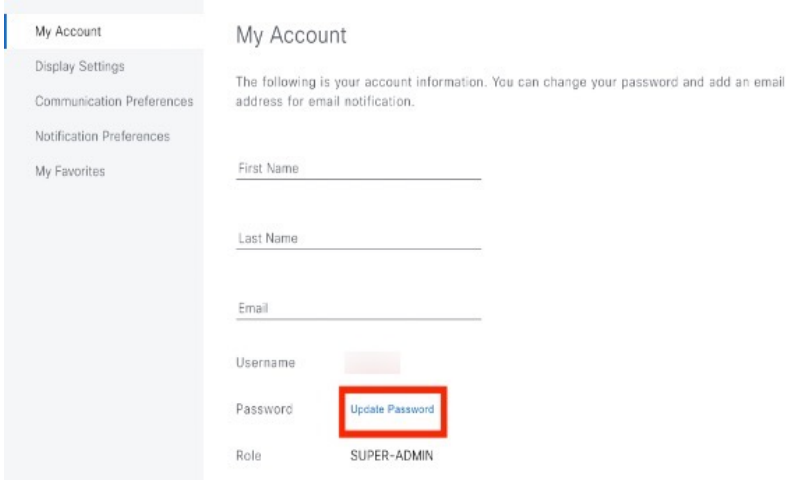
The following procedure describes how to change your password without admin permission.

Procedure

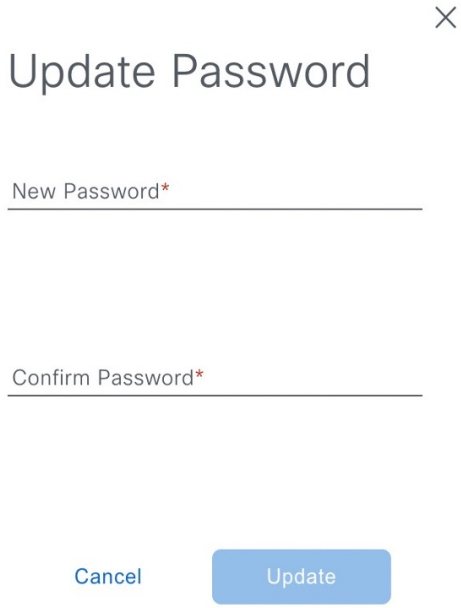
Step 1 From the top-right corner, click your displayed username and choose **My Profile and Settings** > **My Account**.



Step 2 In the **Password** field, click **Update Password**.



Step 3 In the **Update Password** dialog box, enter the new password and confirm the new password.



Step 4 Click **Update**.

Reset a Forgotten Password

If you forgot your password, contact the Cisco Technical Assistance Center (TAC) to reset it.

Configure Role-Based Access Control

Catalyst Center supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict user access to certain Catalyst Center functions.

Use this procedure to define a custom role and then assign a user to that role.

Before you begin

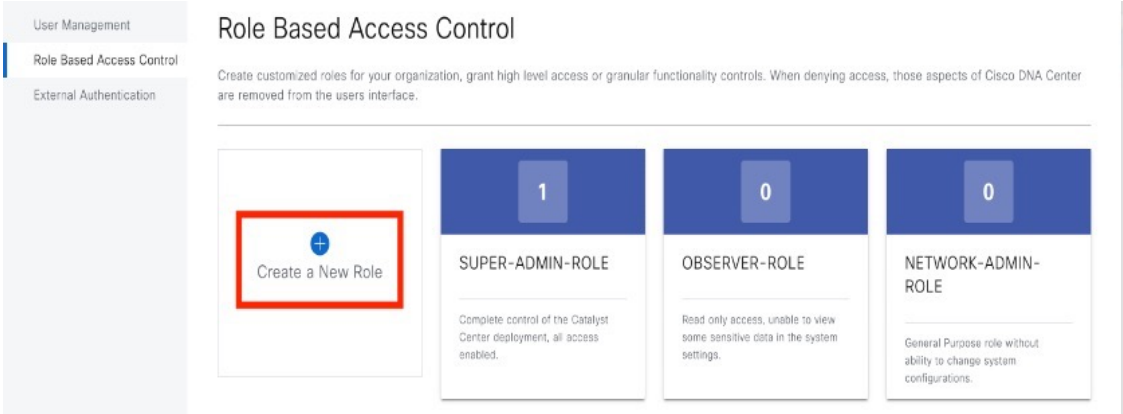
Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

Step 1 Define a custom role.

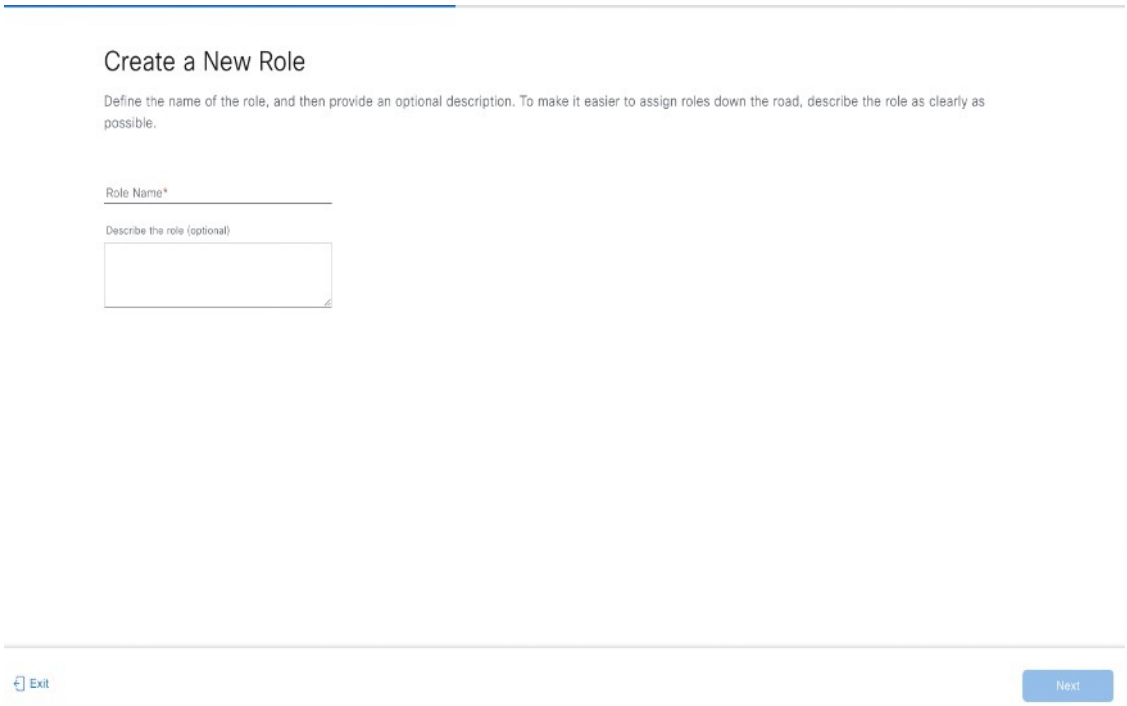
a) From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **Role Based Access Control**.

b) Click **Create a New Role**.

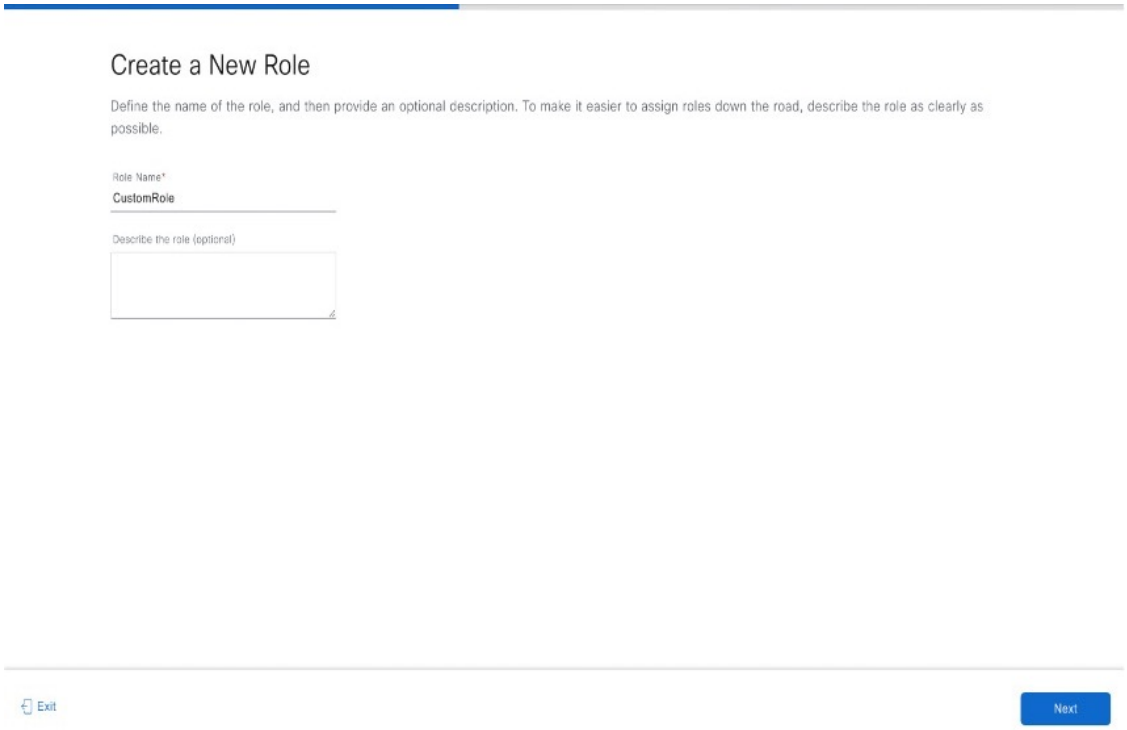


The **Create a Role** window appears. If this is your first iteration of RBAC, after you have created the new role, you will be asked to assign users to the new role.

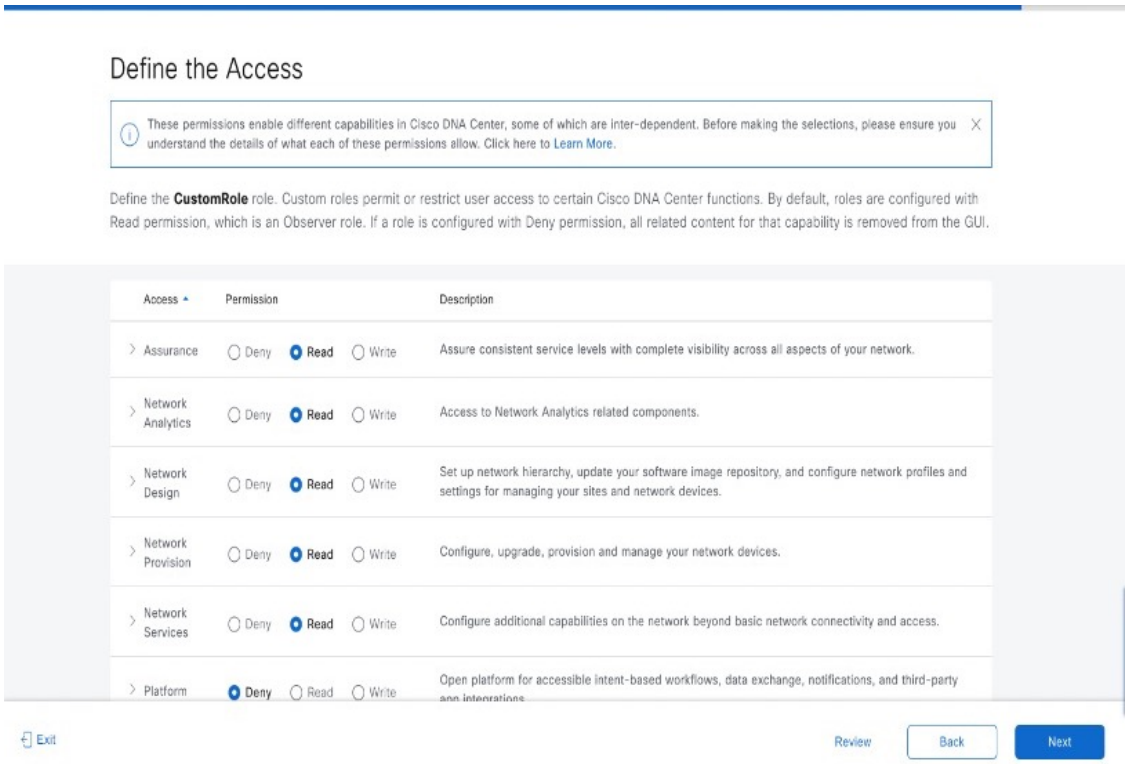
c) If a task overview window opens, click **Let's do it** to go directly to the workflow.
The **Create a New Role** window opens.



d) Enter a name for the role and then click **Next**.



The **Define the Access** window opens with a list of options. By default, the observer role is set for all Catalyst Center functions.

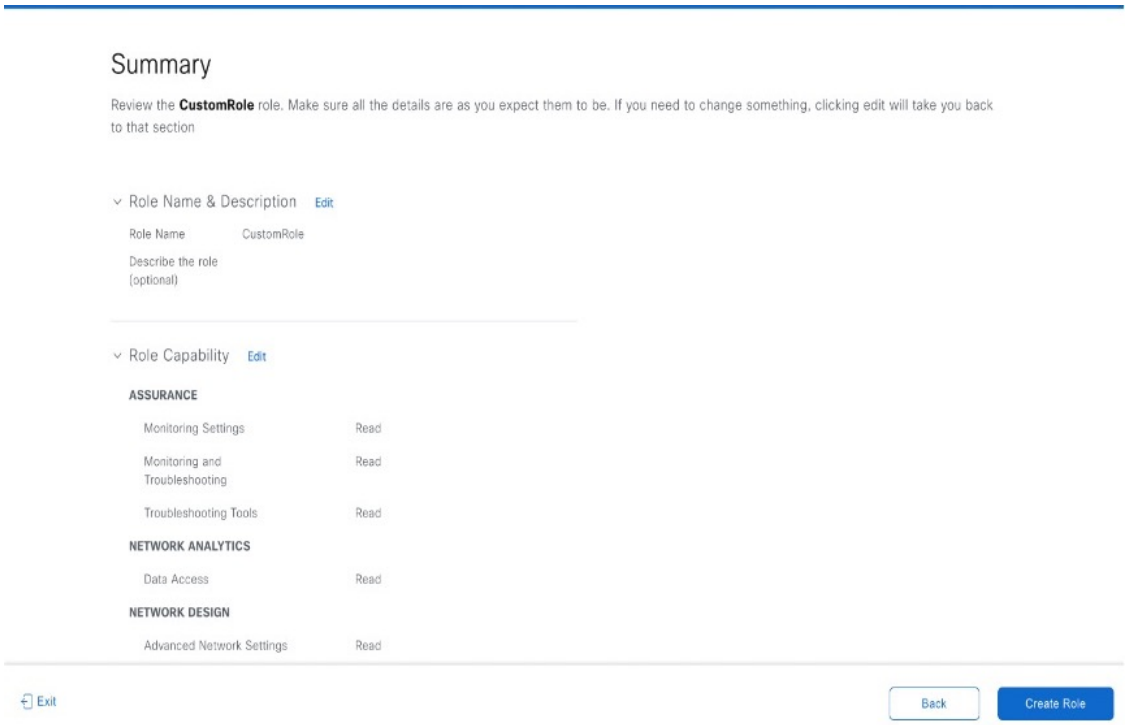


e) Click the > icon corresponding to the desired function to view the associated features.

f) Set the permission level to **Deny**, **Read**, or **Write** for the desired features.

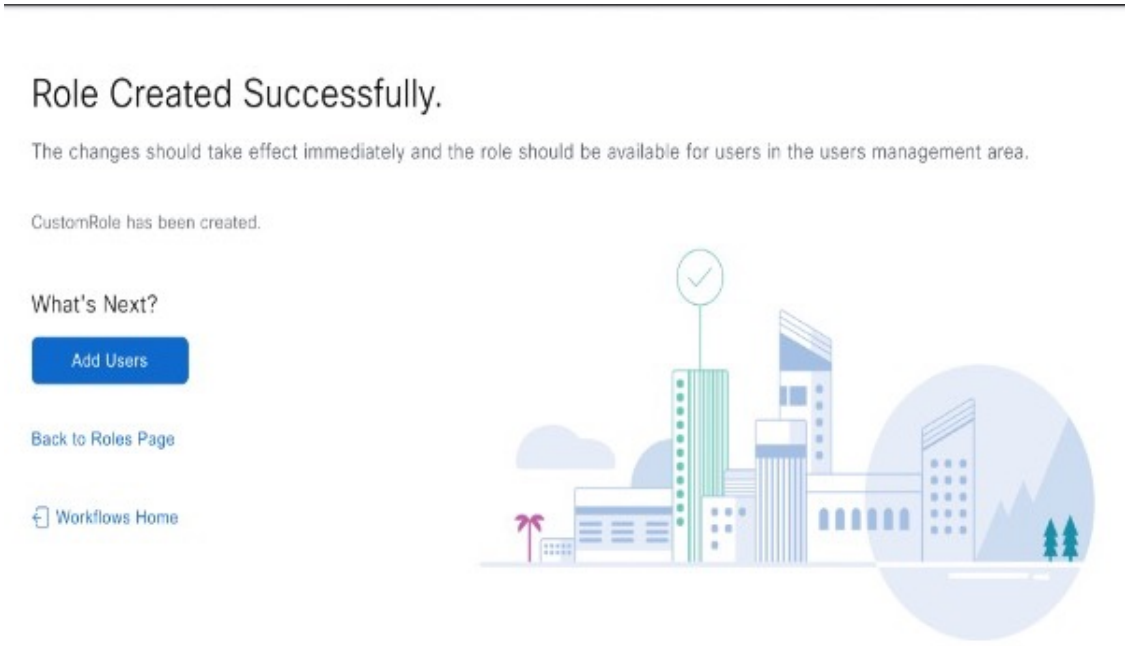
If you set the permission level of a feature to **Deny**, the user to whom you assign this role cannot view this feature in the GUI.

g) Click **Next**.
The **Summary** window opens.



h) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**. If you click **Edit**, the **Role-Name** window opens.

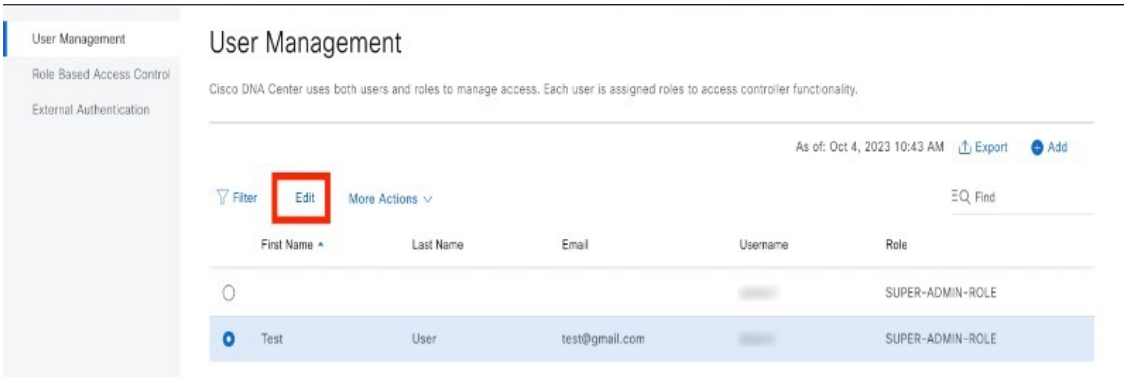
Step 2 To assign a user to the custom role you just created, click **Add Users**.



The **User Management** window opens, which allows you to assign the custom role to an existing user or to a new user.

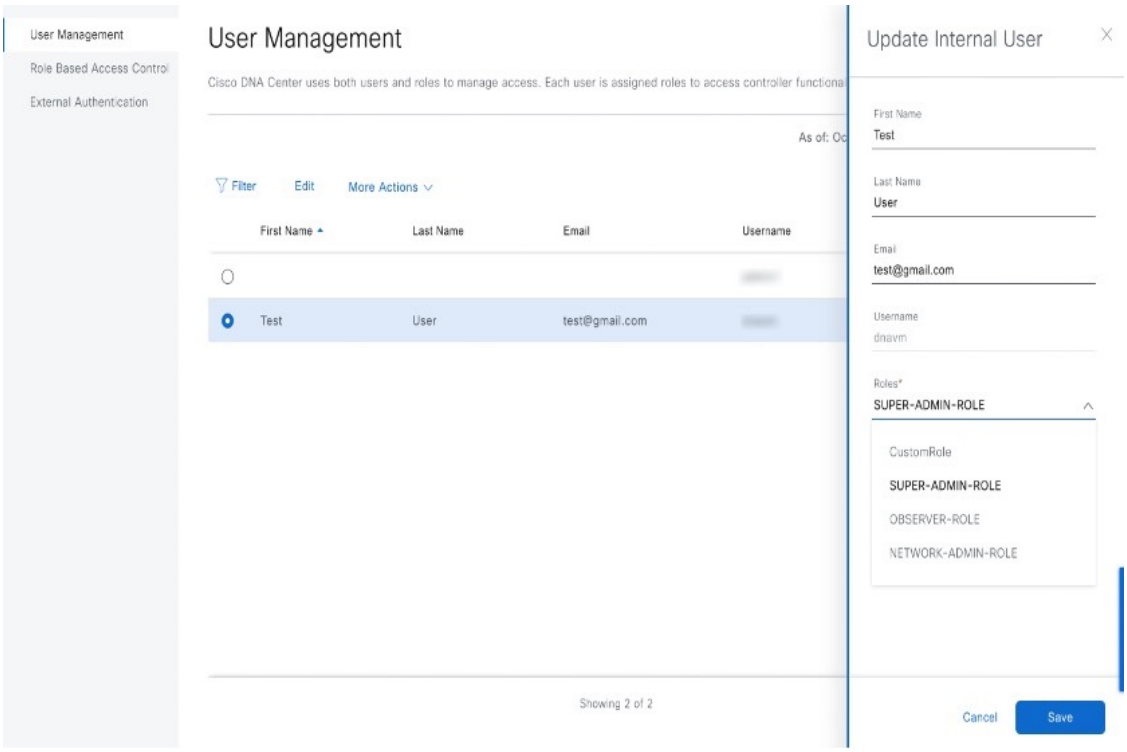
- To assign the custom role to an existing user, do the following:

  a. In the **Internal Users** window, click the radio button next to the user to whom you want to assign the custom role, and then click **Edit**.



  The **Update Internal User** slide-in pane opens.

  b. From the **Roles** drop-down list, choose the custom role, and then click **Save**.



- To assign the custom role to a new user, do the following:

  a. Click **Add**.

  The **Create Internal User** slide-in pane opens.

  b. Enter the first name, last name, and username in the fields provided.

  c. From the **Roles** drop-down list, choose the custom role to assign to the new user.

d. Enter the password and then confirm it.

e. Click **Save**.

Step 3 If you are an existing user who was logged in when the administrator was updating your access permissions, you must log out of Catalyst Center and then log back in for the new permission settings to take effect.

Catalyst Center User Role Permissions

Table 4: Catalyst Center User Role Permissions

Capability	Description
Assurance	Assure consistent service levels with complete visibility across all aspects of your network.
Monitoring and Troubleshooting	Monitor and manage the health of your network with issue troubleshooting and remediation, proactive network monitoring, and insights driven by AI Network Analytics. This role lets you: • Resolve, close, and ignore issues. • Run Machine Reasoning Engine (MRE) workflows. • Analyze trends and insights. • Troubleshoot issues, including path trace, sensor dashboards, and rogue management. • Run workflows for rogue and Cisco Advanced Wireless Intrusion Prevention System (aWIPS). These workflows include AP-allowed list, vendor-allowed list, aWIPS profile creation, assigning an aWIPS profile, and so on.
Monitoring Settings	Configure and manage issues. Update network, client, and application health thresholds. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.
Troubleshooting Tools	Create and manage sensor tests. Schedule on-demand forensic packet captures (Intelligent Capture) for troubleshooting clients. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.
Network Analytics	Manage network analytics-related components.
Data Access	Enable access to query engine APIs. Control functions such as global search, rogue management, and aWIPS. Note: Setting the permission to Deny affects Search and Assurance functionality.
Network Design	Set up the network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.

Capability	Description
Advanced Network Settings	• Update network settings, such as global device credentials, authentication and policy servers, certificates, trusted certificates, cloud access keys, Stealthwatch, Umbrella, and data anonymization. • Export the device inventory and its credentials. Note: To complete this task, you must have Write permission on **Network Settings**.
Image Repository	Manage software images and facilitate upgrades and updates on physical and virtual network entities.
Network Hierarchy	Define and create a network hierarchy of sites, buildings, floors, and areas based on geographic location. Users with this role can also add CMX servers in **System** > **Settings**.
Network Profiles	Create network profiles for routing, switching, and wireless. Assign profiles to sites. This role includes CLI Templates, Tagging, Feature Templates, and Authentication Template. Note: To create SSIDs, you must have Write permission on **Network Settings**.
Network Settings	Common site-wide network settings such as AAA, NTP, DHCP, DNS, Syslog, SNMP, and Telemetry. Users with this role can add an SFTP server and modify the Network Resync Interval in **System** > **Settings**. Note: To create wireless profiles, you must have Write permission on **Network Profiles**. To assign a CMX server to a site, building, or floor, you must have Write permission on **Network Hierarchy**.
Virtual Network	Manage virtual networks (VNs). Segment physical networks into multiple logical networks for traffic isolation and controlled inter-VN communication.
Network Provision	Configure, upgrade, provision, and manage your network devices.
Compliance	Manage compliance provisioning.
EoX	Scan the network for details on publicly announced information pertaining to the **End of Life**, **End of Sales**, or **End of Support** of the hardware and software in your network. Note: To view EoX scans, you must have Read permission on **Compliance**. To run EoX scans, you must have Write permission on **Compliance**.
Image Update	Upgrade software images on devices that don't match the Golden Image settings after a complete upgrade lifecycle.
Inventory Management	Discover, add, replace, or delete devices on your network while managing device attributes and configuration properties. Note: To replace a device, you must have Write permission on **Network Provision** > **PnP**.
Inventory Management > Device Configuration	Device Configuration: Display the running configuration of a device.
Inventory Management > Discovery	Discovery: Discover new devices in your network.

Capability	Description
Inventory Management > Network Device	Network Device: Add devices from Inventory, view device details, and perform device-level actions.
	Inventory Insights: Displays device issues, such as Speed/Duplex settings mismatch and VLAN mismatch, and the number of times each issue occurred. Provides detailed actions for users to perform to revolve the issues. Because this information requires action, including possible configuration changes, it is not displayed to users who have a read-only role.
Inventory Management > Port Management	Port Management: Allow port actions on a device.
Inventory Management > Topology	Topology: Display network device and link connectivity. Manage device roles, tag devices, customize the display, and save custom topology layouts. Note: To view the SD-Access Fabric window, you must have at least Read permission on **Network Provision** > **Inventory Management** > **Topology**.
License	Unified view of your software and network assets relative to license usage and compliance. The role also controls permissions for cisco.com, Cisco credentials, device EULA, and Smart accounts.
Network Telemetry	Enable or disable the collection of application telemetry from devices. Deploy related settings, such as site telemetry receivers, wireless service assurance, and controller certificates, to devices. Note: To enable or disable the collection of application telemetry, you must have Write permission on **Provision**.
PnP	Automatically onboard new devices, assign them to sites, and configure them with site-specific contextual settings.
Provision	Provision devices with the site-specific settings and policies that are configured for the network. This role includes Fabric, Application Policy, Application Visibility, Cloud, Site-to-Site VPN, Network/Application Telemetry, Stealthwatch, Sync Start vs Run Configuration, and Umbrella provisioning. On the main dashboards for rogue and aWIPS, you can enable or disable certain actions, including rogue containment. To provision devices, you must have Write permission on **Network Design** and **Network Provision**.
Network Services	Configure additional capabilities on the network beyond basic network connectivity and access.
Application Hosting	Deploy, manage, and monitor virtualized and container-based applications running on network devices.
Bonjour	Enable the Wide Area Bonjour service across your network to enable policy-based service discovery.

Capability	Description
Stealthwatch	Configure network elements to send data to Cisco Stealthwatch to detect and mitigate threats, even in encrypted traffic. To provision Stealthwatch, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Services** > **Stealthwatch** • **Network Design** > **Advanced Settings**
Umbrella	Configure network elements to use Cisco Umbrella as the first line of defense against cybersecurity threats. To provision Umbrella, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Provision** > **Scheduler** • **Network Services** > **Umbrella** You must also have Read permission on **Advanced Network Settings**.
Platform	Open platform for accessible, intent-based workflows, data exchange, notifications, integration settings, and third-party app integrations.
APIs	Drive value by accessing Catalyst Center through REST APIs.
Bundles	Enhance productivity by configuring and activating preconfigured bundles for ITSM integration.
Events	Subscribe to get notified in near real time about network and system events of interest and initiate corrective actions. You can configure email and syslog logs in **System** > **Settings** > **Destinations**.
Reports	Generate reports using predefined reporting templates for all aspects of your network. Generate reports for rogue devices and for aWIPS. You can configure webhooks in **System** > **Settings** > **Destinations**.
Security	Manage and control secure access to the network.
Group-Based Policy	Manage group-based policies for networks that enforce segmentation and access control based on Cisco security group tags. This role includes Endpoint Analytics.
IP-Based Access Control	Manage IP-based access control lists that enforce network segmentation based on IP addresses.
Security Advisories	Scan the network for security advisories. Review and understand the impact of published Cisco security advisories that may affect your network.

Capability	Description
System	Centralized administration of Catalyst Center, which includes configuration management, network connectivity, software upgrades, and more.
Machine Reasoning	Configure automatic updates to the machine reasoning knowledge base to rapidly identify security vulnerabilities and improve automated issue analysis.
System Management	Manage core system functionality and connectivity settings. Manage user roles and configure external authentication. This role includes Integrity Verification, HA, Disaster Recovery, Debugging Logs, Product Telemetry, System EULA, IPAM, vManage Servers, Cisco AI Analytics, Backup & Restore, and Data Platform.
Utilities	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.
Audit Log	Detailed log of changes made via UI or API interface to network devices or Catalyst Center.
Event Viewer	View network device and client events for troubleshooting.
Network Reasoner	Initiate logical and automated troubleshooting for network issues while drawing on the knowledge wealth of network domain experts.
Remote Device Support	Allow the Cisco support team to remotely troubleshoot the network devices managed by Catalyst Center. With this role enabled, an engineer from the Cisco Technical Assistance Center (TAC) can connect remotely to a customer's Catalyst Center setup for troubleshooting purposes.
Scheduler	Integrated with other back-end services, scheduler lets you run, schedule, and monitor network tasks and activities such as deploy policies, provision, or upgrade the network. You can also schedule rogue containment.
Search	Search for various objects in Catalyst Center, such as sites, network devices, clients, applications, policies, settings, tags, menu items, and more.

Display Role-Based Access Control Statistics

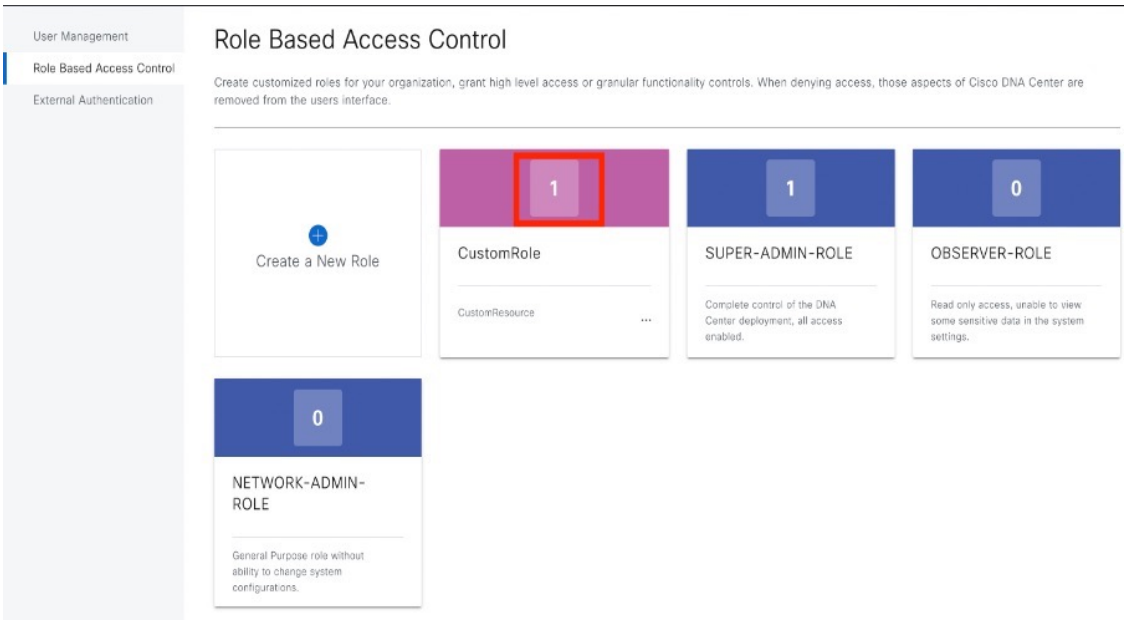
You can display statistics that show how many users belong to each user role. You can also drill down to view the list of users who have a selected role.

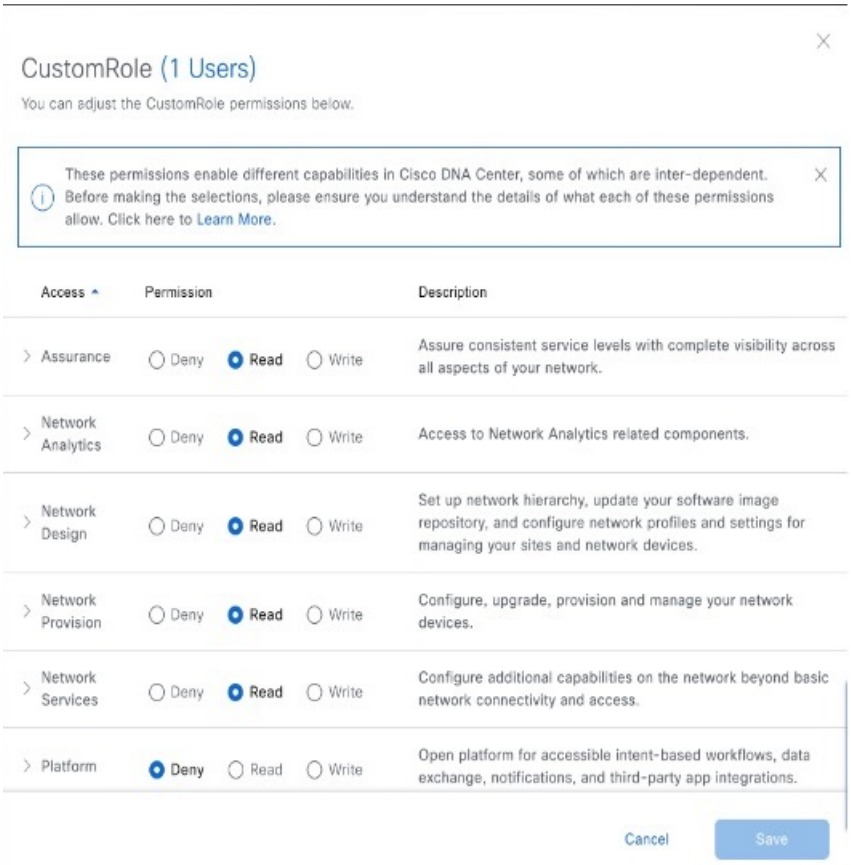
Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **Role Based Access Control**.

All default user roles and custom roles are displayed.

Step 2 Click the number corresponding to each user role to view the list of users who have that role.


User Management
Role Based Access Control
External Authentication
Role Based Access Control
Create customized roles for your organization, grant high level access or granular functionality controls. When denying access, those aspects of Cisco DNA Center are removed from the users interface.
Create a New Role
1
CustomRole
CustomResource
1
SUPER-ADMIN-ROLE
Complete control of the DNA Center deployment, all access enabled.
0
OBSERVER-ROLE
Read only access, unable to view some sensitive data in the system settings.
0
NETWORK-ADMIN-ROLE
General Purpose role without ability to change system configurations.


CustomRole (1 Users)
You can adjust the CustomRole permissions below.
These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to Learn More.
Access
Permission
Description
Assurance
Deny
Read
Write
Assure consistent service levels with complete visibility across all aspects of your network.
Network Analytics
Deny
Read
Write
Access to Network Analytics related components.
Network Design
Deny
Read
Write
Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
Network Provision
Deny
Read
Write
Configure, upgrade, provision and manage your network devices.
Network Services
Deny
Read
Write
Configure additional capabilities on the network beyond basic network connectivity and access.
Platform
Deny
Read
Write
Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
Cancel
Save

Configure External Authentication

If you are using an external server for authentication and authorization of external users, you should enable external authentication in Catalyst Center.

Before you begin

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- You must configure at least one authentication server.

Note In releases earlier than 2.1.x, when external authentication is enabled, Catalyst Center falls back to local users if the AAA server is unreachable or the AAA server rejects an unknown username. In the current release, Catalyst Center does not fall back to local users if the AAA server is unreachable or the AAA server rejects an unknown username.

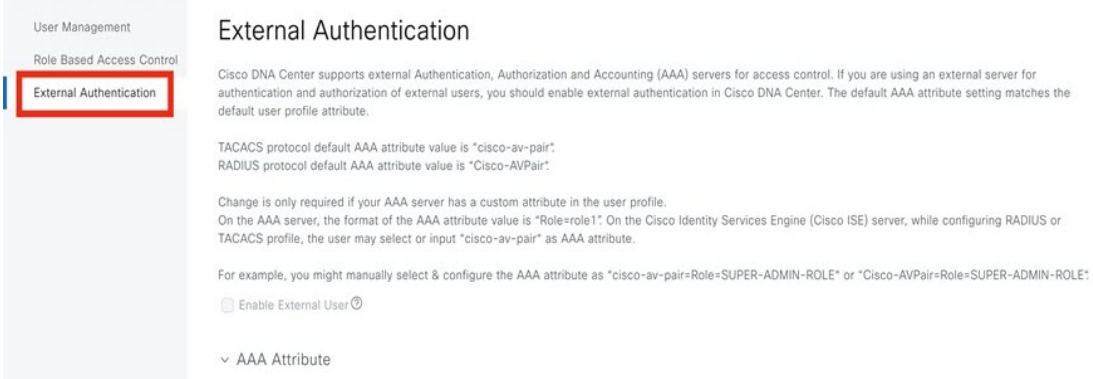
When external authentication fallback is enabled, external users and local admins can log in to Catalyst Center.

To enable external authentication fallback, SSH to the Catalyst Center instance and enter the following CLI command:

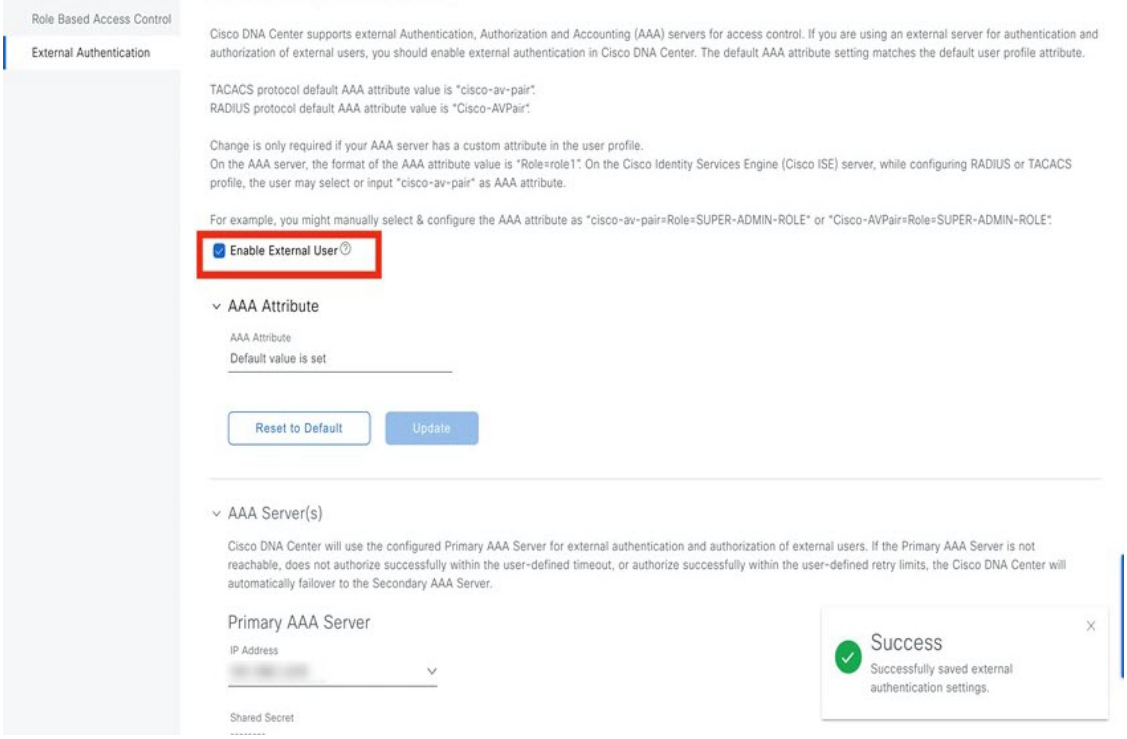
```
magctl rbac external_auth_fallback enable
```

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **External Authentication**.



Step 2 To enable external authentication in Catalyst Center, check the **Enable External User** check box.



Step 3 (Optional) Configure the AAA attribute.

For TACACS authentication, the following AAA attributes are supported:

Catalyst Center	**TACACS**
Empty	cisco-av-pair
cisco-av-pair	cisco-av-pair
Cisco-AVPair	Cisco-AVPair

For RADIUS authentication, the following AAA attributes are supported:

Catalyst Center	**RADIUS**
Empty	cisco-av-pair
Cisco-AVPair	cisco-av-pair

a) In the **AAA Attribute** field, enter the appropriate attribute for your use case, as described in the preceding tables. The default value of the **AAA Attribute** field is null.

b) Click **Update**.

Step 4 (Optional) Configure the AAA server or servers.

Configure these settings only if you want to swap the current primary or secondary AAA servers or define different AAA servers. From the top-left corner, click the menu icon and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers** to open the **Authentication and Policy Servers** window.

a) From the **Primary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.

b) From the **Secondary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.

c) (Optional) If you are using a Cisco ISE server, you can update the settings, if necessary.

For information about Cisco ISE policies, see "Configure and Manage Policies" in the *Cisco Identity Services Engine Administrator Guide*.

Table 5: Cisco ISE Server Settings

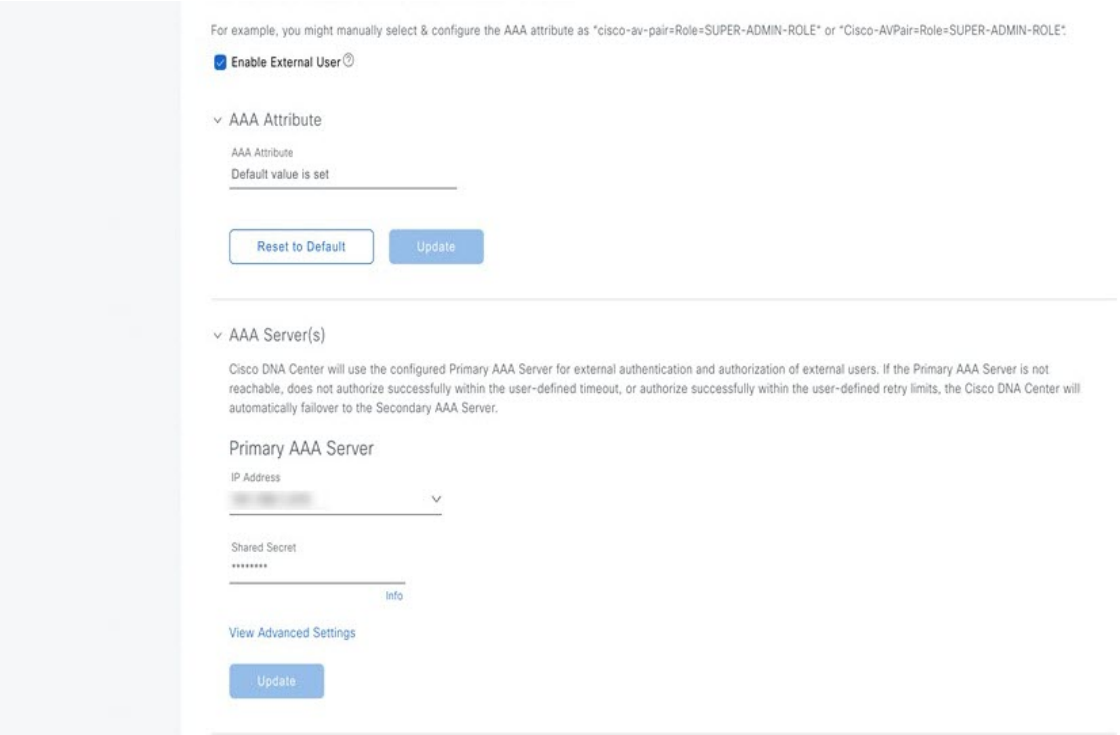
Name	Description
Shared Secret	Key for device authentications. The shared secret can contain up to 100 characters. The shared secret must be provided before the AAA address can be updated.
Username	Name that is used to log in to the Cisco ISE CLI.
Password	Password for the Cisco ISE CLI username.
FQDN	Fully qualified domain name (FQDN) of the Cisco ISE server. The FQDN consists of two parts, a hostname and the domain name, in the following format: *hostname.domainname.com* For example, the FQDN for a Cisco ISE server might be ise.cisco.com.
Subscriber Name	A unique text string—for example, `acme`—that is used during Catalyst Center-to-Cisco ISE integration to set up a new pxGrid client in Cisco ISE.
Virtual IP Address(es)	Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

d) (Optional) To update advanced settings, click **View Advanced Settings** and update the settings, if necessary.

Table 6: AAA Server Advanced Settings

Name	Description
Protocol	TACACS or RADIUS.
Authentication Port	Port used to relay authentication messages to the AAA server. • For RADIUS, the default is UDP port 1812. • For TACACS, the port is 49 and can't be changed.
Accounting Port	Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. • For RADIUS, the default UDP port is 1813. • For TACACS, the port is 49 and can't be changed.
Retries	Number of times that Catalyst Center can attempt to connect with Cisco ISE.

Name	Description
Timeout	Length of time that Catalyst Center waits for Cisco ISE to respond. The maximum timeout value is 60 seconds.



e) Click **Update**.

Two-Factor Authentication

Two-factor authentication, also known as 2FA, adds another layer of security to user verification by using an identifier method in addition to a user's name and password. The identifier method is generally something that only the actual intended user possesses (such as a phone app or keyfob) and is intentionally separated from the original login method.

The Catalyst Center implementation of two-factor authentication supports the use of a token client (that generates single-use token codes after the appropriate PIN is entered), a token server (that validates token codes), and an authentication server to manage user access. Authentication can be handled using either the RADIUS or TACACS+ protocol.

Prerequisites for Two-Factor Authentication

The following prerequisites must be in place to set up two-factor authentication for use with Catalyst Center:

- An authentication server that is able to return attribute-value pairs to convey RBAC role authorizations for authenticated Catalyst Center users. In our example, we use Cisco Identity Services Engine (Cisco ISE) 2.3 Patch 1.
- A two-factor token server that you will integrate with your authentication server. In our example, we use RSA Authentication Manager 7.2.
- A token card application on the client’s machine that generates software tokens. In our example, we use RSA SecurID Software Token.

Two-Factor Authentication Workflow

Here is a summary of what happens when a user logs in to a Catalyst Center appliance on which two-factor authentication has been configured:

1. In an RSA SecurID token client, a user enters their PIN to get a token code.
2. In the Catalyst Center login page, they enter their username and token code.
3. Catalyst Center sends the login request to Cisco ISE using either the RADIUS or TACACS+ protocol.
4. Cisco ISE sends the request to the RSA Authentication Manager server.
5. RSA Authentication Manager validates the token code and informs Cisco ISE whether the user has been authenticated successfully.
6. If the user has been authenticated, Cisco ISE matches the authenticated user with their configured authorization profile and returns the **role=NETWORK-ADMIN-ROLE** attribute-value pair.
7. Catalyst Center grants access to the features and pages associated with the user's role-based access control (RBAC) role.

Configure Two-Factor Authentication

To configure two-factor authentication on your Catalyst Center appliance, complete the following procedure.

Procedure

Step 1 Integrate RSA Authentication Manager with Cisco ISE:

a) In RSA Authentication Manager, create two users: **`example_admin`** (for the Admin user role) and **`example_observer`** (for the Observer role).

For more information, see the "Add a User to the Internal Database" topic in the RSA Self-Service Console Help. To access this topic, do the following:

1. Open the *RSA Self-Service Console Help*.
2. In the **Search help** field, enter **`Add a User to the Internal Database`** and then click **Search help**.

b) Create a new authentication agent.

For more information, see the "Add an Authentication Agent" topic in the *RSA Self-Service Console Help*.

c) Generate the Authentication Manager agent configuration file (sdconf.rec):

1. From the RSA Security Console, choose **Access** > **Authentication Agents** > **Generate Configuration File**.

   The **Configure Agent Timeout and Retries** tab opens.
2. For the **Maximum Retries** and **Maximum Time Between Each Retry** fields, use the default values.
3. Click **Generate Configuration File**.

   The **Download Configuration File** tab opens.
4. Click the **Download Now** link.
5. When prompted, click **Save to Disk** to save a local copy of the zip file.

6. Unzip the file and use this version of the sdconf.rec file to overwrite the version that is currently installed on the agent.

d) Generate a PIN for the **`example_admin`** and **`example_observer`** users that you created in Step 1a.

For more information, see the "Create My On-Demand Authentication PIN" topic in the *RSA Self-Service Console Help*.

e) Start Cisco ISE, choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**, and then click **Add**.

f) In the **RSA SecurID Identity Sources** page, click **Browse**, choose the sdconf.rec file you downloaded, and then click **Open**.

g) Check the **Reauthenticate on Change PIN** check box, then click **Submit**.

Step 2 Create two authorization profiles, one for the Admin user role and one for the Observer user role.

a) In Cisco ISE, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

b) For both profiles, enter the following information:

- **Name**: Enter the profile name.
- **Access Type**: Choose **ACCESS_ACCEPT**.
- **Advanced Attributes Settings** area: Choose **Cisco:cisco-av-pair** from the first drop-down list.

  If you are creating an authorization profile for the Admin user role, choose **Role=NETWORK-ADMIN-ROLE** from the second drop-down list.

  If you are creating an authorization profile for the Observer user role, choose **Role=OBSERVER-ROLE** from the second drop-down list.

Step 3 Create an authentication policy for your Catalyst Center appliance.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authentication Policies" topic.

Step 4 Create two authorization policies, one for the Admin user role and one for the Observer user role.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authorization Policies" topic.

Step 5 In the RSA Authentication Manager Security Console, verify that software tokens have been assigned to both users.

For more information, see the "View a Token" topic in the *RSA Self-Service Console Help*.

Note If you need to assign tokens, complete the steps described in the "Assign a Software Token to a User" topic.

Enable Two-Factor Authentication Using RADIUS

To enable two-factor authentication that uses a Cisco ISE server configured for RADIUS, complete the following procedure:

Procedure

Step 1 Integrate Cisco ISE with Catalyst Center.

In the *Catalyst Center Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.

Step 2 Configure Catalyst Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important Ensure that you specify the same shared secret for both Cisco ISE and Catalyst Center.

Enable Two-Factor Authentication Using TACACS+

To enable two-factor authentication that uses a Cisco ISE server configured for TACACS+, complete the following procedure:

Procedure

Step 1 In Cisco ISE, choose **Administration** > **Network Resources** > **Network Devices** to open the **Network Devices** window.

Step 2 Click **TACACS Authentication Settings** to view its contents. Ensure that a shared secret has already been configured for the Catalyst Center device that you added previously.

Step 3 Choose **Work Centers** > **Device Administration** > **Policy Elements** to open the **TACACS Profiles** window.

Step 4 Create TACACS+ profiles for the example_admin and example_observer user roles:

a) Click **Add**.

b) Complete the following tasks:

- Enter the profile name.
- After clicking the **Raw View** tab, enter the following text into the **Profile Attributes** text box:
  - For the example_admin user role, enter **`Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE`**
  - For the example_observer user role, enter **`Cisco-AVPair=ROLE=OBSERVER-ROLE`**

c) Click **Save**.

Step 5 Integrate Cisco ISE with Catalyst Center.

In the *Catalyst Center Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.

Step 6 Configure Catalyst Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important Ensure that you specify the same shared secret for both Cisco ISE and Catalyst Center.

Log In Using Two-Factor Authentication

To log in to Catalyst Center using two-factor authentication, complete the following procedure:

Procedure

Step 1 From the Catalyst Center login page, enter the appropriate username.

Step 2 Open the RSA SecurID token client and enter the PIN you configured previously to generate a one-time token.

Step 3 Copy this token and paste it into the **Password** field of the Catalyst Center login page.

Step 4 Click **Log In**.

Display External Users

You can view the list of external users who have logged in through RADIUS or TACACS for the first time. The information that is displayed includes their usernames and roles.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **External Authentication**.

Step 2 Scroll to the bottom of the window, where the **External Users** area lists the external users.

Migrate from Cisco Prime Infrastructure to Catalyst Center

Before you begin

This section provides an overview about how to migrate from Cisco Prime Infrastructure to Catalyst Center.

- Using the Cisco Prime Infrastructure Compatibility Matrix, identify the Prime Data Migration Tool (PDMT) release that is compatible with your version of Catalyst Center.
- Download the compatible PDMT release using the Cisco Software Download Tool.

Procedure

Step 1 Perform a readiness check using the Catalyst Center Assessment and Readiness Tool for Cisco Prime Infrastructure (PDART).

For more information about using PDART, click here.

Step 2 Once you have assessed the readiness of the migration, use the PDMT to migrate your sites and devices from Cisco Prime Infrastructure to Catalyst Center.

Multiple Catalyst Center—Limited Availability

Multiple Catalyst Center allows you to define a single global set of virtual networks for software-defined access across multiple Catalyst Center clusters integrated with a single Cisco ISE system. This Multiple Catalyst Center functionality is a Limited Availability offering in Catalyst Center on ESXi.

To facilitate global administration of Cisco SD-Access across multiple Catalyst Center clusters with a consistent set of virtual networks, the Multiple Catalyst Center feature leverages the existing secure connection with Cisco ISE to propagate virtual networks, Security Group Tags (SGTs), access contracts, and Group-Based Access Control (GBAC) Policy from one cluster to another cluster, all integrated with the same Cisco ISE deployment. Cisco ISE takes the information learned from one cluster (the Author node) and propagates it to the other clusters (Reader nodes).

Because there are significant caveats for the Multiple Catalyst Center functionality, the Cisco SD-Access Design Council reviews the requests and provides guidance for use of the Multiple Catalyst Center to participants in the Limited Availability program.

Contact your account team to submit a request to the Cisco SD-Access Design Council to participate in the Limited Availability program.

Customers who are using Cisco ISE Version 3.1 or earlier must request and install the Limited Availability package before enabling Multiple Catalyst Center.

Note After this functionality is enabled, it can be disabled only by deleting Cisco ISE. In addition, if this functionality is enabled, because pxGrid is a required component of the solution, pxGrid cannot be disabled subsequently.

Operation: Monitoring and Troubleshooting

About System Settings

To start using Catalyst Center, you must first configure the system settings so that the server can communicate outside the network, ensure secure communications, authenticate users, and perform other key tasks. Use the procedures described in this chapter to configure the system settings.

Note

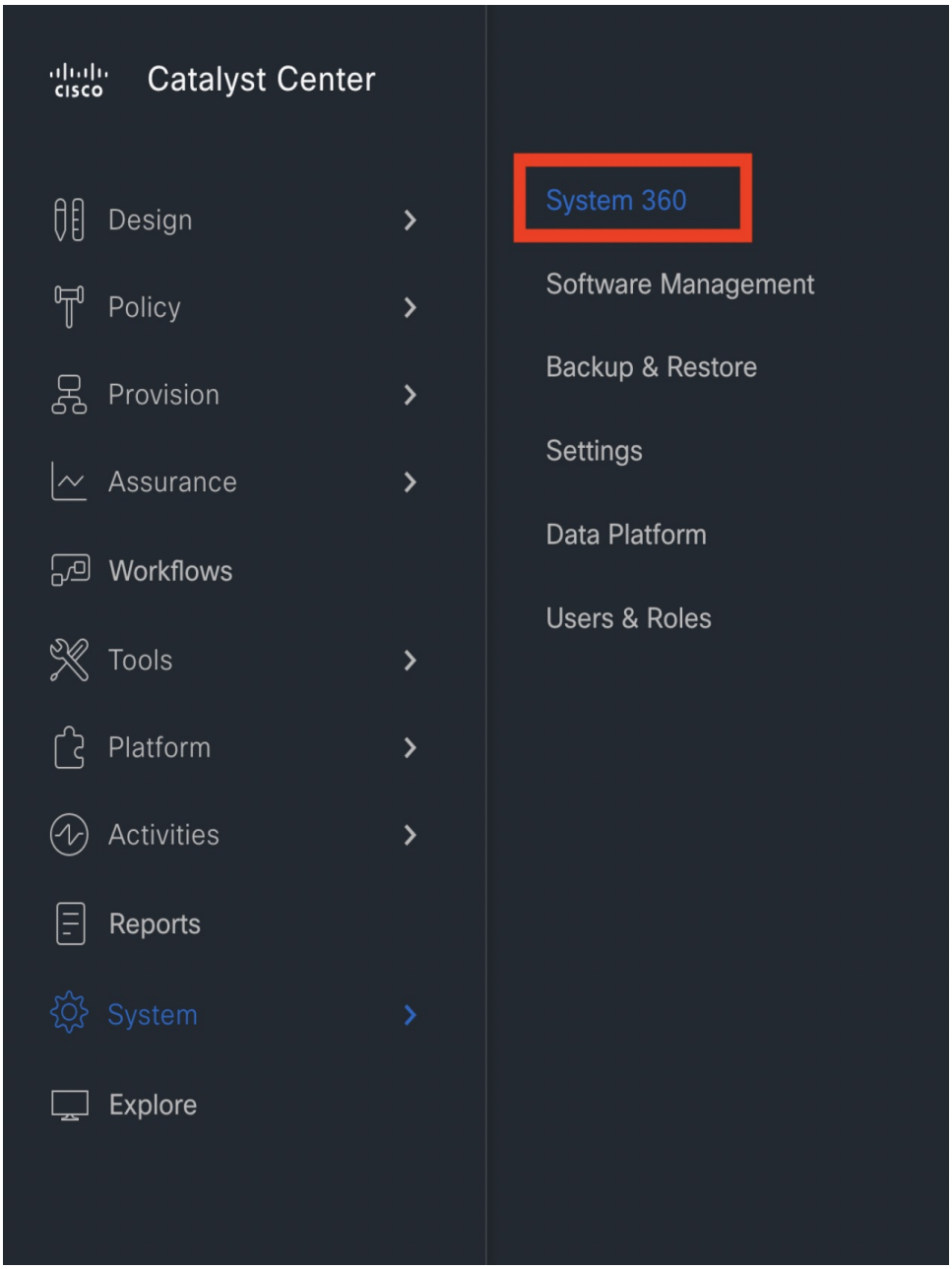
- Any changes that you make to the Catalyst Center configuration—including changes to the proxy server settings—must be done from the Catalyst Center GUI.
- Any changes to the IP address, static route, DNS server, or **maglev** user password must be done from the CLI with the `sudo maglev-config update` command.
- By default, the Catalyst Center system time zone is set to UTC. Do not change this time zone in settings because the Catalyst Center GUI works with your browser time zone.

Use System 360

The **System 360** tab provides at-a-glance information about Catalyst Center.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **System 360**.



Step 2 On the **System 360** dashboard, review the following displayed data metrics:

Cluster

- **Hosts**: Displays information about the Catalyst Center hosts. The information that is displayed includes the IP address of the hosts and detailed data about the services running on the hosts. Click the **View Services** link to view detailed data about the services running on the hosts.

  Note The host IP address has a color badge next to it. A green badge indicates that the host is healthy. A red badge indicates that the host is unhealthy.

  The side panel displays the following information:

- **Node Status**: Displays the health status of the node.

  If the node health is **Unhealthy**, hover your cursor over the status to view additional troubleshooting information.

- **Services Status**: Displays the health status of the services. Even if one service is down, the status is **Unhealthy**.

- **Name**: Service name.

- **Appstack**: App stack name.

  An app stack is a loosely coupled collection of services. A service in this environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.

- **Health**: Status of the service.

- **Version**: Version of the service.

- **Tools**: Displays metrics and logs for the service. Click the **Metrics** link to view service monitoring data in Grafana. Grafana is an open-source metric analytics and visualization suite. You can troubleshoot issues by reviewing the service monitoring data. For information about Grafana, see https://grafana.com/. Click the **Logs** link to view service logs in Kibana. Kibana is an open-source analytics and visualization platform. You can troubleshoot issues by reviewing the service logs. For information about Kibana, see https://www.elastic.co/products/kibana.

- **Actions**: Option available to restart the service. For some of the internal and system specific services, the **Actions** option is disabled.

- **High Availability**: Status of HA is not available through Catalyst Center on ESXi because HA is provided by VMware vSphere. For more information, see High Availability, on page 127.

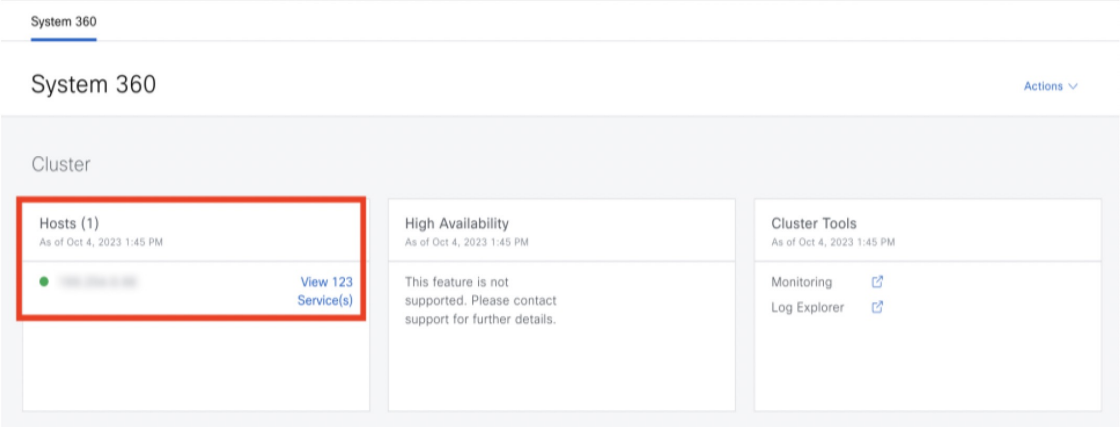
- **Cluster Tools**: Lets you access the following tools:

  - **Monitoring**: Access multiple dashboards of Catalyst Center components using Grafana, which is an open-source metric analytics and visualization suite. Use the **Monitoring** tool to review and analyze key Catalyst Center metrics, such as memory and CPU usage. For information about Grafana, see https://grafana.com/.

    Note In a multihost Catalyst Center environment, expect duplication in the Grafana data due to the multiple hosts.

  - **Log Explorer**: Access Catalyst Center activity and system logs using Kibana. Kibana is an open-source analytics and visualization platform designed to work with Elasticsearch. Use the **Log Explorer** tool to review detailed activity and system logs. In the Kibana left navigation pane, click **Dashboard**. Then, click **System Overview** and view all of the system logs. For information about Kibana, see https://www.elastic.co/guide/en/kibana/current/index.html. For information about Elasticsearch, see https://www.elastic.co/guide/index.html.

    Note All logging in Catalyst Center is enabled by default.



System Management

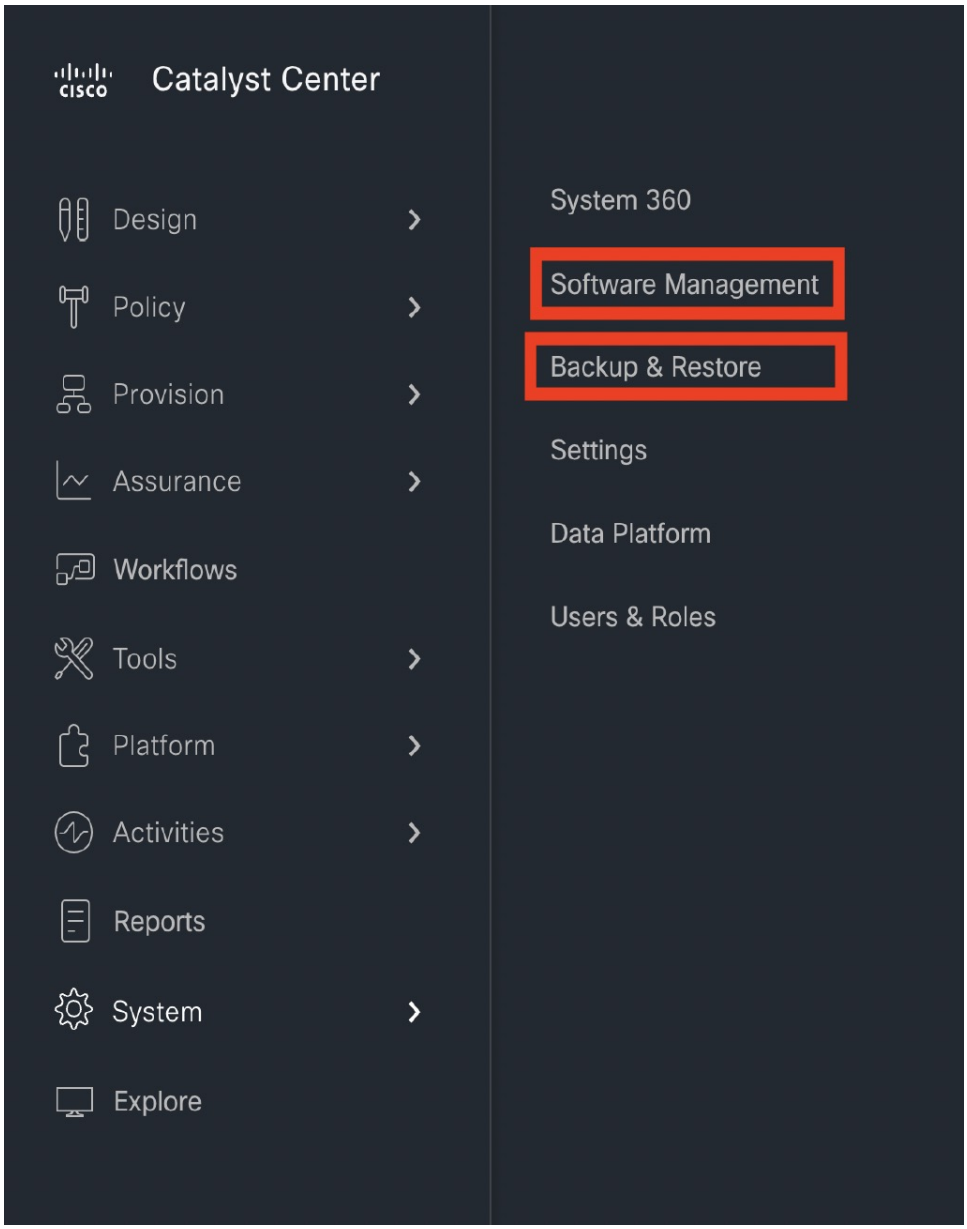
- **Software Management**: Displays information about the installed version status and system updates. Click the **View** link to view the update details. The dashlet notifies when the airgap mode is enabled.

  Note An update has a color badge next to it. A green badge indicates that the update or actions related to the update succeeded. An orange badge indicates that there is an available update.

- **Backup & Restore**: Displays the status of the most recent backup. Click the **View** link to view all backup details.

  Additionally, it displays the status of the next scheduled backup (or indicates that no backup is scheduled). When airgap mode is enabled, the backup configuration is not found.

  Note A backup has a color badge next to it. A green badge indicates a successful backup with a timestamp. An orange badge indicates that the next backup is not yet scheduled.



Configure Debugging Logs

To assist in troubleshooting service issues, you can change the logging level for the Catalyst Center services.

A logging level determines the amount of data that is captured in the log files. Each logging level is cumulative; that is, each level contains all the data generated by the specified level and higher levels, if any. For example, setting the logging level to **Info** also captures **Warn** and **Error** logs. We recommend that you adjust the logging level to assist in troubleshooting issues by capturing more data. For example, by adjusting the logging level, you can capture more data to review in a root cause analysis or RCA support file.

The default logging level for services is informational (**Info**). You can change the logging level from informational to a different logging level (**Debug** or **Trace**) to capture more information.

Caution Due to the type of information that might be disclosed, logs collected at the **Debug** level or higher should have restricted access.

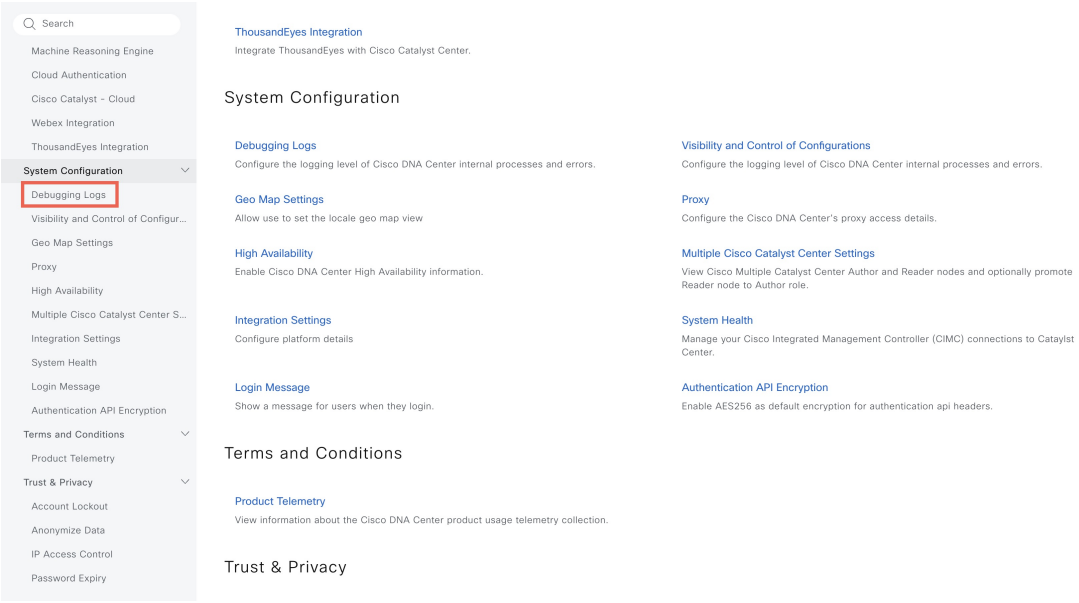
Note Log files are created and stored in a centralized location on your Catalyst Center host for display in the GUI. From this location, Catalyst Center can query and display logs in the GUI (**System** > **System 360** > **Log Explorer**). Logs are available to query for only the last 2 days. Logs that are older than 2 days are purged automatically from this location.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **System Configuration** > **Debugging Logs**.



The **Debugging Logs** window is displayed.

Step 2 From the **Service** drop-down list, choose a service to adjust its logging level.

The **Service** drop-down list displays the services that are currently configured and running on Catalyst Center.

Step 3 Enter the **Logger Name**.

This is an advanced feature that has been added to control which software components emit messages into the logging framework. Use this feature with care. Misuse of this feature can result in loss of information needed for technical support purposes. Log messages will be written only for the loggers (packages) specified here. By default, the Logger Name includes packages that start with *com.cisco*. You can enter additional package names as comma-separated values. Do not remove the default values unless you are explicitly directed to do so. Use * to log all packages.

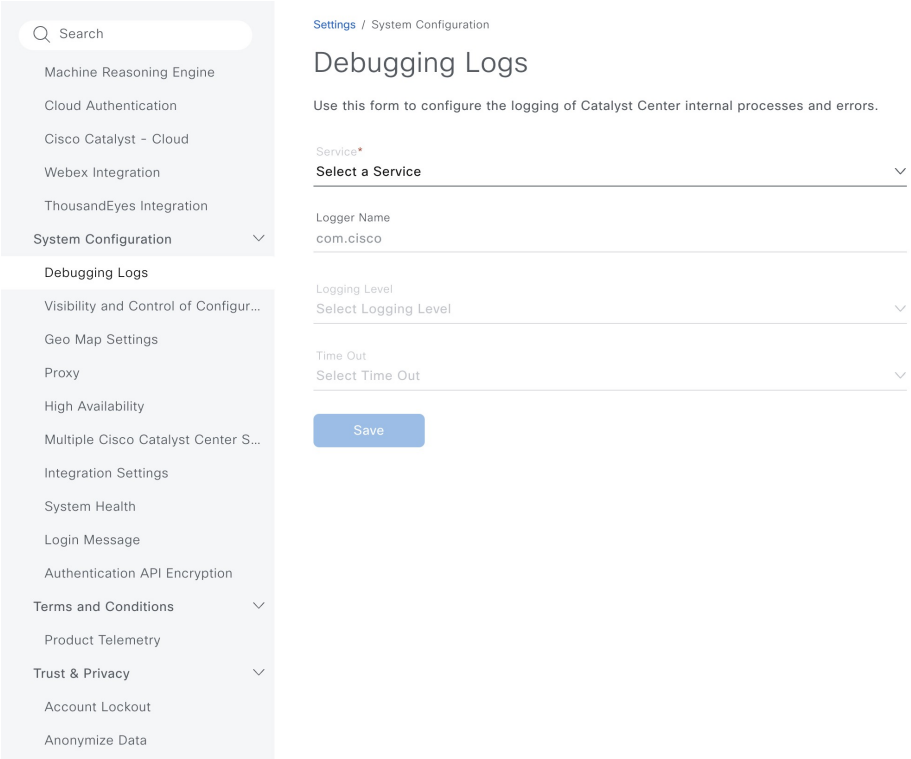
Step 4 From the **Logging Level** drop-down list, choose the new logging level for the service.

Catalyst Center supports the following logging levels in descending order of detail:

- **Trace**: Trace messages
- **Debug**: Debugging messages
- **Info**: Normal, but significant condition messages
- **Warn**: Warning condition messages
- **Error**: Error condition messages

Step 5 From the **Time Out** field, choose the time period for the logging level.

Configure logging-level time periods in increments of 15 minutes up to an unlimited time period. If you specify an unlimited time period, the default level of logging should be reset each time a troubleshooting activity is completed.



Step 6 Review your selection and click **Save**.

View Audit Logs

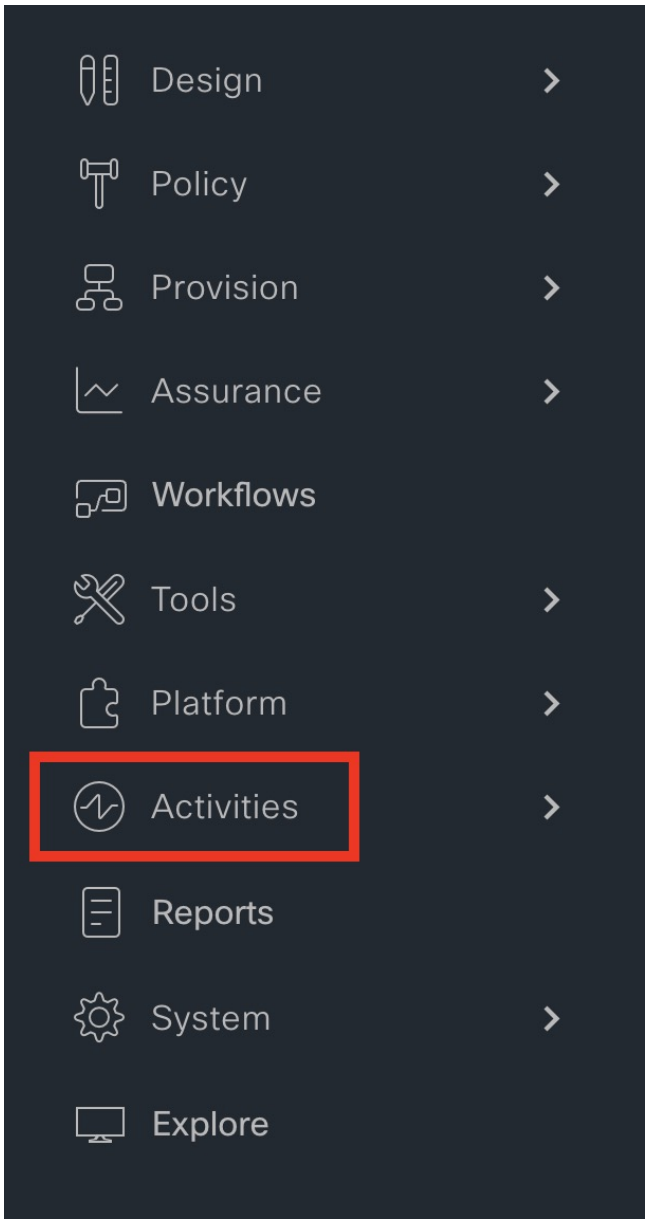
Audit logs capture information about the various applications running on Catalyst Center. Audit logs also capture information about device public key infrastructure (PKI) notifications. The information in these audit logs can be used to help in troubleshooting issues, if any, involving the applications or the device CA certificates.

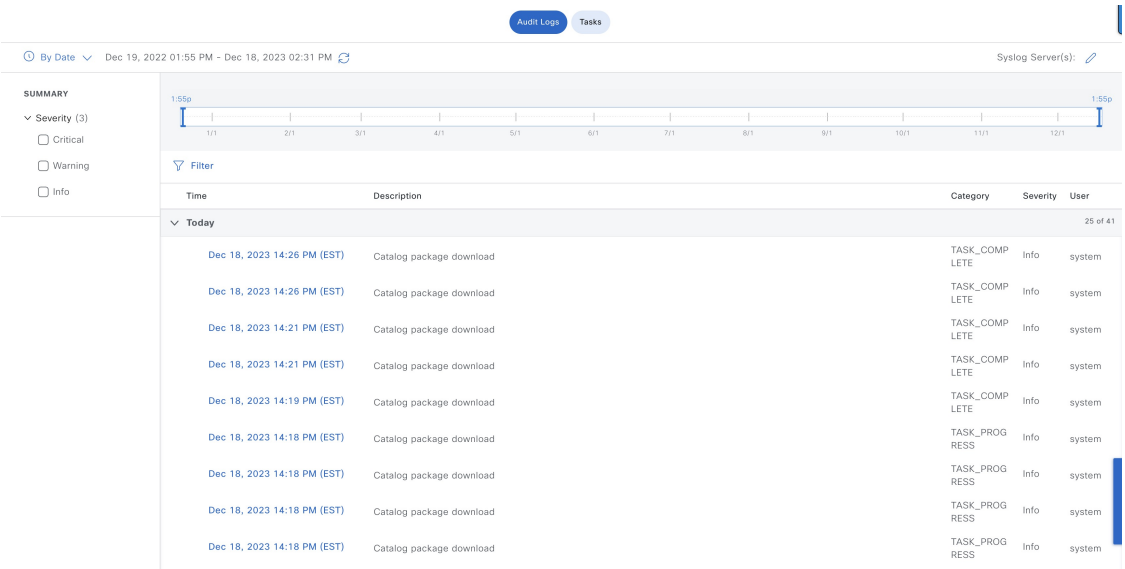
Audit logs also record system events that occurred, when and where they occurred, and which users initiated them. With audit logging, configuration changes to the system get logged in separate log files for auditing.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Activities** > **Audit Logs**.

The **Audit Logs** window opens, where you can view logs about the current policies in your network. These policies are applied to network devices by the applications installed on Catalyst Center.


Design
Policy
Provision
Assurance
Workflows
Tools
Platform
Activities
Reports
System
Explore



Step 2 Click the timeline slider to specify the time range of data you want displayed on the window:

a. In the **Time Range** area, choose a time range—**Last 2 Weeks**, **Last 7 Days**, **Last 24 Hours**, or **Last 3 Hours**.

b. To specify a custom range, click **By Date** and specify the start and end date and time.

c. Click **Apply**.

Step 3 Click the arrow next to an audit log to view the corresponding child audit logs.

Each audit log can be a parent to several child audit logs. By clicking the arrow, you can view a series of additional child audit logs.

Note An audit log captures data about a task performed by Catalyst Center. Child audit logs are subtasks to a task performed by Catalyst Center.

Step 4 (Optional) From the list of audit logs in the left pane, click a specific audit log message. In the right pane, click **Event ID** > **Copy Event ID to Clipboard**. With the copied ID, you can use the API to retrieve the audit log message based on the event ID.

The audit log displays the **Description**, **User**, **Interface**, and **Destination** of each policy in the right pane.

Note The audit log displays northbound operation details such as POST, DELETE, and PUT with payload information, and southbound operation details such as the configuration pushed to a device. For detailed information about the APIs on Cisco DevNet, see Catalyst Center Platform Intent APIs.

Step 5 (Optional) Click **Filter** to filter the log by **User ID**, **Log ID**, or **Description**.

Step 6 Click **Subscribe** to subscribe to the audit log events.

A list of syslog servers is displayed.

Step 7 Check the syslog server check box that you want to subscribe to and click **Save**.

Note Uncheck the syslog server check box to unsubscribe from the audit log events and click **Save**.

Step 8 In the right pane, use the **Search** field to search for specific text in the log message.

Step 9 From the top-left corner, click the menu icon and choose **Activities** > **Tasks** to view the upcoming, in-progress, completed, and failed tasks (such as operating system updates or device replacements) and existing, pending-review, and failed work items.

Export Audit Logs to Syslog Servers

Security Recommendation: We strongly encourage you to export audit logs from Catalyst Center to a remote syslog server in your network, for more secure and easier log monitoring.

You can export the audit logs from Catalyst Center to multiple syslog servers by subscribing to them.

Before you begin

Configure the syslog servers in the **System** > **Settings** > **External Services** > **Destinations** > **Syslog** area.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Activities** > **Audit Logs**.

Step 2 Click **Subscribe**.

Step 3 Select the syslog servers that you want to subscribe to and click **Save**.

Step 4 (Optional) To unsubscribe, deselect the syslog servers and click **Save**.

Use APIs to View Audit Logs in Syslog Servers

With the Catalyst Center platform, you can use APIs to view audit logs in syslog servers. Using the **Create Syslog Event Subscription** API from the **Developer Toolkit**, create a syslog subscription for audit log events.

Whenever an audit log event occurs, the syslog server lists the audit log events.

Configure the Proxy

If Catalyst Center on ESXi has a proxy server configured as an intermediary between itself and the network devices that it manages, you must configure access to the proxy server.

Note Catalyst Center on ESXi does not support a proxy server that uses Windows New Technology LAN Manager (NTLM) authentication.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see the "About User Roles" topic in the *Cisco Catalyst Center on ESXi Administrator Guide*.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **System Configuration**.

Step 2 From the **System Configuration** drop-down list, choose **Proxy** > **Outgoing Proxy**.

Step 3 Enter the proxy server's URL address.

Step 4 Enter the proxy server's port number.

Note
- For HTTP, the port number is usually 80.
- The port number ranges from 0 through 65535.

Step 5 (Optional) If the proxy server requires authentication, click **Update** and enter the username and password for access to the proxy server.

Step 6 Check the **Validate Settings** check box to have Catalyst Center on ESXi validate your proxy configuration settings when applying them.

Step 7 Review your selections and click **Save**.

To cancel your selection, click **Reset**. To delete an existing proxy configuration, click **Delete**.

After configuring the proxy, you can view the configuration in the **Proxy** window.

Important It can take up to five minutes for Catalyst Center on ESXi services to get updated with the proxy server configuration.

About Restricted Shell

For added security, access to the root shell is disabled. With restricted shell, users can't access the underlying operating system and file system, which reduces operational risk.

Restricted shell is enabled for security purposes. However, if you want to access the root shell temporarily, you must contact the Cisco TAC for assistance.

If necessary, you can use the following restricted list of commands:

Table 7: Restricted Shell Commands

Command	Description
cat	Concatenate and print files in restricted mode.
clear	Clear the terminal screen.
date	Display the current time in the given FORMAT or set the system date.
debug	Enable console debug logs.
df	File system information.
dmesg	Print or control the kernel ring buffer.
du	Summarize disk usage of the set of FILEs recursively for directories.
free	Quick summary of memory usage.
history	Enable shell commands history.
htop	Interactive process viewer.

Command	Description
ip	Print routing
network devices	interfaces and tunnels.
kubectl	Interact with Kubernetes Cluster in a restricted manner.
last	Show a listing of last logged in users.
ls	Restricted file system view chrooted to maglev Home.
lscpu	Print information about the CPU architecture.
magctl	Tool to manage a Maglev deployment.
maglev-config	Tool to configure a Maglev deployment.
manufacture_check	Tool to perform manufacturing checks.
netstat	Print networking information.
nslookup	Query Internet name servers interactively.
ntpq	Standard NTP query program.
ping	Send ICMP ECHO_REQUEST to network hosts.
ps	Check status of active processes in the system.
rca	Root cause analysis collection utilities.
reboot	Reboot the machine.
rm	Delete files in restricted mode.
route	Print the IP routing table.
runonce	Execute runonce scripts.
scp	Restricted secure copy.
sftp	Secure file transfer.
shutdown	Shutdown the machine.
ssh	OpenSSH SSH client.
tail	Print the last 10 lines of each FILE to standard output.
top	Display sorted list of system processes.
traceroute	Print the route packets trace to network host.
uname	Print system information.
uptime	Tell how long the system has been running.
vi	Text editor.
w	Show who is logged on and what they are doing.

Glossary

Term	Definition
Cisco ISE	Cisco Identity Service Engine
DR	Disaster Recovery
HA	High Availability
VA	Virtual Appliance

Feedback and Discussions

For comments and suggestions about our guides, please join the discussion on Cisco Community.

References

- *Cisco Catalyst Center 2.3.7.4 on ESXi Deployment Guide*
- *Cisco Catalyst Center 2.3.7.4 on ESXi Administrator Guide*
- *Release Notes for Cisco Catalyst Center on ESXi, Release 2.3.7.4*

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.