Cisco Catalyst Center 2.3.7.x on ESXi Deployment Guide

First Published: 2023-12-20

Last Modified: 2024-04-08

Catalyst Center on ESXi Deployment Guide

Catalyst Center on ESXi Deployment Overview

Catalyst Center on ESXi provides Catalyst Center functionality in a virtual form factor. Its straightforward deployment process allows you to quickly deploy Catalyst Center in your network. It also allows you to try out Catalyst Center without having to purchase a physical appliance.

This guide provides the following information:

- The requirements that need to be met in order to successfully deploy a Catalyst Center on ESXi virtual appliance.
- Procedures that detail how to create a virtual machine on a VMware ESXi host, configure a virtual appliance, execute the Quick Start workflow, and complete post-deployment tasks that should be carried out before you use Catalyst Center on ESXi.

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 Xeon Scalable server processor (Cascade Lake or newer) or AMD EPYC Gen2 with 2.1 GHz or better clock speed. 32 vCPUs with 64-GHz reservation must be dedicated to the VM.

Feature	Description
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.

Cisco Catalyst Assurance uses near real-time streaming analytics, which requires additional guarantees on resource availability. When operating Catalyst Center on ESXi close to maximum scale, this functionality may be impacted by uncontrolled external events, such as host resource oversubscriptions and edge use cases that result in a resource usage spike. A number of things can indicate that these events are taking place, such as slow performance, data processing gaps, high I/O latency, and a CPU readiness percentage that's higher than normal.

Note For more information about troubleshooting performance problems, see the "Troubleshoot and Enhance Performance" topic for your VMware vSphere version:

- For VMware vSphere Client 7.0, click here.
- For VMware vSphere Client 8.0, click here.

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

Catalyst Center on ESXi Packages

For a listing of the packages used by the virtual appliance, see the "Package Versions in Cisco Catalyst Center 2.3.7.x on ESXi" topic in *Cisco Catalyst Center 2.3.7.x on ESXi Release Notes*.

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 4.
- Reserve Enterprise Interface, on page 4.
- Prepare the DNS, NTP, and Proxy Servers, on page 5.
- Prepare for the Quick Start Workflow, on page 6.

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.

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.

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.

Refer to the following table for the new and changed features available in Catalyst Center 2.3.7.x on ESXi.

Feature	Description
Default Single Network Interface Card (NIC)	By default, one NIC is enabled when you install Catalyst Center 2.3.7.x as a virtual appliance on ESXi. For setup instructions, see Deploy a Virtual Appliance, on page 7.
Second NIC Installation (Day-N)	As an option, after you install Catalyst Center 2.3.7.x on ESXi, you can add an additional NIC to your deployment. See Configure an Additional Network Adapter, on page 9.
CC VA Launcher Enhancements	You can configure a virtual appliance using the CC VA Launcher in interactive mode or silent mode. For information, see the following topics: • Configure a Virtual Appliance Using the Interactive CC VA Launcher, on page 28 • Configure a Virtual Appliance Using the CC VA Launcher in Silent Mode, on page 32

Deploy a Virtual Appliance

To set up a Catalyst Center on ESXi virtual appliance, you'll need to complete the following tasks:

1. Create a Virtual Machine.
2. Configure a Catalyst Center on ESXi Virtual Appliance.
3. Complete the Quick Start Workflow.

If you want to set up your virtual appliance using the CC VA Launcher, you'll first complete the steps described in one of the following topics:

- Configure a Virtual Appliance Using the Interactive CC VA Launcher, on page 28
- Configure a Virtual Appliance Using the CC VA Launcher in Silent Mode, on page 32

Then you'll Complete the Quick Start Workflow.

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 a Catalyst Center on ESXi Virtual Appliance

Complete one of the following procedures to configure a Catalyst Center on ESXi virtual appliance on a VMware ESXi host:

- Configure a Virtual Appliance Using the Maglev Configuration Wizard: Default Mode, on page 10
- Configure a Virtual Appliance Using the Maglev Configuration Wizard: Advanced Mode, on page 14
- Configure a Virtual Appliance Using the Install Configuration Wizard, on page 20
- Configure a Virtual Appliance Using the Advanced Install Configuration Wizard , on page 24

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.

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 38.

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

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**.

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 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 whether you want to use IPv4 or IPv6 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/IPv6 Address field	Enter the IP address for the Enterprise interface. This is required.

IPv4 Netmask/IPv6 Prefix Length field	Do one of the following: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/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.
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 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/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.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 Address field	Leave this field blank.
IPv4/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 IPv4/IPv6 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/IPv6 Prefix Length field	Do one of the following if you entered an IP address: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/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.
IPv4/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 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.

Step 4 Complete the Quick Start Workflow, on page 38.

Configure a Virtual Appliance Using the 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 1.

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 Advanced Install Configuration 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 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 Advanced Install Configuration Wizard . 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**.

This is the password you'll use to log in to Catalyst Center on ESXi for the first time after configuring the virtual appliance. After logging in, you'll be prompted to configure a new admin user (as a security measure). See Complete the Quick Start Workflow, on page 38.

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 38.

Configure a Virtual Appliance Using the Advanced Install Configuration Wizard

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 1.

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	If you want to use IPv6 addressing, check this check box. If you want to use IPv4 addressing instead, leave this check box blank.
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: • If you entered an IPv4 address, you can enter either a netmask or CIDR address. • If you entered an IPv6 address, you can only enter a CIDR address.
Default Gateway Address field	Specify the default gateway that will be used to route traffic.
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.

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 38.

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.x-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.

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.x-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 33 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.
- If any of the passwords you specify in this command contain OS-specific special characters, we recommend that you enter them as an escape sequence. An escape sequence is a backslash (\) followed by the characters or their corresponding octal or hexadecimal number.

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.

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.

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

View CC VA Launcher Appliance Configuration Progress

During a silent mode configuration of a Catalyst Center on ESXi virtual appliance, you can monitor the configuration process by viewing the **progress.json** file. Located in the same directory where the CC VA Launcher resides, this file provides the following information.

Field	Description
stage	Stage that the appliance configuration process is currently in: • launcher_start: The launcher has been started. • config_file_validation: The configuration file is being validated. • connectivity_verification: Connectivity with the vCenter/ESXi host is being verified. • import_information_validation: Import information (such as datastores, resource pool, and OVA path) is being verified. • import_ova: The Catalyst Center on ESXi OVA file is being imported. • post_import_configuration: Post-import configuration is taking place. • power_on: The virtual machine is being powered on. • deployment: Deployment of the virtual appliance is almost complete.
status	Status of the configuration process' current stage: • in-progress • completed • failed • waiting • aborted
percentage	Percentage of the Catalyst Center on ESXi OVA file that's been imported.
error_code	The error code associated with an operation that failed. Refer to the following table for a description of these codes.
error_desc	Description of an error.

Error Code	Description
0	Success
101	Manually terminated
102	Configuration file not found
103	Incorrect configuration file entry
104	Failed to connect to vCenter/ESXi host
105	Import operation failed

Error Code	Description
106	Specified OVA file path is invalid
107	Datastore field is empty
108	Invalid import information
109	Invalid datastore
110	Invalid datacenter
111	Datastore does not have the required amount of free space
112	Invalid disk provisioning
113	Invalid cluster
114	Virtual machine not found
115	Power on operation failed
116	Chose "No" in the deployment confirmation message
117	Incorrect command line arguments
118	Failed to add Management interface
119	Invalid json file
120	Mandatory silent mode fields are missing information
121	Specified OVA file is a different file type
122	Virtual machine name filed is empty
123	Enterprise network name field is empty
124	Invalid resource pool
125	Invalid management network
126	Virtual name exceeds character limit
127	Maglev password does not meet password requirements
129	Invalid ESXi host
130	Empty datacenter provided for vCenter-based import
131	Empty hostname provided for vCenter-based import
132	Invalid network was specified for the vCenter/ESXi host
133	Virtual machine has insufficient CPU or memory
134	Incorrect Catalyst Center on ESXi information was provided

Error Code	Description
135	No suitable datacenter was found during discovery
136	Empty OVA file path was provided

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 a Reservation for the Recovery Site's VM

If you enable disaster recovery for Catalyst Center on ESXi using vSphere's Site Recovery Manager (SRM), ensure that the required resources are reserved during failover by completing the following procedure. When you configure vSphere replication on the virtual appliance, the recovery site’s VM (also referred to as the placeholder VM) will not have a reservation configured on the main site. You'll need to configure the reservation manually after replication takes place.

Procedure

Step 1 In the vSphere Client's navigation pane, click the secondary site's placeholder VM.

Step 2 Click **Actions**, then choose **Edit Settings**.

Step 3 With the **Virtual Hardware** tab selected, configure a 64-GHz reservation for the **CPU** parameter and a 256-GB reservation for the **Memory** parameter.

Step 4 Click **OK**.

Configure a Reservation for the Recovery Site VM's Resource Pool

If you have deployed a virtual appliance in a resource pool and mapped its primary site resource pool to a secondary site resource pool using vSphere's Site Recovery Manager (SRM), ensure that the secondary site's resource pool reserves the resources required by the virtual appliance.

Enable an Air-Gapped Deployment

An air gap is a security measure that involves isolating a network and preventing it from establishing external connections. The only way data can be transferred into an air-gapped network is by physically inserting removable media (such as a USB drive) or connecting a laptop. If you need to enable an air gap for your Catalyst Center on ESXi deployment, complete the following steps.

Procedure

Step 1 Deploy a Virtual Appliance, ensuring that you don't configure a proxy server.

Step 2 Contact the Cisco TAC, who will enable an air gap for your network.

Upgrade to Catalyst Center 2.3.7.5 on ESXi

Before you begin

- Create a backup of your Catalyst Center on ESXi database.
- If your deployment uses a firewall, allow Catalyst Center on ESXi to access the following location on each cluster node for system and package downloads: https://www.ciscoconnectdna.com:443.

Note Only SUPER-ADMIN-ROLE users can complete this procedure.

Procedure

Step 1 In the top-right corner, a pop-up window opens, indicating that a new version of Catalyst Center on ESXi is available. Click the **Go to Software Management** link.

Note If you don't see this pop-up window, you can also click the menu icon from the top-left corner and choose **System** > **Software Management**.

Step 2 In the **Software Management** page, click **Upgrade**.

Step 3 In the **Upgrade Release** dialog box, click **Install**.

Step 4 In the **Schedule Upgrade** dialog box, specify when you want to start the upgrade, then click **Download**.

You can track the upgrade progress from the **Activities** page.

Upgrade to Catalyst Center 2.3.7.5 on ESXi in an Air-Gapped Deployment

Procedure

Step 1 Download the *.tar.gz file from the location specified by Cisco.

Step 2 Enter the following command to copy the file to the virtual appliance's **/airgap** folder:

```
scp -P 2222 *.tar.gz maglev@<appliance-IP-address>:/airgap
```

Step 3 Log in to the Catalyst Center on ESXi GUI.

Step 4 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Step 5 From the top-right corner, click **Scan**.

Step 6 After Catalyst Center on ESXi locates the files required to complete the upgrade, choose one of the following options:

- Click **PreLoad** to download the upgrade files. If you choose this option, you'll need to schedule when the upgrade will take place.
- Click **Upgrade** to download the relevant files and begin the upgrade immediately.