



Cisco Catalyst Center Global Manager Deployment Guide, Release 1.2.1

First Published: 2025-07-10

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Catalyst Center Global Manager Overview	1
	Cisco Catalyst Center Global Manager	1
	Audience	2
CHAPTER 2	Deployment Requirements	3
	Create an order to automate generation of CRS profile	3
	Firewall ports and security	4
	Additional requirements	5
CHAPTER 3	Prepare for Deployment	9
	Prepare for deployment	9
	Install VMware	9
	Download OVA for Catalyst Center Global Manager	9
	Reserve enterprise interface	10
	Import the IdenTrust certificate chain	10
	Prepare the DNS, NTP and proxy servers	11
	Enable storage input/output control	11
CHAPTER 4	Deploy Catalyst Center Global Manager	13
	Deploy Catalyst Center Global Manager VM on VMware ESXi	13
	Modes of deployment	13
	Create the Catalyst Center Global Manager VM	13
	Configure Catalyst Center Global Manager on ESXi virtual appliance	15
	Configure a virtual appliance using the maglev configuration wizard: default mode	16
	Configure a virtual appliance using the maglev configuration wizard: advanced mode	19
	Configure a virtual appliance using the web install configuration wizard	23

Configure a virtual appliance using the advanced web install configuration wizard 27

CHAPTER 5**Get Started 33**

Log in to Catalyst Center Global Manager and run it 33

First-time registration of Catalyst Center to CRS 36

Site Hierarchy 37

Rename Sites 38

Monitor from the overview dashboard 39

Monitor controller health 40

Monitor network status changes 41

Monitor health of devices 41

Alerts 42

Device Infrastructure 43

Device Health 43

Software-Defined Access 44

Endpoints 44

Situational dashboard (Beta) 45

Create Dashboard 45

Controllers 47

Cross-Launch to Controllers 52

System 360 52

System health 52

Software management 52

Global search 53

Workflows 53

Developer Toolkit 54

Activities 54

System 55



CHAPTER 1

Catalyst Center Global Manager Overview

- [Cisco Catalyst Center Global Manager, on page 1](#)
- [Audience, on page 2](#)

Cisco Catalyst Center Global Manager

Catalyst Center Global Manager is a platform that provides you with a single-pane-of-glass (SPoG) interface to easily manage multiple Catalyst Centers. Catalyst Center Global Manager integrates information from various Catalyst Center platforms into a single display.

Key features of Catalyst Center Global Manager are:

- Unified view with all the sites, inventories, and alerts of all the connected controllers.
- Enhanced administrative efficiency

Catalyst Center Global Manager provides an overview of network status changes, including alerts and visibility into well-performing sites, as well as poor-performing sites. It allows you to view and monitor summaries reported by any connected Catalyst Center, covering:

- Routing
- Switching
- Wireless
- Endpoints
- Software-Defined Access

Catalyst Center Global Manager supports up to 25 controllers and a maximum of 10 active users. Once these controllers are registered with Catalyst Center Global Manager, they will continue to monitor and control networks.

Catalyst Center Global Manager provides a global search view allowing you to search by many attributes such as IP address, hostname, MAC address, software version, client user name, application name and site name of any device or client. This enables cross-launching into the 360 view of the client or device in Catalyst Center. You can cross launch into the Catalyst Center interfaces without needing to enter your username and password again, as long as the same user exists on both systems. The passwords do not need to be the same.

Audience

This guide is designed for:

- System administrators responsible for deploying the Catalyst Center Global Manager virtual appliance, connecting controllers, and provisioning access to other users to enable further configurations.
- Network administrators responsible for monitoring aggregated network details and controller health via a Single Pane of Glass (SPOG).
- Users or operators responsible for managing or operating Enterprise-scale network infrastructure.



CHAPTER 2

Deployment Requirements

- [Create an order to automate generation of CRS profile, on page 3](#)
- [Firewall ports and security, on page 4](#)
- [Additional requirements, on page 5](#)

Create an order to automate generation of CRS profile

Ensure you select the appropriate Stock Keeping Unit (SKU) for the Catalyst Center Global Manager. You also need a valid Smart Account (SA) and Virtual Account (VA) to order Catalyst Center Global Manager.



Note You must be part of the SA and VA placing the order to register Catalyst Center Global Manager.

Registration of Catalyst Center with Catalyst Center Global Manager happens automatically using SA/VA workflow.

Before you begin deploying Catalyst Center Global Manager, you need to first create and place an order to get a license using the Cisco Commerce Workspace (CCW). After you obtain the license only, the Cloud Registration Service (CRS) profile gets created in the CRS dashboard automatically. When you order Catalyst Center Global Manager, a CRS Profile is automatically created, which is required to register Catalyst Center Global Manager and enroll Catalyst Centers into it.



Note You need to wait 3 days after placing the Catalyst Center Global Manager order to allow time for the CRS profile to be created. During the initial registration, Catalyst Center Global Manager registers itself with the CRS profile. This ensures that any new Catalyst Center can discover the Catalyst Center Global Manager IP and enroll with it seamlessly.

CRS Profile

The CRS profile is responsible for both Catalyst Center Global Manager and Catalyst Center authentication and maintains all necessary metadata required for auto-enrollment. It simplifies the process of registering Catalyst Center instances with Cisco cloud services through a centralized configuration.

Administrators configure the CRS Profile within Catalyst Center Global Manager by providing:

- **Cloud service credentials** (For example, Cisco SA details).

- **Authentication tokens** or certificates for secure communication.
- **Endpoint details** for the Cisco cloud services the instance is registering with.

Once configured, the CRS Profile ensures secure and continuous communication between the on-premises Catalyst Center instances and the Cisco cloud services.



Note Only one CRS Profile with SA/VA combination per Catalyst Center Global Manager is allowed.

Firewall ports and security

- **Firewall Access:** Must allow outbound access to ciscoconnectdna.com.
- **Connectivity:** There must be connectivity from the Catalyst Center Global Manager to the controllers, and vice versa. For Catalyst Center Global Manager, only one interface is supported for the enterprise edition.
- **Supported Infrastructure:**
 - Physical or virtual Catalyst Center appliances (single node or High Availability (HA) or Virtual Appliance (VA)).
 - VMware ESXi and vCenter, version 7.0.x or later
 - Network Time Protocol (NTP) needs to either be in synchronization between the Catalyst Center Global Manager and Catalyst Centers or maintain a maximum time difference of one second.
- **Ports needed to be opened:** Make sure the following ports are opened on the Firewall. These ports need to be opened on the firewall to enable communication with the CRS portal and allow Catalyst Center Global Manager to interact with Catalyst Centers globally.

Port	Service name	Purpose	Recommended action
Administering or configuring Catalyst Center Global Manager			
TCP 443	UI, REST, HTTPS	GUI, REST, HTTPS management port.	Port must be open.
TCP 2222	Catalyst Center Global Manager shell	Connect to the Catalyst Center Global Manager shell.	Port must be open. Restrict the known IP address to be the source.
TCP 9004	Web UI installation	Serves the GUI based installation page (required only if you decide to install Catalyst Center Global Manager using the web-based option).	Port must be open until the installation of the node is complete.
Catalyst Center Global Manager outbound to Catalyst Center and other systems			

Port	Service name	Purpose	Recommended action
TCP 49	TACACS+	Needed only if you are using external authentication such as Cisco ISE with a TACACS+ server.	Port must be open only if you are using external authentication with a TACACS+ server.
UDP and TCP 53	DNS	Used to resolve a DNS name to an IP address.	Port must be open if DNS names are used instead of IP addresses for other services (such as an NTP DNS name).
UDP 123	NTP	Catalyst Center Global Manager uses NTP to synchronize the time from the source that you specify.	Port must be open for time synchronization.
TCP 443	HTTPS	Catalyst Center Global Manager uses HTTPS for cloud-tethered upgrades, periodic polling from Catalyst Center and communication with CRS portal.	Port must be open.
UDP 1645 or 1812	RADIUS	Needed only if you are using external authentication with a RADIUS server.	Port must be open only if an external RADIUS server is used to authenticate user login to Catalyst Center.
111	NFS	Used for Assurance backups.	Port must be open.
2049	NFS	Used for Assurance backups.	Port must be open.
20048	NFS	Used for Assurance backups.	Port must be open.
TCP and UDP 32767	NFS	Used for Assurance backups.	Port must be open.

Additional requirements

Catalyst Center Global Manager is deployed as a virtual machine (VM) on VMware ESXi version 7.x or later.

The following requirements must be met in order to successfully deploy a Catalyst Center Global Manager 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, Update 3](#) (PDF)
- VMware vSphere Client 8.0: [Performance Best Practices for VMware vSphere 8.0](#) (PDF)

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. 8 vCPUs with 16 GHz reservation must be dedicated to the VM.
Hard Disk Drive (HDD)	100 GB + 550 GB (2 HDDs).
Memory	16 GB RAM.
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 Global Manager to Catalyst Center connectivity: 350 ms.
Active Sessions	Up to 10 active user connections are supported for network admins to log in to Catalyst Center Global Manager.

Server requirements

Feature	Description
vCenter and ESXi	7.0x+.
Intel CPU	2.1 GHz and later.

Supported browsers

The Catalyst Center Global Manager GUI is compatible with these HTTPS-enabled browsers:

- Google Chrome: Version 134 or later
- Mozilla Firefox: Version 120.0.1 or later

Screen resolution:

- Minimum: 1368 x 768 pixels
- Recommended: 1920 x 1080 pixels

We recommend that the client systems you use to log in to Catalyst Center Global Manager be equipped with 64-bit operating systems and browsers.

Scale numbers

The table lists the number of controllers, users and sites that Catalyst Center Global Manager supports.

Component	Maximum Number Supported
Controllers	25 controllers
Users	10 active users
Sites	25000 (maximum aggregated sites) • 100 (sites on multiple controllers) • 5 (same site on maximum number of controllers)

Security Limitations

Catalyst Center Global Manager does not support managing Catalyst Centers with:

- Disaster Recovery (DR)
- Federal Information Processing Standards (FIPS)
- IPv6 configurations-only setups
- Air-gapped configurations

User Access Roles

- Users must exist on both Catalyst Center Global Manager and Catalyst Center with matching usernames.
- Access permissions are inherited from individual Catalyst Centers.



CHAPTER 3

Prepare for Deployment

- Prepare for deployment, on page 9
- Install VMware, on page 9
- Download OVA for Catalyst Center Global Manager, on page 9
- Reserve enterprise interface, on page 10
- Import the IdenTrust certificate chain, on page 10
- Prepare the DNS, NTP and proxy servers, on page 11
- Enable storage input/output control, on page 11

Prepare for deployment

Catalyst Center Global Manager is deployed as a virtual machine (VM) on VMware ESXi version 7.x or later.

To prepare for the deployment of a Catalyst Center Global Manager on VMware ESXi virtual appliance, complete the following tasks.

Install VMware

To run Cisco Catalyst Center Global Manager on ESXi, VMware vSphere (which includes ESXi and vCenter Server) 7.0.x or later, including all patches, is required. Click [here](#) to access an overview of the installation and setup process of VMware vSphere. 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.

You can use a web browser to access the vCenter 7.0.x to deploy the OVA of Catalyst Center Global Manager virtual appliance.

Download OVA for Catalyst Center Global Manager



Note

If you purchase Catalyst Center Global Manager through CCW, there is a waiting period of three days before you can download the software. Additionally, since you have purchased Catalyst Center Global Manager, you must be part of the same SA/VA as the individual who performs the deployment during the initial setup process. However, the user who downloads the OVA file can belong to a different SA/VA.

Save the OVA files to the computer on which you will deploy Catalyst Center Global Manager. From the Cisco-provided link, download the .ova file that you will use to deploy the Catalyst Center Global Manager. The OVA can also be hosted on a web server.



Note The size of the .ova file is approximately 23 GB, and the time it takes to download is dependent on the network bandwidth.

Reserve enterprise interface

Before you configure the Catalyst Center Global Manager virtual appliance, you need to reserve one 10-Gbps enterprise interface to access the Catalyst Center Global Manager GUI. Write down the IP address for this interface, because you'll need to enter it during appliance configuration.



Note During the installation process, you must also configure a secondary interface known as the intracluster interface with a non-routable IP address. In the standard installer, this IP address is predefined and cannot be changed. If this IP address needs to be changed due to network overlap, use the Advanced installer.

The intracluster interface's IP address is predefined by Cisco, so the Maglev Configuration wizard populates this information automatically during the configuration process.

Import the IdenTrust certificate chain

The Catalyst Center Global Manager 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 Catalyst Center Global Manager host or cluster where your virtual appliance will reside, download **trustidevcodesigning5.pem** from the same location that Cisco specified to download the Catalyst Center Global Manager 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

In the Maglev Configuration wizard, you'll be prompted to specify two items:

- The Domain Name System (DNS) server that Catalyst Center Global Manager will use to convert domain names to IP addresses.
- The Network Time Protocol (NTP) server that Catalyst Center Global Manager will use for clock synchronization. The NTP server must be accessible to the Catalyst Centers, or they should maintain synchronization with a time deviation of less than one second.

Before you configure your Catalyst Center Global Manager, do these steps:

- Ensure that the servers you want to use are available and running.
- For an NTP server, obtain its IP address or hostname.
- For a proxy server, obtain either its URL or IP address 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/output (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**.
-



CHAPTER 4

Deploy Catalyst Center Global Manager

- [Deploy Catalyst Center Global Manager VM on VMware ESXi, on page 13](#)
- [Modes of deployment, on page 13](#)
- [Create the Catalyst Center Global Manager VM, on page 13](#)
- [Configure Catalyst Center Global Manager on ESXi virtual appliance, on page 15](#)

Deploy Catalyst Center Global Manager VM on VMware ESXi

This section includes the modes of deployment and the necessary steps required to deploy Catalyst Center Global Manager VM on ESXi 7.0 or later. Before the deployment, ensure that you have downloaded the OVA of Catalyst Center Global Manager.

Modes of deployment

Catalyst Center Global Manager can be deployed by using the:

- Configuration wizard or command-line interface (CLI)
- Web install or graphical user interface (GUI)

Catalyst Center Global Manager deployment has the following capabilities:

- Deploy Catalyst Center Global Manager on VM (VMware ESXi/vCenter).
- Ability to install Catalyst Center Global Manager using two deployment modes—CLI or web install.

Create the Catalyst Center Global Manager VM

Use the **Deploy OVF Template** wizard in the VMware vSphere Web Client to deploy the OVF-formatted file.

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

Procedure

Step 1 Download the Catalyst Center Global Manager OVA file from the location specified by Cisco.

Step 2 Log in to the VMware vSphere Web Client using the applicable credentials.

The **VMware vSphere Web Client** page opens.

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**.

The **Deploy OVF Template** wizard opens.

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 field populates with the OVA file name you're about to create. Additionally, the path shows the location within the Navigator directory where the ESXi host or cluster is listed, which corresponds to the deployment location you chose previously in Step 3.

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

Optionally, if you want to use different values such as naming the VM or selecting a different folder location in the VMwarevSphere Web Client directory, 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**.

The **Review details** page opens that lists deployment template details.

- 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**.

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

- e) On the **Select storage** page, 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.

Note

Thick Provision is recommended here.

3. In the **VM Storage Policy** drop-down list, keep the **Datastore Default**.
4. Click **Next**.

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

- f) To assign the interface that Catalyst Center Global Manager will use, on the **Select networks** indicate the interface that connects the system to the enterprise network. Do the following:

1. In the **VM Network** drop-down list, choose the interface that connects the system to the enterprise network.

Note

This interface/IP address is used for UI/SSH access to Catalyst Center Global Manager as well as establishing connection with controllers. So connectivity to and from the controllers must be ensured through this IP.

Only one NIC is supported for Catalyst Center Global Manager VM.

2. Click **Next**.

The **Ready to complete** wizard page opens and displays a summary of the deployment settings you've entered.

- 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 and make the changes.
- If the settings are correct and you want to proceed with deployment, click **Finish**.

The **Deploy OVF Template** wizard closes and the deployment of the Catalyst Center Global Manager begins immediately.

Important

- In general, deployment takes around 45 minutes to complete. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.
- Available bandwidth, vCPUs, and RAM and hard disk space can affect the time that this process takes.
- When the tasks are completed, you can power on the virtual machine and configure it.

Configure Catalyst Center Global Manager on ESXi virtual appliance

Before using Catalyst Center Global Manager, you must first complete the relevant appliance configuration workflow according to your requirements. Complete one of the following procedures to configure Catalyst Center Global Manager on ESXi virtual appliance on a VMware ESXi host.

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 intracenter interface is preconfigured when using this wizard.

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

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 after you power it on. 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>>** to advance to the next screen for CLI based installed.

The **Welcome to Maglev Configuration Wizard** window opens. Select Catalyst Center Global Manager and then hit **Enter**.

- b) Click **Create Catalyst Center Global Manager Virtual Appliance**.
- c) Select the **Start using MKS pre manufactured cluster** option.

The premanufactured cluster option allows for a faster install time but does not allow for the customization of the cluster port.

- d) Select the manufacture cluster. It will take you to a series of maglev configuration wizard questions.

1. This is the enterprise address. Its purpose is to enable Catalyst Center Global Manager to communicate with and manage your network.
 2. Click **Next** to proceed to the next screen. This is the cluster default IP address. No need to do any changes here.
- e) Enter the configuration values for **NETWORK ADAPTER #1**, as shown in the following table, then click **next>>** to proceed the wizard to validate the host networking.

Host IP address	Enter the IP address for the Enterprise port.
Netmask	Enter the mask for your IP address.
Default Gateway IP Address	Enter the default gateway IP address to use for the port.
Static routes	If a Default gateway is entered, then there is no need for static routes.

The wizard validates the settings after the DNS step. If you receive an error message, check that the value you entered is correct, then reenter it. If needed, click <<**back** to reenter it. This process will take approximately 4 to 5 minutes.

- f) You do not need to enter configuration values for **NETWORK ADAPTER #2**. The **NETWORK ADAPTER #2** is the cluster port. If **pre manufactured** was selected, these values will be prepopulated and can not be changed. If advance install was selected, please enter the desired cluster interface information. Select **next>>** to proceed.
- g) In the **DNS Configuration** page, enter the IP address of the preferred DNS server and then select **next>>**. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.

Important

Configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for a virtual appliance.

- h) Do one of the following:
- If you need to change any settings, select <<**back** as needed, make the necessary changes, and then return to this wizard page.
 - If you're happy with the settings you've entered, select **proceed>>**.
- i) After the network adapter configuration is complete, the wizard prompts you to enter configuration values for the **NETWORK PROXY** you are using.

After validation successfully completes, do one of the following:

- If your network does *not* use a proxy server to access the internet, select **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 select **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 Global Manager 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.
----------------------------	---

- j) (Optional) 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.

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

- Catalyst Center Global Manager 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 it manages.

After you provide the necessary information, select **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 select **next>>**.

Linux Password field	Enter and confirm the password for the <code>maglev</code> user. Note According to the CLI password policy, your new password must differ from the last 24 passwords you have used.
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 select **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. The Catalyst Centers and the Catalyst Center Global Manager are required to either use a common NTP or achieve synchronization with a maximum time difference of one second between them. Note For NTP, ensure port 123 (UDP) is open between Catalyst Center Global Manager and your NTP server.
-------------------	---

NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center Global Manager, 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, select **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 to 30 minutes for services to be stabilized so that you can log in to the virtual appliance GUI.

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

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 select **skip>>**.
- b) Click **Create Catalyst Center Global Manager Virtual appliance**.
- c) Select 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) Select **proceed>>**.

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

- e) Select **next>>**.
- f) You don't need to enter any settings in the **Layer2 mode used for the services** wizard page, so select **next>>**.
- g) Enter the configuration values for **NETWORK ADAPTER #1**, as shown in the following table, then select **next>>**.

Catalyst Center Global Manager uses this interface to link the virtual appliance with your network.

Host IPv4 Address field	Enter the IP address for the Enterprise interface. This is required.
IPv4 Netmask field	Enter the netmask for the interface's IP address. This is required.
Default Gateway IPv4 Address field	Enter a default gateway IP address to use for the interface.
IPv4 Static Routes field	Enter one or more static routes in the following format, separated by spaces: <network>/<netmask>/<gateway>.
Cluster Link field	Leave this field blank. It is required on the Intracenter 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, select <<**back** to reenter it.

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

Important

Configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for a virtual appliance.

- i) Do one of the following:
 - If you need to change any settings, select **<<back** as needed, make the necessary changes, and then return to this wizard page.
 - If you're happy with the settings you've entered, select **proceed>>**.
- j) After the network adapter configuration is complete, the wizard prompts you to enter configuration values for the NETWORK PROXY you are using, as shown below.

HTTPS Proxy field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. Note Connection from Catalyst Center Global Manager 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 validation successfully completes, do one of the following:

- If your network does *not* use a proxy server to access the internet, select **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 above table), then select **next>>**.
- k) (Optional) 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.

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

- Catalyst Center Global Manager 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 Global Manager manages.

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

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

Linux Password field	Enter and confirm the password for the <code>maglev</code> user. Note According to the CLI password policy, your new password must differ from the last 24 passwords you have used.
----------------------	--

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).

- m) Enter the configuration values for the settings provided in the wizard's **NTP SERVER SETTINGS** page (as described in the following table), then select **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. The Catalyst Centers and the Catalyst Center Global Manager are required to either use a common NTP or achieve synchronization with a maximum time difference of one second between them. Note For NTP, ensure port 123 (UDP) is open between Catalyst Center Global Manager and your NTP server.
NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with, 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.

- n) 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 Global Manager 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 Global Manager on 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 Global Manager 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 Global Manager 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.

- o) To apply the settings you've entered to the virtual appliance, select **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.

Configure a virtual appliance using the web 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. For more information on "supported browsers", see the [Deployment requirements](#) section.

Ensure that you enabled ICMP on the firewall between Catalyst Center Global Manager 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 Global Manager and the DNS server 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:

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

- In the **STATIC IP CONFIGURATION** page, do one of the following:
 - Select **skip>>** to go to the CLI based install.
 - 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 select **configure>>**.

For IPv4 deployments, this check box needs to be unchecked.

IPv6 Mode check box	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.

- Open the URL that was displayed in the **Static IP Configuration** page.
- Click the **Start a Cisco Catalyst Center Global Manager** radio button, then click **Next**.

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

The **Overview** window 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 Global Manager 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**.

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 Global Manager, 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 Global Manager 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 Global Manager 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**.

Note

According to the CLI password policy, your new password must differ from the last 24 passwords you have used.

This is the username and password to access the CLI for troubleshooting. After logging in, you'll be prompted to configure a new admin user (as a security measure).

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 Global Manager virtual appliance, click **Start Configuration**.

The **Appliance Configuration in Progress** page 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, the **Appliance Configuration Complete!** page opens. Then click the copy icon to copy the default admin superuser password.

Important

Catalyst Center Global Manager 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 Global Manager for the first time.

Note

As a security measure, you'll be prompted to setup a new username and password after you log in. The default admin account will be deleted.

Configure a virtual appliance using the advanced web 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.

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:

- Select **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 select **configure>>**.

For IPv4 deployments, this check box needs to be unchecked.

IPv6 Mode check box	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.

- Open the URL that was displayed in the **Static IP Configuration** page.
- Click the **Start a Cisco Catalyst Center Global Manager** radio button, then click **Next**.
- Click the **Advanced Install** radio button, then click **Start**.

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

- 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:

- Click **Next**.

The **How would you like to set up your virtual 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 Global Manager 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 Global Manager 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.

- 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 Global Manager 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 Global Manager 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**.

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 Global Manager, 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 Global Manager 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 Global Manager 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**.

Note

According to the CLI password policy, your new password must differ from the last 24 passwords you have used.

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 Global Manager virtual appliance, click **Start Configuration**.

The **Appliance Configuration in Progress** page 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, the **Appliance Configuration Complete!** page opens. Then click the copy icon to copy the default admin superuser password.

It can take from 15 to 30 minutes for services to be stabilized before you can log in to the GUI.

Important

Catalyst Center Global Manager 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 Global Manager for the first time.



CHAPTER 5

Get Started

- [Log in to Catalyst Center Global Manager and run it, on page 33](#)
- [First-time registration of Catalyst Center to CRS, on page 36](#)
- [Site Hierarchy, on page 37](#)
- [Monitor from the overview dashboard, on page 39](#)
- [Alerts, on page 42](#)
- [Device Infrastructure, on page 43](#)
- [Endpoints, on page 44](#)
- [Situational dashboard \(Beta\), on page 45](#)
- [Controllers, on page 47](#)
- [Global search, on page 53](#)
- [Workflows, on page 53](#)
- [Developer Toolkit, on page 54](#)
- [Activities, on page 54](#)
- [System, on page 55](#)

Log in to Catalyst Center Global Manager and run it

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

Before you begin

The first-time setup requires you to create and place an order to obtain a license through the Cisco Commerce Workspace (CCW). Once the license is obtained, a profile is automatically created in the Cloud Registration Service (CRS) dashboard. You can then use the same virtual account to retrieve the license as part of first-time setup workflow.



Note A waiting period of approximately three days is needed between placing an order in Cisco Commerce Workspace (CCW) and the Day 0 First Time Setup (FTS) in Catalyst Center Global Manager.

Procedure

Step 1 Access the Catalyst Center Global Manager GUI by using HTTPS:// and the IP address of the Catalyst Center Global Manager GUI that was displayed at the end of the configuration process.

The Catalyst Center Global Manager login page is displayed.

Note

It is recommended to use a private or incognito browser window when accessing the GUI. Ensure that you are using a supported browser. For more information on "supported browsers" and "screen resolution", see the [Deployment requirements](#) section.

Step 2 Log in to Catalyst Center Global Manager with the login credentials. Enter the default username and password you configured for the new admin user.

- In the **Username** field, type **admin**
- In the **Password** field, type **P@ssword9**

Note

These are the default login credentials for accessing the GUI for the first time and it will be deleted once a new user account is created in step 3.

Step 3 Create a new user account for Catalyst Center Global Manager after the password is authenticated.

- Catalyst Center Global Manager will log out and you need to login back using the new user account created.
- Each of the controllers managed by Catalyst Center Global Manager should have an identical user account created on it.

Step 4 Click **Log In**.

The Catalyst Center Global Manager **First Time Setup** window is displayed.

Here, you will need to enter the email address associated with the Smart Account or Virtual Account that was used to purchase the Catalyst Center Global Manager.

Step 5 Click **Continue**.

The **Terms and Conditions** window is displayed, providing links to the **Cisco General Terms** (formerly known as End User License Agreement (EULA)) and any supplemental terms that are currently available.

Step 6 Click **Next** to accept the terms and conditions.

Activate your device window is displayed.

Step 7 Click **Next** to activate the Catalyst Center Global Manager to Cisco Catalyst Cloud.

Cisco Catalyst Cloud window is displayed where you will be presented with a pop-up and a code.

Note

Make sure that you enable the pop-ups for the page in the browser.

After you have logged in successfully, the screen will show the registration status between the Catalyst Center Global Manager and the Cisco Catalyst Cloud.

Note

In case you fail to log in, you will get a failure message stating that you are unable to complete registration with Cisco Catalyst Cloud due to authentication issue. In this scenario, you need to sign in again after a few minutes or check your browser pop-ups settings.

Step 8

Enter the virtual account administrator email and password to register Catalyst Center Global Manager to Cisco Catalyst Cloud. Upon successful registration of the Catalyst Center Global Manager with the CRS Profile using the virtual account administrator email, you should observe that the device is activated and registered.

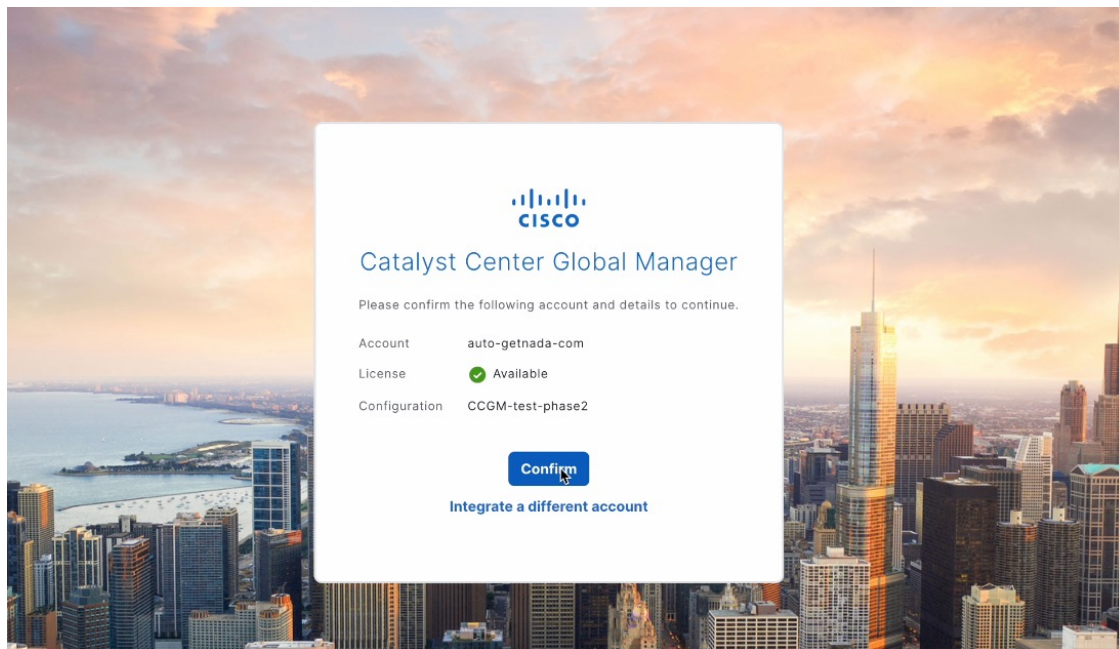
Note

View the CRS profile configuration details once the profile is successfully claimed in Catalyst Center Global Manager.

Step 9

Click **Confirm** to enter the Catalyst Center Global Manager GUI dashboard for the first time.

Figure 1: First-time login setup



You will be redirected to the **Overview** page within Catalyst Center Global Manager, with instructions to enroll the Catalyst Center controller.

Note

Only a few menu options are shown in the menu because no controllers are enrolled.

The Catalyst Center Global Manager can have a different admin user, with the only requirement being that the user's email id must be connected to the same VA that is tied to the CRS profile.

First-time registration of Catalyst Center to CRS

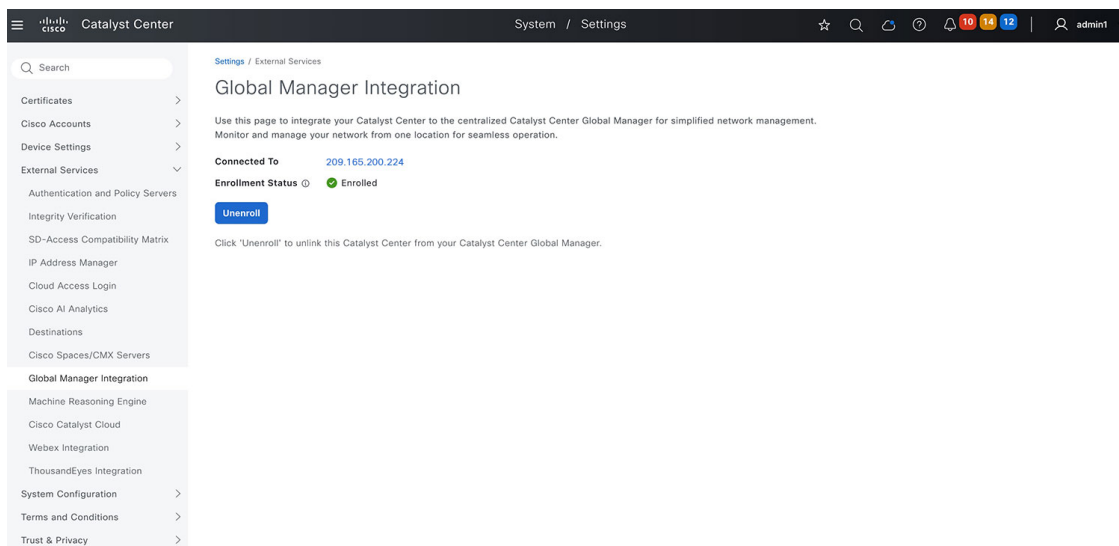
To register Catalyst Center with Catalyst Center Global Manager, it's necessary to integrate Catalyst Center with the CRS dashboard. Begin this process by logging in to Catalyst Center.



Note The minimum supported version of the Catalyst Center is 2.3.7.9.

Procedure

-
- Step 1** From the menu () icon, choose **System** > **Settings**.
The **Settings** window is displayed.
- Step 2** Search for **Global Manager Integration** and click **Enroll**.
The **Activate your device** window is displayed. You will be shown an **Activation Code** here.
- Step 3** Click **Next** to activate Catalyst Center to the CRS dashboard. At this point, enter the email and password associated with your Cisco Virtual Account.
The **Device activated** window is displayed after the Catalyst Center registers to the CRS Profile with the virtual account administrator email.
Catalyst Center connects to the CRS dashboard, where it locates the **Profile** you previously set up containing the Catalyst Center Global Manager IP address. Then, it transmits authentication details to Catalyst Center Global Manager to establish a connection with Catalyst Center Global Manager.
After you click **Enroll**, Catalyst Center establishes a connection with the Catalyst Center Global Manager at the IP address where you previously set up the **Profile**.
Click **Unenroll** if you want to unlink the Catalyst Center from your Catalyst Center Global Manager.



What to do next

Go to the Catalyst Center Global Manager dashboard, you will see a toast notification for the newly enrolled controller, with a **Refresh** link to update the page and view data from the controller.

Additionally, menu options will be updated, and you can go to the **Controllers** page, view the new Catalyst Center added to Catalyst Center Global Manager.



Note

You can view the configured **CCO** account through **Enroll** in the **System > External Services > Cisco Catalyst Cloud** page.

Site Hierarchy

The **Site Hierarchy** selector in Catalyst Center Global Manager offers an aggregated view of all sites across different controllers. When multiple controllers share the same site (for example, Global/USA/East Coast), those sites are combined and presented as a single node in the site selector. The content displayed on the pages will be filtered based on the site that you select. An unfiltered view is also available.

The **Site Hierarchy** selector lists the first 100 nodes at each level. You can search for a specific site by entering a string and then click **Enter** or the **Search** button to initiate the search.

Refresh site hierarchy

There are effectively three scenarios to trigger a refresh of site hierarchy:

1. If there any updates on the sites in any of the controllers, you need to manually click the **Refresh** button in the site selector to reload the data from all the controllers.
2. If any updates on the controller's reachability, such as updates on the controller or changes in reachability (for example, a controller becoming reachable or unreachable), then a manual **Refresh** is required in the site selector.



Note Selecting a site will reflect the network health and alerts data on the **Overview** dashboard, as well as the other second-level pages data.

The network health and alerts are specific to each site, whereas the controller health is not site-specific.

3. In case of any error while populating the site data, an error count shows up in the bottom bar next to the **Refresh**.

The site selector does not automatically refresh for all changes; it only automatically refreshes the controller's sites in response to specific events such as:

- Controller enrollment with toast notification refresh.
- Unenrollment with toast notification refresh.

For these events, there's no need to manually click the **Refresh** button. In contrast, an on-demand refresh in the Catalyst Center Global Manager site selector is required when there are changes to the sites on the controller side, such as adding, deleting, or modifying sites.

Rename Sites

You can rename sites in the **Site Hierarchy** from **Site management** for all related controllers. These modifications get configured on the Catalyst Centers.



Note You can only rename the buildings and areas; the global site and floors cannot be renamed.

You can edit the sites as long as they are included in the site hierarchy, regardless of whether they are fabric sites or non-fabric sites. There is no support for fabric zones functionality in Catalyst Center Global Manager, which means that the Catalyst Center Global Manager does not provide functionality to configure fabric zones.

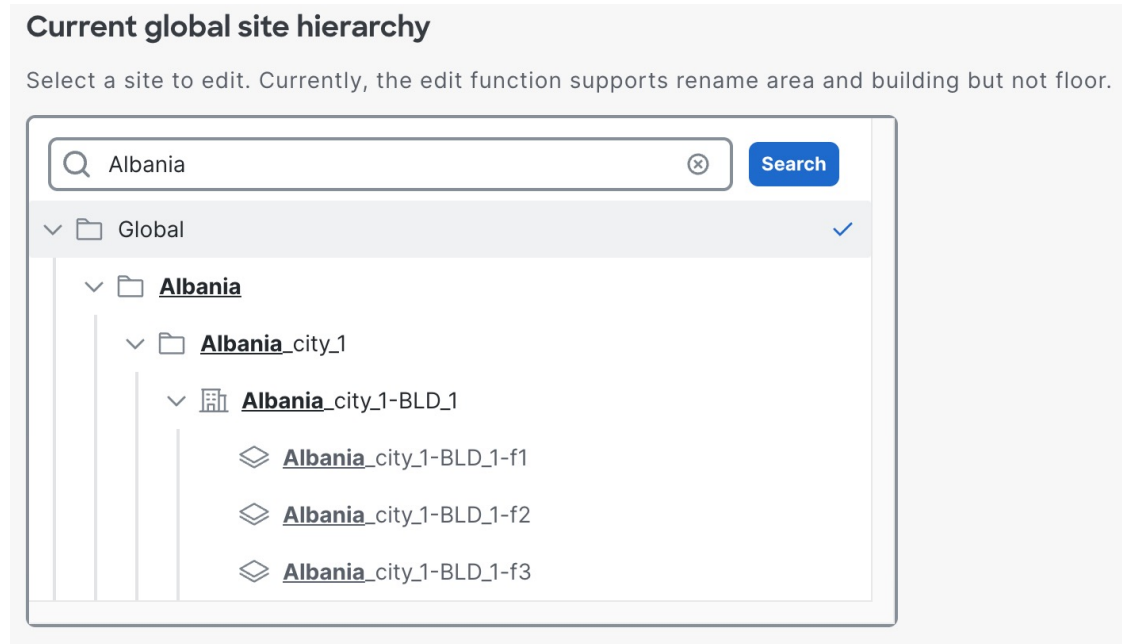
Procedure

- Step 1** From the Catalyst Center Global Manager dashboard, go to the **Site Hierarchy Global > Site management** to rename the site.
- The **Site Hierarchy Management** window appears.

Step 2 Locate the site you want to rename and click **Search** on the **Site Hierarchy Management** page.

Step 3 Click on the site you want to rename.

A popup window appears showing the impacted controllers for this site.



Step 4 On the Edit page, update the site name or other relevant details as needed.

Step 5 Click on the **Save** button to apply the changes.

The site gets renamed successfully and the modified site name is reflected in the site selector.

Note

In the site selector, the modified site name appears immediately; however, on other second-level pages such as **Alerts**, **Endpoints**, **Health**, and **Software-Defined Access**, it takes approximately 15 to 30 minutes for the new site name to reflect.

If any errors occur, they are displayed in the final status of the operation.

Monitor from the overview dashboard

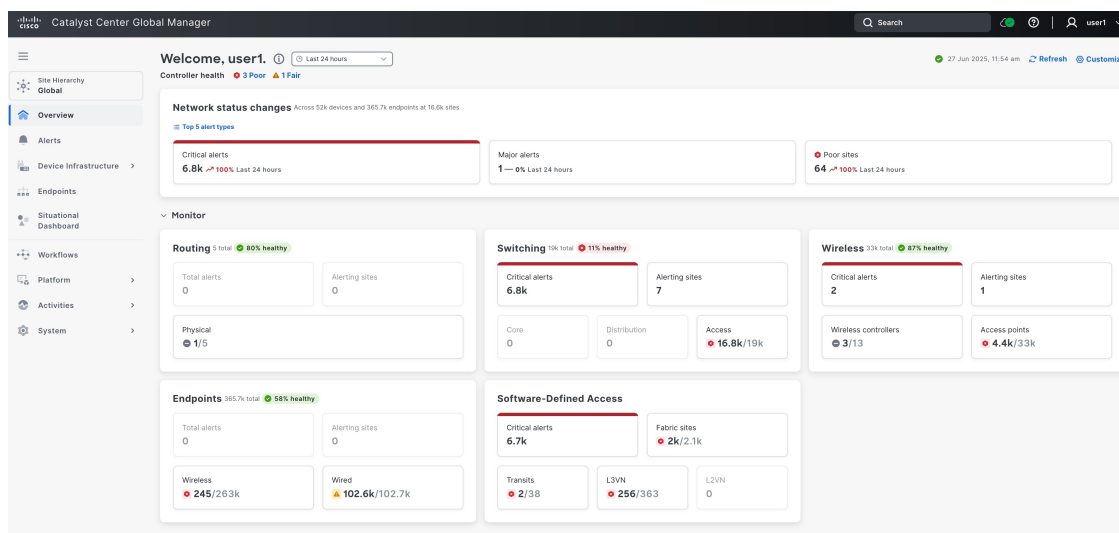
The Catalyst Center Global Manager **Overview** page includes controller health and additional details about individual controllers.

When you log in to Catalyst Center Global Manager after adding controllers, Catalyst Center Global Manager starts rendering the data on the **Overview** page progressively. You can see a progress bar on the **Overview** page when the data loads incrementally as Catalyst Center Global Manager receives data from the enrolled controllers. This process is known as progressive loading.

After all the enrolled controllers responded with data, the progress bar turns green. The progress bar disappears within 15 seconds after the data load is complete.



Note If there is any error in the data fetching from the enrolled controllers, then the progress bar with error alerts will be shown on the page. You can mouse over to see how many controllers have responded. You can further drill down the details about the individual failure by clicking the loading status icon located near the date and time to view the specific failure details for each dashlet in the **Overview** page.



Note Click **Refresh** to update the information displayed, ensuring you have the most current status of your network devices and components. This will provide you with the latest data on device health, performance, and any ongoing issues.

Click **Customize** to rearrange the dashlets within the different sections of the **Overview** page.

Monitor controller health

Support is available to view the controller health status from Catalyst Center Global Manager for individual Catalyst Centers.

From the Catalyst Center Global Manager **Overview** page, click on the controller's health status. This action will redirect you to the **Controllers** page within the Catalyst Center Global Manager displaying filtered data based on your selection.

Procedure

- Step 1** From the Catalyst Center Global Manager dashboard, go to the **Overview** page and click on the controller health status to view the health of the number of controllers shown, or go to the **System > Controllers** to view the same.
- Step 2** Click one of the controller's name to view the details and do the cross-launch to respective controller **System health** to view the health details and troubleshoot.

After this, you can proceed with additional troubleshooting steps on the Catalyst Center.

For information about controllers, see the [Controllers](#).

Monitor network status changes

Network status changes provides an overview of networks across all devices and endpoints at multiple sites managed by all the Catalyst Centers. This information allows you to identify potential issues that may need to be addressed.

Procedure

From the Catalyst Center Global Manager dashboard, go to the **Overview** page to view the **Network status changes** section.

You can view these dashlets under **Network status changes**:

- Critical Alerts
 - Major Alerts
 - Poor Sites
-

Monitor health of devices

Monitor the following summaries and health of the devices:

- **Routing** allows you to view:
 - Minor alerts
 - Alerting sites
 - Physical
- **Switching** allows you to view:
 - Minor alerts
 - Alerting sites
 - Core
 - Distribution
 - Access
- **Wireless** allows you to view:
 - Minor alerts

- Alerting sites
- Wireless controllers
- Access points
- **Endpoints** allows you to view:
 - Minor alerts
 - Alerting sites
 - Wireless
 - Wired
- **Software-Defined Access summaries** allows you to view:
 - Total alerts
 - Fabric sites
 - Transits
 - L2 VN
 - L3 VN

Clicking on each sub-card count opens the corresponding second-level pages, such as **Alerts**, **Health**, **Software-Defined Access**, and **Endpoints**.

Alerts

The **Alerts** feature in Catalyst Center Global Manager allows you to view and explore details about alerts that require your attention. This includes information on different alert types and analytics, highlighting the top site groups and segment types of individual alert.

To view the alerts, navigate to the Catalyst Center Global Manager dashboard and click **Alerts**. Then the data gets loaded on this page progressively as it receives the data from the enrolled controllers.

The alerts are categorized into four levels:

- Critical
- Major
- Minor
- Informational

To see more information about a specific alert, click the alert type name on **Alert types** to cross-launch or navigate to their respective controller.

The **Alerts** page also gives information on:

- Analytics- Analytics shows the top site groups and top segment types.

- Alert types- Alert types display a table of all alerts filtered by priority, segment type, and category.

Device Infrastructure

The **Device Infrastructure** in Catalyst Center Global Manager provides filtered details of each device health and fabric site, ensuring that all devices and fabric sites are functioning optimally and securely.

Device Health

To view the health status of each device, navigate to the Catalyst Center Global Manager dashboard and click **Device Infrastructure > Health**. Then the data gets loaded on this page progressively as it receives the data from the enrolled controllers.

The health status categories are:

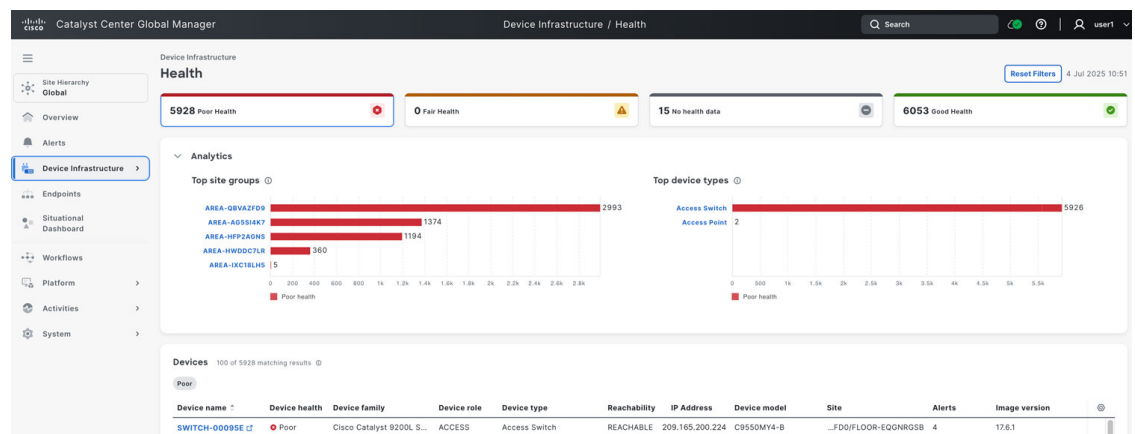
- Poor Health- Devices with a health score range from 1 to 3.
- Fair Health- Devices with a health score range from 4 to 7.
- No Health Data- Devices with no data.
- Good Health- Devices with a health score range from 8 to 10.

To see more information about a specific device, click the device name on **Devices** to cross-launch or navigate to their respective controller **Device 360** page.

The **Health** page also gives information on:

- Summary- Summary of network health based on each health category.
- Analytics- Analytics shows the top site groups and top device types.

You can interact with site groups and device types by selecting and unselecting the filter and based on the devices that are listed in a table as shown in the image.



For example: When a site group is selected from the **Top site groups** chart, the **Top device types** chart will highlight the device types associated with that selected site group. Conversely, selecting a device type from the **Top device types** chart will highlight the site groups in the **Top site groups** chart that include those device types.

You can select filters from both the **Top site groups** and **Top device types** analytics sections simultaneously. The **Devices** table below will then display devices filtered by the combination of these selected criteria, with the active filters visually highlighted. Unselecting a site group or device type selection from the analytics charts will clear the corresponding filter and update the **Devices** table accordingly.

- **Devices**- Devices display a table of all devices with device name, device health, device family based on your selection.

The devices table displays only 100 entries.

Software-Defined Access

To view the Software-Defined Access health status of each fabric site, transit, layer 3 virtual network (L3 VN), and layer 2 virtual network (L2 VN), navigate to the Catalyst Center Global Manager dashboard and click **Device Infrastructure > Software-Defined Access**. Then the data gets loaded on this page progressively as it receives the data from the enrolled controllers.

The health status categories are:

- **Poor Health**- Devices with a health score range from 1 to 3.
- **Fair Health**- Devices with a health score range from 4 to 7.
- **No Health Data**- Devices with no data.
- **Good Health**- Devices with a health score range from 8 to 10.

The **Software-Defined Access** page also gives information on:

- **Fabric site health**- It displays a table of fabric sites.
- **Transit health**- It displays a table of transits.
- **Layer 3 virtual network health**- It displays a table of L3 VNs.
- **Layer 2 virtual network health**- It displays a table of L2 VNs.

Endpoints

To view the endpoints, navigate to the Catalyst Center Global Manager dashboard and click **Endpoints**. Then the data gets loaded on this page progressively as it receives the data from the enrolled controllers.

Endpoints are also now available on the second-level page of the Catalyst Center Global Manager apart from the endpoints dashlet on the **Overview** dashboard.

It gives the health details about both wireless and wired endpoints. Both the wireless and wired endpoints populates top site groups and top metrics information. The **Endpoints** page, like other second-level pages in the Catalyst Center Global Manager, also provides additional health categories.

To see more information about a specific endpoint, click the **Endpoint** name on the **Endpoints** page of wireless or wired endpoints to cross-launch or navigate to their respective controller page.

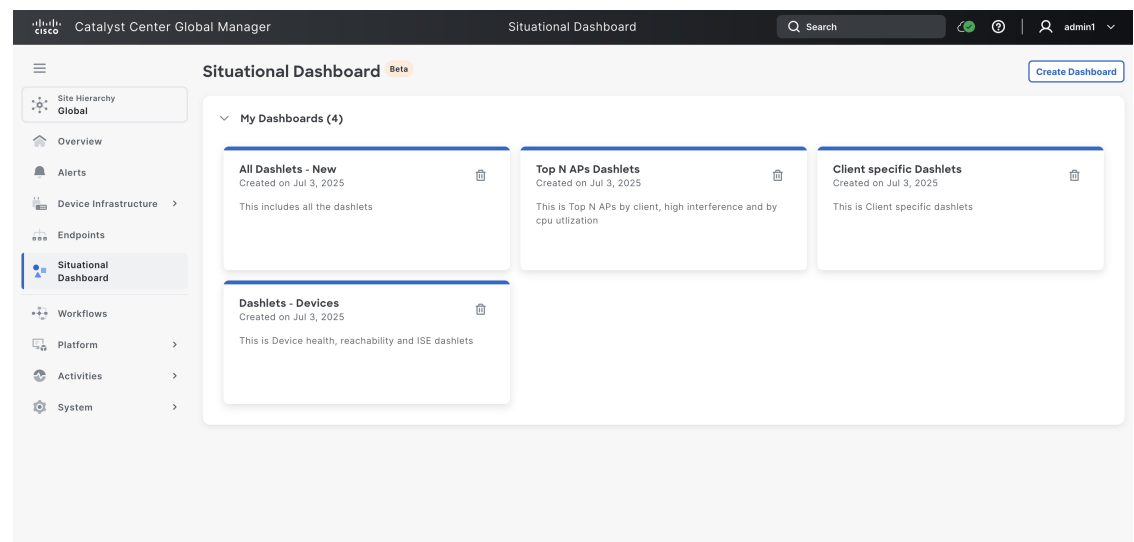
To see more information about **Connected AP**, click the Access Point (AP) name on the **Endpoints** page of wireless or wired endpoints to cross-launch or navigate to their respective controller **Device 360** page of the specific AP page.

To see more information about **Connected AP**, click the Access Point (AP) name on the **Endpoints** page wireless endpoints to cross-launch to their respective controller **Device 360** page of the specific AP page. Similarly, to see more information about **Connected Switch**, click the connected switch name on the **Endpoints** page wired endpoints to cross-launch to their respective controller **Device 360** page of the specific controller switch page

Situational dashboard (Beta)

A situational dashboard enables you to design custom pages using pre-built dashlets available in Catalyst Center Global Manager, based on your requirements. The dashboard provides aggregated views of client and device health, connectivity, and performance metrics.

To view the situational dashboard, navigate to the Catalyst Center Global Manager dashboard and click **Situational Dashboard**. Then the data gets loaded on this page progressively as it receives the data from the enrolled controllers.



Create Dashboard

Procedure

- Step 1** From the Catalyst Center Global Manager dashboard, navigate to **Situational Dashboard** > **Create Dashboard** to create a customised page using the 12 available pre-defined dashlets.
- Step 2** Enter the **Dashboard Title**, enter the **Description**, and choose the views you want to enable in your dashboard from these dashlets.
 - Client onboarding times

- Client roaming times
- Client connectivity Received Signal Strength Indicator (RSSI)
- Client connectivity Signal-to-Noise Ratio (SNR)
- Client count per Service Set Identifier (SSID)
- Client physical link connectivity
- Top Access Points (APs) by client count
- Top APs by high interference
- Top APs by CPU utilization
- Device health count
- Total network reachability
- Identity Services Engine (ISE)

Step 3 Click **Save**.

Your customised page appears as one of the dashboards you have created under **My Dashboards**.

Step 4 Click the page you have created to get the aggregated view of data with multiple controllers.

Note

Click **Refresh** to update the information displayed, ensuring you have the most current status.

Click **Customize** to edit the dashboard.

You can switch between the created dashboard using the drop-down selection on dashboard title arrow icon.

Controllers

After the Catalyst Centers have been enrolled to Catalyst Center Global Manager, you can view all the Catalyst Centers on the **Controllers** page.

There are two ways to navigate to the **Controllers** page.

- From the **Overview** page, click on the controller health status.
- Alternatively, from the **System > Controllers** page.

Then select the controller name for more detailed information.



Note The health status of the controller may take up to 10 minutes to be displayed.

The **Controllers** page displays these details:

Controller	IP address	Health	Connectivity	System version	Cluster configuration	Type
Controller 1	209.165.200.224	Fair	Reachable	3.1.3-75664	single-node	Catalyst Center
Controller 2	209.165.200.225	Poor	Reachable	3.1.3-75664	single-node	Catalyst Center
Controller 3	209.165.200.226	Poor	Reachable	3.1.3-75667	3-node	Catalyst Center
Controller 4	209.165.200.227	Poor	Reachable	2.3.7.9-75335	single-node	Catalyst Center



- Note**
- **Controller**—Name of the Catalyst Center controller.
 - When the controller is upgraded to the latest version, the **System version** column on the controller page will automatically display the new updated version.

Click one of the **Controllers** to view the controller details. The **Controller Details** window appears from where you can click on any of the links to cross-launch to the controller page for further information.

The **Controller Details** include:

- **Controller name**- Shows the name of the controller which is displayed as an IP address.
- By default, name of the controller is populated during enrollment with the hostname configured in Catalyst Center controller or their VIP address or management or Enterprise interface IP address. However, you have the option to update the name to a customized one using the **Edit** feature on the controller page.



Note You can edit only the **Controller** name and the edited name is visible only on the **Controllers** page within the Catalyst Center Global Manager, and it will not propagate to the controller itself.

- **View details**- Shows the cross-launch link to **System 360**.
- **IP Address**- Shows the IP addresses of all the controllers that have been added to Catalyst Center Global Manager.
- **Connectivity**: Shows whether the controllers are reachable or unreachable.
- **Health status**- Shows the health of all the controllers.
- **Description**- Shows the domain system certificate, alert or any system health event description of all the controllers.
- **Type of controller**- Shows whether the controller is Catalyst Center.
- **Enterprise VIP**- Shows the virtual IP address of the controller.
- **Cluster configuration**- Shows whether the controller is single-node or 3-node.
- **System Version**- Shows the software versions running on Catalyst Centers.
- **Cloud Member ID**- Shows the Cloud member ID of the controller.
- **Last collected on**- Shows the controller details collected date.



Note

-
- You can edit only the name of the controller.

The name will determine how the controller is labeled in Catalyst Center Global Manager, but it will not be reflected on the controller itself. This is strictly a UI setting and does not affect the controller's configuration. Additionally, this name will not be visible when you cross-launch to the controller.

If you want to edit the controller, click one of the **Controllers** name that you want to edit. The **Controller Details** window is displayed. Click **Edit** and change the controller's name and then save.

Controller Details



View controller details, or cross launch to controller for further details.

Controller name 209.165.200.224

View details [System 360](#)

IP address ⓘ 209.165.200.224

Connectivity Reachable

Health status Fair

[System health](#)

Description The following URLs are not reachable directly: ... ⓘ
 A newer Cisco trusted certificate bundle is avai... ⓘ

Type of controller Catalyst Center

Enterprise VIP 209.165.200.224

Cluster configuration single-node

Node hostname 209.165.200.224

Node health Good

Enterprise IP 209.165.200.224

Node serial number FCH2202W015

System version 3.1.3-75664

[Software management](#)

Cloud member ID 681b1dec591d004dbb6164d3

Last collected on 27 Jun 2025, 2:10 pm

Cancel

Edit

- You can edit the table settings.

You can decide what you want to see and what you want to hide from the **Controllers** page. For this, you can change the table settings of the **Controllers** page by clicking the gear icon on the table header. The **Table Settings** window is displayed. You can check or uncheck the items under **Table Density** and **Table Columns** based on your requirement and click **Apply**.

Cross-Launch to Controllers

The **Controllers** page displays the following types of cross-launches in the **Controller Details** for a selected controller—system 360, system health, and software management.

Cross-launch is available from all pages within the Catalyst Center Global Manager. With a single login to the Catalyst Center Global Manager, you can access all registered controllers without the need to log in again.

System 360

The **System 360** provides detailed information about the app stacks and services running on the selected Catalyst Center. You can use this information to assist in troubleshooting issues with specific applications or services.

Procedure

Step 1 In the **Controllers** page, click one of the controllers.

The **Controller Details** window is displayed.

Step 2 Click **System 360** to view the details.

A new window opens from the Catalyst Center Global Manager dashboard after cross-launching to a specific page of the selected controller.

Note

For cross-launch to function properly for an enrolled Catalyst Center, the same users in Catalyst Center Global Manager must exist in all the controllers managed by Catalyst Center Global Manager.

System health

The **System Health** provides detailed information about the health of the selected Catalyst Center from the **Controllers** page.

When you click **System Health** in the **Controller Details** window of the selected controller, the system cross-launches to the corresponding Catalyst Center page.

Software management

The **Software Management** displays the available installed applications or system updates of the selected Catalyst Center from the **Overview** page.

When you click **Software Management** in the **Controller Details** window of the selected controller on the **Overview** page, the system cross-launches to the corresponding controller page.

Global search

Global search box is available in the top-right corner of the Catalyst Center Global Manager home page. It supports searches based on MAC address, platform, software version, and IP address. You can use it to search for these categories:

- Devices
- Endpoints
- Applications
- Sites
- Users

For instance, from the Catalyst Center Global Manager home page, click the global search bar at the top right to search for devices, endpoints, and so on. You can enter or type the hostname strings of the devices you are looking for to search across the controllers.

You don't need to enter the complete hostname. For example, type **Core** to view all devices with **Core** in their names. Then, click on **More results...** to expand the list of devices. After that, select any device from the list to access more detailed information. Remember to press the **Return** or **Enter** key to initiate the search, because the autosearch feature is not functional. Then the matching search results appear on the left panel.

Click **Device 360**. The **Cross Launch** dialog box appears. Then click **Confirm** to go to the device 360 page for that device from the controller where the core-01 devices are located.

You can do the same thing for other search categories: Enter the name or IP address of the client to get a list of network devices or clients with that name.

Click one of the clients to go to the **Client 360** page of the client in the controller.



Note

In addition to the cross-launch feature, global search provides various functionalities, including viewing the device name, serial number, connected Catalyst Center or controller, version number, and more. This applies to applications, endpoints, and other elements as well.

Workflows

Catalyst Center Global Manager provides you with the support to trigger notifications when certain events occur. It helps you to pick your preferred method of receiving event notifications. The notification channels supported are:

- **EMAIL**- Send an email notification.
- **PAGERDUTY**- Post event notifications to Pagerduty.
- **REST**- Send data via HTTP push API.

- **SNMP**- Send data via an SNMP trap.
- **SYSLOG**- Send data to a Syslog server.
- **WEBEX**- Post event notifications to Webex.

Developer Toolkit

The **Developer Toolkit** page provides you with a new set of intent APIs to create and manage applications within the Catalyst Center Global Manager environment:

To view the developer toolkit, navigate to the Catalyst Center Global Manager dashboard and click **Platform > Developer Toolkit**.

This toolkit provides a new set of intent APIs:

- Authentication
- Event Management
- Know Your Network
- Site Management
- System

For more information on these APIs, see or download **Swagger docs** available on the **APIs GUI**.

Activities

The **Activities** page allows you to view the audit log details of Catalyst Center Global Manager.

To view the audit logs, navigate to the Catalyst Center Global Manager dashboard and click **Activities > Audit Logs**.

Audit logs in Catalyst Center Global Manager capture detailed information about various activities and events within the system performed by the logged in user, system-level changes such as user login options, controller operation initiated from the Catalyst Center Global Manager, and controller connectivity status.

It provides the following information:

- Created date and time
- Description
- Category
- Severity
- User

**Note**

- You can refine the search summary for the following periods:
 - last 2 weeks
 - last 7 days
 - last 24 hours
 - last 3 hours
 - by date
- You can also enhance the search summary by categorizing it according to different severity levels:
 - critical
 - warning
 - info

The Catalyst Center Global Manager audits the following operations:

- All user logins.
- Catalyst Center Global Manager operations such as:
 - backup and restore
 - upgrade
 - create user
 - configure AAA Server
 - enroll or unenroll controller
 - controller connectivity status change (reachable or unreachable)
- Controller operations initiated from Catalyst Center Global Manager.

System

The **System** page allows you to view these basic details of Catalyst Center Global Manager.

- **System 360**- The **System 360** view provides detailed information about the app stacks and services running on Catalyst Center Global Manager. In Catalyst Center Global Manager, the **System 360** GUI supports only monitoring under the cluster tools.

The System 360 GUI offers a view of cluster-level services under hosts and allows monitoring of services through cluster tools. It also provides system management operations such as software management and information about backups. Within backups, you can view the NFS storage configuration. Therefore, the four supported functionalities are:

- Hosts

- Cluster Tools
- Software Management
- Backups

Monitoring- Access multiple dashboards of Catalyst Center Global Manager components using Grafana, which is an open-source metric analytics and visualization suite. Use the **Monitoring** tool to review and analyze key Catalyst Center Global Manager metrics, such as memory and CPU usage.



Note In a multihost Catalyst Center Global Manager environment, expect duplication in the Grafana data due to the multiple hosts.

- **System Health-** The **System Health** view provides detailed information about the health and topology of Catalyst Center Global Manager and lets you run the validation tool for Catalyst Center Global Manager.

On the **System Health** topology view, click one of the nodes of the Catalyst Centers to view details which will list the **Controller Details** similar to the **Controller Details** on the **Controllers** page:

- Controller name
- View details
- IP address of controller
- Connectivity
- Health status
- Description
- Type of controller
- Enterprise VIP
- Cluster configuration
- Node hostname
- Node health
- Node serial number
- System Version
- Cloud Member ID
- Last collected on

On the **System Health** page, choose **Validation Tool** from the **Tools** drop-down to view the validation runs and status. The validation tool provides these information:

- Name
- Description
- Selected set(s)

- Status
- Start time
- Duration
- Actions

A validation tool is provided to you to assess the system health of Catalyst Center Global Manager, which can be run on demand. The tool is divided into two sections: 'infra' and 'upgrade,' each containing its own specific set of validations. These validations are provided to you as part of the Catalyst Center Global Manager release.

Additionally, the same validations are uploaded to the validation catalog. To update your validation set, navigate to **System > Settings > System Health** to download and import the latest set of validations.

Click **Refresh** to view the displayed health status of your network devices and components. This ensures that you are viewing the most current information regarding the health and performance of your system.

- **Software Management-** The **Software Management** view displays all the applications or system updates, and the status of the applications.

Click **View Installed Applications** or **View Release Activities** to view the update details.



Note

An update has a color badge next to it. A green badge indicates that the update or actions related to the update succeeded. A yellow badge indicates that there is an available update.

- **Backup and Restore-** The **Backup and Restore** displays the status of the most recent backup. Catalyst Center Global Manager allows both Network File System (NFS) and physical disk backup to be configured in the backup configuration. It schedules a backup with 2 options: **Now** or **Daily**.
- **Settings-** Catalyst Center Global Manager settings provides you with these details:
 - **Certificates**
 - **System Certificates-** Helps you to view information about the server's currently active SSL certificate or information about how to replace it.
 - **External Services**
 - **Destinations-** Allows you to configure these types of destinations to deliver event notifications from Catalyst Center Global Manager: webhook, email, syslog, and SNMP.
 - **Cisco Catalyst Cloud-** Allows you to register Catalyst Center Global Manager with **Cisco Catalyst Cloud** to access and download Catalyst Center Global Manager configurations.



Note

The settings page will show the Catalyst Center Global Manager configuration claimed through **First Time Setup** workflow.

De-registering will unclaim the Catalyst Center Global Manager profile and unenroll all controllers registered on the server. Following this, the Catalyst Center Global Manager will display the absence menus for controllers.

• System Configuration

- **System Health**- Allows you to update Catalyst Center Global Manager with most recent validation catalog. The validation catalog serves as a repository of validation sets, which define the specific checks or tests to be performed.

The purpose of updating the **Validation Catalog** in Catalyst Center Global Manager is to keep the set of validation checks or tests current, accurate, and relevant. This update refreshes the repository of validation criteria that the validation tool uses to perform system checks and enabling the detection of new issues.

- **Proxy**- Allows you to configure the system proxy to access the internet.
- **Debugging Logs**- Use this form to configure the logging of internal processes and errors.
- **Backup Configurations**- Allows you to configure backup mount path, encryption passphrase and data retention.
- **Authentication API Encryption**- Allows you to configure AES Encryption settings.
- **Integration Settings**- Allows you to configure platform details
- **Login Message**- This shows a message for users when they log in.

• Terms and Conditions

- **Product Offer**- This provides the general terms and conditions for Catalyst Center Global Manager. Catalyst Center Global Manager is governed solely by the [Cisco General Terms](#) (formerly "End User License Agreement").

• Trust and Privacy

- **Account Lockout**- Manages user login attempts, account lockout period, and login retries.
- **Password Expiry**- Sets the user password expiry check.
- **IP Access Control**- Configures IP addresses list for access restriction.
- **Product Telemetry**- Provides product telemetry terms for Catalyst Center Global Manager. Catalyst Center controller collects Systems Information (formerly "Product Usage Telemetry") to improve your product experience. Catalyst Center Global Manager does not collect or process Systems Information.

- **Users & Roles**- Catalyst Center Global Manager uses both users and roles to manage access. Each user is assigned roles to access controller functionality.

- **Role Based Access Control**- Role-Based Access Control (RBAC) in Catalyst Center Global Manager currently supports only the default roles: super-admin-role, observer-role, and network-admin-role. Custom role creation is not supported. Additionally, the user experience in Catalyst Center Global Manager may be impacted if there is a mismatch in permissions for the same user between Catalyst Center Global Manager and Catalyst Center. For example, if a user in Catalyst Center Global Manager does not have identical privileges in Catalyst Center due to site-based restrictions or custom roles, the Catalyst Center Global Manager may display limited data based on the user's access privileges.

Also, accessing Catalyst Center Global Manager with a custom role or a site-based user from Catalyst Center is currently not supported, which may result in a suboptimal user experience.

- The **SUPER-ADMIN-ROLE** has full control over the Catalyst Center Global Manager deployment, with all access permissions enabled.
- The **OBSERVER-ROLE** has read-only access and cannot view certain sensitive data within the system settings.
- The **NETWORK-ADMIN-ROLE** is a general-purpose role that does not have the capability to alter system configurations.

On installation of Catalyst Center Global Manager, a user with super-admin privilege is created. The user in super-admin role will have the ability to create local users on Catalyst Center Global Manager.

- **External Authentication-** Catalyst Center Global Manager supports external Authentication, Authorization and Accounting (AAA) servers for access control. If you are using an external server for authentication and authorization of external users, you should enable external authentication in Catalyst Center Global Manager. The default AAA attribute setting matches the default user profile attribute.

Catalyst Center Global Manager enables external authentication with either AAA–RADIUS/TACACS or Cisco ISE server type. The external authentication process disables local user authentication.

