Cisco Catalyst Center Global Manager Deployment Guide, Release 1.6.1

Cisco Catalyst Center
Updated November 5, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Abbreviated Cisco Trademarks

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)

Topics included

1 Catalyst Center Global Manager Overview.....7

Cisco Catalyst Center Global Manager.....8

Audience.....10

2 Deployment Requirements.....11

Required firewall ports and connectivity.....12

Additional deployment requirements.....13

3 Prepare for Deployment.....17

Prepare for deployment.....18

Install VMware.....18

Download the OVA for Catalyst Center Global Manager.....18

Reserve enterprise interface.....18

Import the IdenTrust certificate chain.....19

Prepare the DNS, NTP, and proxy servers.....20

Enable storage input/output control.....20

Check HA Admission Control Setting.....21

4 Deploy Catalyst Center Global Manager VM on VMware ESXi.....23

Deployment Modes of Catalyst Center Global Manager VM on VMware ESXi.....24

Create the Catalyst Center Global Manager VM.....24

Configure Catalyst Center Global Manager on ESXi virtual appliance.....26

Configure a virtual appliance using the maglev configuration wizard (default mode).....26

Configure a virtual appliance using the maglev configuration wizard (advanced mode).....31

Configure a virtual appliance using the web install configuration wizard.....35

Configure a virtual appliance using the advanced web install configuration wizard.....39

5 Deploy Catalyst Center Global Manager on AWS.....45

Deployment methods.....46

Deployment using AWS CloudFormation.....46

Prerequisites for deployment of Catalyst Center Global Manager using AWS CloudFormation.....47

Deploy Catalyst Center Global Manager on AWS using AWS CloudFormation.....50

Deployment using AWS Marketplace.....54

Prerequisites for deployment using AWS Marketplace.....54

Deploy Catalyst Center Global Manager on AWS using AWS Marketplace.....58

6 Deploy Catalyst Center Global Manager on Azure 59

Deployment methods....60
Deployment using an ARM template....60
Prerequisites for deployment using an ARM template....61
Configure a custom NTP server....62
Deploy Catalyst Center Global Manager using an ARM template....63
Verify the Catalyst Center Global Manager on Azure deployment....65
Deployment using Azure Marketplace....66
Prerequisites for deployment using Azure Marketplace....66
Deploy Catalyst Center Global Manager using Azure Marketplace....67
Verify the Catalyst Center Global Manager deployment....75

7 Deploy Catalyst Center Global Manager on Ubuntu KVM....77
Catalyst Center Global Manager on Ubuntu KVM....78
Deployment methods....78
Deployment requirements....78
Deployment prerequisites....79
Deploy Catalyst Center Global Manager on Ubuntu KVM....81
Prepare for the Catalyst Center Global Manager virtual machine....82
Deploy the Catalyst Center Global Manager virtual machine using Ubuntu Desktop....82
Configure additional NICs....84
Deploy the Catalyst Center Global Manager virtual machine using Ubuntu Server....85
Configure a Catalyst Center Global Manager virtual appliance....87
Verify the Catalyst Center Global Manager deployment....87

8 Get Started....89
Log in to Catalyst Center Global Manager and run it....90
Enable an air-gapped deployment on Catalyst Center Global Manager....91
Enroll Catalyst Centers to Catalyst Center Global Manager....92
Enroll Catalyst Centers to Catalyst Center Global Manager in air gap mode....95
Site Hierarchy....99
Rename a site....100
Monitor from the overview dashboard....102
Monitor controller health....103
Monitor network status changes....104
Monitor health of devices....104
Alerts....105
Device infrastructure....106
Device health....106
Software-Defined Access health....108
End-of-Life Devices....108
Endpoints....109
Situational dashboard....110
Create a dashboard....111
Controllers....113

Cross-launch to controllers....115
Controller backups....116
Controller upgrades....118
View controller upgrade status....120
Upgrade a Controller....124
Pre-upgrade checks....126
Cancel or delete a downloaded release....126
Edit or delete an upgrade schedule....126
Monitor download or upgrade progress....127
Handle upgrade failures....127
Controller certificates....127
Certificate categories....128
Certificate statuses....128
Monitor system certificates....129
Monitor trusted certificates....130
Global search....131
Workflows....132
Platform....132
Overview....133
Manage....133
Developer toolkit....134
Activities....134
System....135
Use System 360....135
Software Management....138
About backup and restore....139
System settings....151
Users and roles....153

1 Catalyst Center Global Manager Overview

Topics:

- Cisco Catalyst Center Global Manager
- Audience

Cisco Catalyst Center Global Manager

Defines the platform as a single pane of glass for managing multiple Catalyst Centers, integrating information, and providing an overview of network status changes, alerts, and visibility into sites.

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.

For example, you may have multiple Catalyst Centers deployed across your enterprise, each dedicated to a specific region. Rather than logging into each Catalyst Center individually, you can link the Catalyst Centers to a single Catalyst Center Global Manager, allowing you to monitor all operations from one centralized location.

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. You can 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 20 active users. Once these controllers are registered with Catalyst Center Global Manager, they will continue to monitor and control networks.

Note

The minimum supported versions of the Catalyst Center are:

- 2.3.7.9
- 2.3.7.10
- 2.3.7.11
- 3.1.3
- 3.1.5
- 3.1.6
- 3.2.1
- 3.2.3
- 3.3.1
- 3.3.2

Single-node and 3-node clusters, supported Catalyst physical appliance, virtual appliances (VA) on VMware ESXi, Amazon Web Services (AWS), Azure, and Ubuntu KVM can be integrated in to Catalyst Center Global Manager.

Catalyst Center Global Manager has a global search feature that lets you search for devices or clients by many attributes such as IP address, hostname, MAC address, software version, client user name, application name, or site name. You

can cross-launch into the 360 view of the client or device in Catalyst Center. You can also cross launch into the Catalyst Center interfaces without entering your username and password again, if the same user exists in both the systems. Your passwords can be different.

Key features of Catalyst Center Global Manager are:

- **Scale and Enterprise Readiness**: Ensures the system is capable of handling large-scale operations and meets the robust operational requirements of enterprise environments.
- **System Health and Monitoring**: Provides tools and capabilities to continuously observe and assess the operational status and performance of Catalyst Center Global Manager and the underlying Catalyst Center control plane.
- **SSO Cross-Controller Navigation**: Enables you to seamlessly navigate between different controllers and Catalyst Center Global Manager with a single sign-on authentication.
- **Global Search**: Allows you to quickly find information or resources across the entire system from a centralized search bar.
- **Dashboard Customization**: Lets you personalize dashboard views and display relevant information and metrics based on your preferences.
- **UI Error Handling Improvements**: Enhances the user interface to better manage and communicate errors, improving the overall user experience.
- **Role-Based Access Control (RBAC)**: Implements security measures that restrict system access based on each user's organizational role.
- **Day 0 Setup Improvements**: Streamlines and improves the initial configuration and deployment process for new installations.
- **Control Plane and System Visualization**: Displays a graphical representation of the system's control plane, providing insights into its architecture and operational status.
- **Site Hierarchy Unification**: Integrates and standardizes the organizational structure of different sites, creating a unified and consistent view.
- **Network Summary**: Presents an overview of the network status, performance, and key metrics.
- **Endpoint Visibility**: Offers comprehensive insight into all connected endpoints for improved monitoring and management.
- **EoL Visibility**: Shows clear information about the End-of-Life (EoL) and End-of-Sale (EoS) status of hardware and software components.
- **SDA Visibility**: Provides monitoring and insights for Software-Defined Access (SDA) deployments.
- **Inventory**: Lists all assets and resources managed on the network.
- **Device Infrastructure Health Devices Export** : Lets you export all matching results based on the filter selected. Data table export is only available for device **Health** under **Device Infrastructure**.
- **Drill-Down for Sites, Clients, Devices, and Issues**: Enables you to navigate from a high-level overview to detailed information about specific sites, clients, devices, or issues.
- **Improved Cross-Launch**: Enhances the functionality and user experience of launching cross-system applications and tools.
- **Controller backup**: Offers a centralized and aggregate view of your environment. It allows you to monitor backup status, schedule single or bulk backups for the selected controllers, configure backup settings, and troubleshoot backup failures through cross-launch to the controller.
- **Situational Dashboard**: Offers dashboard-building tools to design to customized, real-time, context-specific views into operational telemetry.

- **Complete UI/API parity**: Ensures that all functionalities available through the user interface are also accessible and controllable via the Application Programming Interface (API), providing consistent capabilities across both interfaces.

Audience

Explains the intended audience for Catalyst Center Global Manager, outlining which users and roles will benefit from its features and providing guidance on who should use this deployment guide.

This guide is designed for:

- System administrators: to deploy the Catalyst Center Global Manager virtual appliance, connecting controllers, and provisioning access for other users to allow additional configurations.
- Network administrators: to monitor aggregated network details and controller health via a Single Pane of Glass (SPOG).
- Users or operators: to manage or operate enterprise-scale network infrastructure.

2 Deployment Requirements

Topics:

- Required firewall ports and connectivity
- Additional deployment requirements

Required firewall ports and connectivity

Details the necessary firewall access rules, specific TCP/UDP ports to open for various services (UI, shell, TACACS+, DNS, NTP, HTTPS, RADIUS, NFS), and connectivity requirements between Catalyst Center Global Manager and controllers.

- **Firewall Access**: Allow outbound access to ciscoconnectdna.com.
- **Connectivity**: Ensure connectivity exists between the Catalyst Center Global Manager and the controllers. Catalyst Center Global Manager supports only one interface for the enterprise edition.

> **Note**
>
> In air gap mode, Catalyst Center Global Manager does not require direct outbound internet access to Cisco cloud services. However, it must have internal connectivity to Catalyst Center controllers, DNS, NTP, and optional authentication or backup servers for deployment and operation.

Allow the following internal connectivity:

Table 1: Internal connectivity requirements

Connection	Purpose
Administrator workstation to Catalyst Center Global Manager	Access the GUI, REST APIs, and installation or setup workflows over HTTPS.
Catalyst Center Global Manager to Catalyst Center controllers	Enroll, monitor, and manage supported controllers.
Catalyst Center Global Manager to DNS	Resolve internal hostnames and FQDNs.
Catalyst Center Global Manager to NTP	Synchronize time.
Catalyst Center Global Manager to authentication servers	Support external authentication, if configured.
Catalyst Center Global Manager to external backup servers	Transfer and store backup files on an NFS or SSH remote server configured as the backup destination.

When you enable airgap mode, provide the allowed IP ranges that can communicate with Catalyst Center Global Manager. Include the subnets used by managed Catalyst Center controllers and other required internal services.

- **Supported Infrastructure**: includes:
  - 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
  - KVM on Ubuntu 22.04 LTS or Ubuntu 24.04 LTS for hosting the Catalyst Center Global Manager virtual machine. Deployment uses a Cisco-provided KVM TAR package containing QCOW2 disk images.
  - Network Time Protocol (NTP) needs to be synchronized between the Catalyst Center Global Manager and Catalyst Centers. Alternatively, ensure they maintain a maximum time difference of one second.
- **Ports required to be open on the firewall**: Open these ports on the firewall to enable communication with the HTTPS-enabled browsers 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.	Open the port.
TCP 2222	Catalyst Center Global Manager shell	Connect to the Catalyst Center Global Manager shell.	Keep the port open. Restrict the known IP address to be the source.
TCP 9004	Web UI installation	Serves the GUI-based installation page. (This port is required only if you decide to install Catalyst Center Global Manager using the web-based option.)	Keep the port open until the node installation is complete.
Catalyst Center Global Manager outbound to Catalyst Center and other systems.			
TCP 49	TACACS+	Needed only if you are using external authentication such as Cisco ISE with a TACACS+ server.	Open the port 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.	Open the port when you use DNS names 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.	Open the port for time synchronization.
TCP 443	HTTPS	Catalyst Center Global Manager uses HTTPS for cloud-tethered upgrades, periodic polling from Catalyst Center and communication with HTTPS-enabled browsers.	Open the port.
UDP 1645 or 1812	RADIUS	Needed only if you are using external authentication with a RADIUS server.	Open the port only if an external RADIUS server is used to authenticate user login to Catalyst Center.
TCP and UDP 111, 2049, 20048, and 32767	NFS	Used for backups.	Open the port.

Additional deployment requirements

Describes the requirements that need to be met to deploy a Catalyst Center Global Manager virtual appliance.

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

You must meet these requirements listed here to deploy a Catalyst Center Global Manager virtual appliance. For performance tips on the most critical areas of VMware vSphere, refer to:

- 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

Requirement	Detail
Virtualization platform and hypervisor	VMware vSphere (which includes ESXi and vCenter Server) 7.0.x or later, including all updates.
Processors	Intel Xeon Scalable server processor (Cascade Lake or newer) or AMD EPYC Gen2 with 2.1 GHz or better clock speed. Dedicate 8 vCPUs with a 16 GHz reservation 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 (less than or equal to 350 ms).
Active Sessions	The system supports up to 20 active user connections when network administrators log in to Catalyst Center Global Manager.

Server requirements

Requirement	Detail
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

Ensure that the client systems used to log in to Catalyst Center Global Manager have 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 **Note** 3-node controllers are treated as a single controller within the 25-controller scale limit
Users	20 active users
Sites	25,000 (maximum aggregated sites) • 100 (sites on multiple controllers) • 5 (same site on maximum number of controllers)

Note

For more information on the Catalyst Center scale limit, refer to the Cisco Catalyst Center Data Sheet.

Security limitations

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

- Federal Information Processing Standards (FIPS)
- Dual stack setups

Note

Catalyst Center Global Manager supports controllers operating in air gap mode starting with release 1.5.1. The enrolled Catalyst Center controller version must be release 3.3.1 and later.

User access role requirements

- You have matching user accounts on both Catalyst Center Global Manager and Catalyst Center.
- You get the access permissions come from individual Catalyst Centers.

Air gap support requirements
Table 2: Air gap support requirements

Requirement	Detail
Catalyst Center Global Manager release	Release 1.6.1.
Supported Catalyst Center controllers	Catalyst Center 3.3.1 and later.
Supported deployment files	OVA, ISO, appliance ISO, and KVM-based VM.
Initial deployment mode	The virtual appliance is first installed in non-airgap mode, and air gap mode is then enabled with the help of Cisco Technical Assistance Center (TAC). You must deploy downloaded non-airgapped OVA or Qcow2 image. Once deployment is complete, contact TAC to enable air gap mode.
Controller management	Air gap mode supports enrolling supported Catalyst Center controllers into Catalyst Center Global Manager by using offline enrollment file.

3 Prepare for Deployment

Topics:

- Prepare for deployment
- Install VMware
- Download the OVA for Catalyst Center Global Manager
- Reserve enterprise interface
- Import the IdenTrust certificate chain
- Prepare the DNS, NTP, and proxy servers
- Enable storage input/output control
- Check HA Admission Control Setting

Prepare for deployment

States that Catalyst Center Global Manager is deployed as a VM on VMware ESXi 7.x or later and outlines the initial tasks required for its 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 these tasks.

Install VMware

Instructs to install VMware vSphere 7.0.x or later and confirm accessibility from the deployment computer.

VMware vSphere 7.0.x or later (which includes ESXi and vCenter Server), including all patches, is required to run Cisco Catalyst Center Global Manager on ESXi. Access an overview of the VMware vSphere installation and setup process using this link. After installing VMware vSphere, confirm that you can access it from the computer used to deploy the Open Virtual Appliance (OVA) file for the virtual appliance.

Use a web browser to access the vCenter 7.0.x to deploy the OVA for Catalyst Center Global Manager virtual appliance.

Download the OVA for Catalyst Center Global Manager

Directs users to download the Catalyst Center Global Manager .ova file from Cisco-provided links, noting its size and download time.

Save the OVA files to the computer on which you will deploy Catalyst Center Global Manager. Download the .ova file from the Cisco-provided link to use it for deploying the Catalyst Center Global Manager. You can also host the OVA on a web server.

> **Note**
>
> The size of the .ova file is approximately 23 GB, and the download time depends on network bandwidth.

Reserve enterprise interface

Advises reserving one 10-Gbps enterprise interface for GUI access, recording its IP address, and mentions the secondary intracluster interface with a predefined IP.

Reserve one 10-Gbps enterprise interface to access the Catalyst Center Global Manager GUI before you configure the virtual appliance. Record the IP address for this interface, because you will need to enter it during appliance configuration.

Note

During the installation process, you must also configure a secondary interface called the intracluster interface, assigning it a non-routable IP address. The standard installer uses a predefined IP address for this interface that cannot be changed. If you need to change this IP address due to network overlap, use the Advanced installer.

Cisco predefines the IP address for the intracluster interface. The Maglev Configuration wizard automatically populates this information during the configuration process.

Import the IdenTrust certificate chain

Provides steps to import the IdenTrust CA certificate chain into VMware vSphere to prevent invalid certificate messages during OVA deployment.

The Catalyst Center Global Manager OVA file is signed with an IdenTrust CA certificate. This certificate is not included in the default VMware truststore. As a result, the **Deploy OVF Template** wizard's **Review details** page displays an invalid certificate message after you complete the wizard. To prevent this, import the IdenTrust certificate chain to the host or cluster where you plan to deploy the OVA file.

Before you begin

- You must have a VMware ESXi host or cluster where the Catalyst Center Global Manager virtual appliance will be deployed.
- Confirm you have administrator access to the target vSphere host or cluster.
- Locate the download site for both the OVA file and the related IdenTrust CA certificate (**trustidevcodesigning5.pem**).

Procedure

1. On the VMware Catalyst Center Global Manager host or cluster where your virtual appliance will reside, download and extract **trustidevcodesigning5.pem** from the same location specified for downloading the Catalyst Center Global Manager OVA file.
2. Unzip this file if it is compressed.
3. Log in to the vSphere Web Client managing the host or cluster.
4. Choose **Administration** > **Certificates** > **Certificate Management**.
5. In the **Trusted Root Certificates** field, click **Add**.
6. In the **Add Trusted Root** dialog box, click **Browse**.
7. Navigate to the location of the certificate chain you downloaded in Step 1 (**trustidevcodesigning5.pem**). Select the file, then click **Open**.
8. Check the **Start Root certificate push to vCenter Hosts** check box, then click **Add**.

You see a message confirming that the certificate chain was imported successfully.

After you complete the **Deploy OVF Template** wizard, the **Review details** page shows that you are using a trusted certificate in the **Publisher** field.

Prepare the DNS, NTP, and proxy servers

Details the need to configure DNS and NTP servers for domain name resolution and clock synchronization, and to obtain proxy server details if applicable.

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

- The Domain Name System (DNS) server is used by Catalyst Center Global Manager to convert domain names to IP addresses.
- The Network Time Protocol (NTP) server is used by Catalyst Center Global Manager for clock synchronization. Ensure that the NTP server is accessible to the Catalyst Centers, or confirm they maintain synchronization with a time deviation of less than 1 second.

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

- Make sure 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 its URL, IP address, or hostname, as well as its login credentials.

Enable storage input/output control

Explains how to enable Storage I/O Control in vSphere to prioritize the virtual appliance's I/O during datastore congestion.

Complete the procedure for the datastore where you plan to deploy the appliance to prioritize the virtual appliance’s input/output (I/O) over other virtual machines during network I/O congestion.

Enable Storage I/O Control in vSphere so the deployed virtual appliance receives preferred I/O resources during datastore congestion.

Before you begin

- Make sure you have administrator access to the vSphere Client.
- Identify the target datastore for your virtual appliance deployment.

Procedure

1. In the vSphere Client, navigate to and click the datastore in which you plan to deploy a virtual appliance.
2. Click the **Configure** tab, and then click **General**.
3. In the **Datastore Capabilities** area, click **Edit**.
4. In the **Configure Storage I/O Control** window, complete these steps:
   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.
5. Click **OK**.

Storage I/O Control is enabled. The VM for the virtual appliance now receives prioritized I/O during datastore congestion.

Check HA Admission Control Setting

To ensure high availability for Catalyst Center Global Manager on ESXi, use VMware vSphere high availability (HA) with strict admission control instead of creating 3-node clusters.

You cannot create three-node clusters by connecting Catalyst Center Global Manager on ESXi. To enable high availability (HA), use the HA functionality in VMware vSphere. Enable strict admission control to ensure that:

- The system does not power on a virtual machine if that action would violate availability constraints.
- The system enforces configured failover capacity limits.
- HA operates as expected during a failover.

4 Deploy Catalyst Center Global Manager VM on VMware ESXi

Topics:

- Deployment Modes of Catalyst Center Global Manager VM on VMware ESXi
- Create the Catalyst Center Global Manager VM
- Configure Catalyst Center Global Manager on ESXi virtual appliance

Deployment Modes of Catalyst Center Global Manager VM on VMware ESXi

Provides step-by-step instructions for deploying the OVF-formatted file using the VMware vSphere Web Client, including selecting storage, networks, and reviewing settings.

This section describes the deployment modes and the steps to deploy Catalyst Center Global Manager VM on ESXi 7.0 or later.

Catalyst Center Global Manager can be deployed using one of these methods:

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

Catalyst Center Global Manager deployment provides these capabilities:

- Deploy Catalyst Center Global Manager on a VM (VMware ESXi/vCenter).
- Install Catalyst Center Global Manager using CLI or web install.

Create the Catalyst Center Global Manager VM

Provides step-by-step instructions for creating a virtual machine to deploy Catalyst Center Global Manager.

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

Follow these steps to deploy your virtual machine on the VMware ESXi host or cluster where your virtual appliance will reside.

Procedure

1. Download the Catalyst Center Global Manager OVA file from the location specified by Cisco.
2. Log in to the VMware vSphere Web Client using the applicable credentials.

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

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.

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 filename field shows the OVA file name you are about to create. The path shows the location within the Navigator directory where the ESXi host or cluster is listed. This location corresponds to the deployment location you chose 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 VMware vSphere Web Client directory, complete these steps:

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 you selected for OVA deployment—this is the same one you right-clicked in Step 3. Then click **Next**.

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

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

- To make changes, click **Back** to return to the appropriate wizard page.
- To proceed, click **Next**.

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

e) On the **Select storage** page, complete these steps:

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, complete these steps:

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

> **Note**
>
> This interface or IP address is used for UI or 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 these steps:

- 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

  - Deployment typically takes about 45 minutes to complete. Monitor the deployment progress in the vSphere Client's **Recent Tasks** tab.
  - Available bandwidth, vCPUs, RAM, and hard disk space can affect the time that this process takes.
  - After the deployment tasks are completed, power on your virtual machine and configure it.

What to do next

After creating a virtual machine, configure the virtual appliance.

Configure Catalyst Center Global Manager on ESXi virtual appliance

Outlines the initial configuration workflow for the virtual appliance after deployment, preparing it for use.

Before using Catalyst Center Global Manager, complete the appliance configuration workflow that meets your requirements. Complete one of the procedures below to configure Catalyst Center Global Manager on an ESXi virtual appliance on a VMware ESXi host.

Configure a virtual appliance using the maglev configuration wizard (default mode)

Details the process of quickly configuring a virtual appliance with preset settings using the maglev configuration wizard, including network, DNS, NTP, and user account settings.

To quickly configure a virtual appliance with preset appliance settings, use the maglev configuration wizard by completing this procedure.

> **Note**
>
> The intracluster interface is preconfigured when using this wizard.

Configure the virtual appliance using these steps:

Before you begin

Before you start, gather this information for the virtual appliance:

- Static IP address

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

Procedure

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**.

   The virtual machine becomes operational in about 45 minutes after you power it on. The actual time depends on available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor progress in the VMware VM Console.
2. Launch either the remote console or web console by clicking the appropriate link.
3. Configure the virtual machine by completing the maglev configuration wizard:
   a) You do not need to enter any settings on the **STATIC IP CONFIGURATION** page. Click **skip>>** to continue 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 pre-manufactured cluster option enables faster installation but prevents customization of the cluster port.
   d) Select the manufacture cluster option. The wizard displays a series of questions about maglev configuration.
      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**, and click **next>>** to validate the host networking. See the table for required network settings.

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 you enter a default gateway, do not configure static routes.

      The wizard validates the settings after the DNS step. If you receive an error message, check your entry and correct it. Click **<<back** to reenter if needed. The validation process takes 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 you selected **pre manufactured**, these values are prepopulated and cannot be changed. If you selected advance install, 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 these steps:

- If you need to change any settings, select **<<back** as needed, make the necessary changes, and then return to this wizard page.
- If you are satisfied with the settings you 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 these steps:

- If your network does *not* use a proxy server to access the Internet, select **skip proxy>>** to proceed.
- If your network uses a proxy server, enter the configuration values in the **NETWORK PROXY** wizard page by referring to this 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) 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 perform these functions:

- Catalyst Center Global Manager accesses your virtual appliance’s web interface and the Representational State Transfer (REST) APIs used by devices in the enterprise network it manages with this hostname.

Select **next>>** to proceed after you provide the necessary information. Correct any validation errors as you did in earlier screens.

k) Enter the configuration values for the settings provided in the wizard's **USER ACCOUNT SETTINGS** page by referring to this table, then select **next>>**.

Linux Password field	Enter and confirm the password for the `maglev` 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.

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 by referring to this 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 must use a common NTP server or be synchronized within a maximum time difference of one second. **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 these 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 stabilize, after which you can log in to the virtual appliance GUI.

Configure a virtual appliance using the maglev configuration wizard (advanced mode)

Explains how to configure a virtual appliance using the maglev wizard with advanced settings, allowing customization beyond presets for network, DNS, NTP, proxy, user accounts, and container/cluster subnets.

To configure a virtual appliance using the maglev configuration wizard and to specify settings that are different from the preset appliance settings, follow this procedure.

Before you begin

Before you start, gather this information for the virtual appliance:

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

Procedure

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**.

   The virtual machine becomes operational in about 45 minutes after you power it on. The actual time depends on available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.
2. Click the link to open the remote console or web console.
3. Configure the virtual machine by completing the maglev configuration wizard:
   a) You do not need to enter any settings in the **STATIC IP CONFIGURATION** page in the wizard, 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.

      If you choose this option, you cannot return to the default appliance setup workflow. Review this limitation 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 this 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 this format, separated by spaces: *<network>/<netmask>/<gateway>*.
Cluster Link field	Leave this field blank. It is required on the Intracluster interface only.
LACP Mode field	Leave this field blank, it does not apply 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, verify the entered value and correct it. If needed, select **<<back** to make another change.

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 these steps:

- If you need to change any settings, select **<<back** as needed, make the necessary changes, and then return to this wizard page.
- If you are satisfied with the settings you 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 described in this table.

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 these steps:

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

k) (Optional) The wizard prompts you to enter the virtual IP address for the appliance 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 this step:

- 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 any validation errors if they occur.

l) Enter the configuration values for the settings provided in the **USER ACCOUNT SETTINGS** page in the wizard as described in this table. Then select **next>>**.

Linux Password field	Enter and confirm the password for the `maglev` 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. You can use this password as is or further edit this automatically 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 **NTP SERVER SETTINGS** page in the wizard as described in this 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 these 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 **MAGLEV ADVANCED SETTINGS** page in the wizard, as described in this 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

Guides users through configuring a virtual appliance via a browser-based wizard with preset settings, covering IP, DNS, proxy, NTP, and CLI password configurations.

To quickly configure a virtual appliance using preset appliance settings, use the browser-based install configuration wizard.

Important

Enter valid IPv4 addresses with matching netmasks during this procedure. Make sure addresses and their subnets do not overlap. If subnets or addresses overlap, service communication issues can occur.

Before you begin

Collect these information before you begin:

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

Use a supported browser. For more information on supported browsers, see the Additional deployment requirements section.

Enable ICMP on the firewall between Catalyst Center Global Manager and the DNS servers you plan to specify. 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. If ICMP is not enabled, you cannot complete the wizard.

Procedure

1. After deployment completes, power on the new virtual machine:
   a) In the vSphere Web Client, right-click the virtual machine.
   b) Choose **Power** > **Power On**.

   It takes around 45 minutes for the virtual machine to become operational. The actual time depends on available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the **Recent Tasks** tab in vSphere Client.
2. Launch either the remote console or web console by clicking the appropriate link.
3. Start the install configuration wizard:
   a) In the **STATIC IP CONFIGURATION** page, do one of these steps:
      - 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 this table and then select **configure>>**.

   For IPv4 deployments, this check box must be cleared.

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	Leave this field blank; you cannot specify static routes in this wizard.

   Note the URL listed in the **Web Installation** field. Save this information for the next step.

   b) Open the URL that was displayed in the **Static IP Configuration** page.
   c) 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.
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. If you configure more than three DNS servers for an appliance, you may encounter problems.

c) Click **Next**.

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

d) Do one of these steps:

- 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 uses a proxy server to access the internet, enter the values described in this 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 **Advanced Appliance Settings** page opens in the wizard.

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, we recommend that you configure at least 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 these information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value is the key ID 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, nonrouted 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, nonrouted 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.

Use this username and password to access the CLI for troubleshooting. After you log in, the system prompts you to configure a new admin user for security.

The wizard validates the information that you entered and notifies you if you need to change any settings before you can proceed. 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. To update settings, click the corresponding **Edit** link.

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. Click the **Download** link to save a local copy of this information as a text file.

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 set up 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

Provides instructions for configuring a virtual appliance using the browser-based advanced web install wizard, allowing detailed customization of network interfaces, DNS, proxy, NTP, and subnet settings.

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 these steps.

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. If the addresses and subnets overlap, service communication issues may occur.

Procedure

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**.

The virtual machine typically becomes operational in 90 to 120 minutes, depending on available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.

2. Launch either the remote console or web console by clicking the appropriate link.
3. Open the advanced install configuration wizard:
   a) In the **STATIC IP CONFIGURATION** page, do one of these steps:
      - 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 table and then select **configure>>**.

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

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	Do not specify static routes with this wizard; leave the field blank.

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

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

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

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

4. Configure your virtual appliance by completing the advanced install configuration wizard:
   a) Click **Next**.

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

   If your network resides behind a firewall, perform these actions:

   - 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.

b) Complete these steps 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. If you configure more than three DNS servers for an appliance, you may encounter problems.
- 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 these steps 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 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 uses 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 these 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 the settings that you 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.

The virtual machine typically becomes operational in 180 to 210 minutes, depending on available bandwidth, RAM, hard disk space, and the number of vCPUs. You can monitor the progress in the vSphere Client's **Recent Tasks** tab.

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 cannot log in to Catalyst Center Global Manager for the first time.

5 Deploy Catalyst Center Global Manager on AWS

Topics:

- Deployment methods
- Deployment using AWS CloudFormation
- Deployment using AWS Marketplace

Deployment methods

Describes and compares the available deployment methods for Catalyst Center Global Manager on AWS.

You can manually deploy Catalyst Center Global Manager on AWS using either AWS CloudFormation or AWS Marketplace.

Manual deployment using AWS CloudFormation

You manually deploy the Catalyst Center Global Manager on AWS using the AWS CloudFormation deployment tool. Then you manually configure Catalyst Center Global Manager by creating the AWS infrastructure, establishing a VPN tunnel, and deploying your Catalyst Center Global Manager VA.

Manual deployment using AWS Marketplace

You manually deploy the Catalyst Center Global Manager on AWS using AWS Marketplace , an online software store. You launch the software through the Amazon EC2 console. Then you manually deploy Catalyst Center Global Manager by creating the AWS infrastructure, establishing a VPN tunnel, and configuring your Catalyst Center Global Manager VA. Only Launch through EC2 is supported for this method. The other two launch options–Launch from Website and Copy to Service Catalog–are not supported.

Choose a deployment method

Consider the benefits and drawbacks of each manual deployment method using this table.

Table 3: Comparison Table

Manual deployment using AWS CloudFormation	Manual deployment using AWS Marketplace
The AWS CloudFormation file is required to create Catalyst Center Global Manager on AWS.	The AWS CloudFormation file is not required to create Catalyst Center Global Manager on AWS.
You create the AWS infrastructure, such as VPCs, subnets, and security groups, in your AWS account.	
You establish a VPN tunnel.	
You deploy Catalyst Center Global Manager.	
Deployment time may take from a couple of hours to a couple of days.	
You need to manually configure monitoring through the AWS console.	
You can only configure an on-premises NFS for backups.	

Deployment using AWS CloudFormation

Describes how to deploy Catalyst Center Global Manager on AWS using AWS CloudFormation.

This chapter explains how to deploy Catalyst Center Global Manager on AWS using AWS CloudFormation. It covers the required prerequisites, step-by-step deployment instructions, and procedures for the TAR file verification and Catalyst Center Global Manager VA deployment validation.

Prerequisites for deployment of Catalyst Center Global Manager using AWS CloudFormation

Lists the network, AWS infrastructure, and Catalyst Center Global Manager instance requirements–including VPC, security group, and region settings–needed to prepare for a Catalyst Center Global Manager on AWS deployment using AWS CloudFormation.

Before deploying Catalyst Center Global Manager on AWS, ensure you meet these network, AWS, and requirements.

Network environment requirements

You have this information about your network environment on hand:

- Enterprise DNS server IP address
- (Optional) HTTPS network proxy details

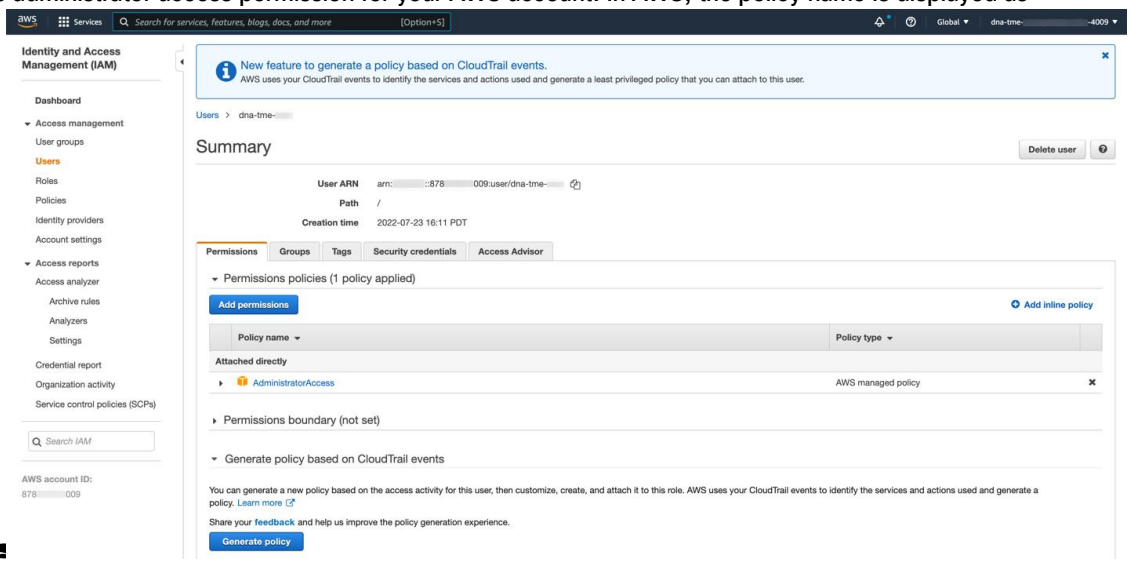
AWS account requirements

You must meet these AWS account requirements:

- You have valid credentials to access your AWS account.

> **Tip**
>
> We recommend that your AWS account be a subaccount (a child account) to maintain resource independence and isolation. A subaccount ensures that the Catalyst Center Global Manager deployment does not impact your existing resources.

- **Important**: Your AWS account is subscribed to Cisco Catalyst Center Global Manager Virtual Appliance - BYOL in AWS Marketplace.
- You have administrator access permission for your AWS account. In AWS, the policy name is displayed as



AWS network infrastructure requirements

You must set up these resources and services in AWS:

- **VPC**: The recommended CIDR range is /25. In IPv4 CIDR notation, the last octet (the fourth octet) of the IP address can only be 0 or 128. For example, x.x.x.0 or x.x.x.128 are valid options.
- **Subnets**: The recommended subnet range is /28, and it should not overlap with your corporate subnet.
- **Route tables**: Make sure that your VPC subnet is allowed to communicate with your enterprise network through your VPN Gateway (VPN GW) or Transit Gateway (TGW).
- **Security groups**: To ensure communication between Catalyst Center Global Manager on AWS and the Catalyst Center in your enterprise network, the AWS security group attached to Catalyst Center Global Manager on AWS must allow the TCP port 443.
  - TCP ports: 443

  For more information about the ports that Catalyst Center Global Manager uses, see Required firewall ports and connectivity.
- **VPN GW or TGW**: You must have an existing connection to your enterprise network, which is your Customer Gateway (CGW).

  For your existing connection from the CGW to AWS, ensure that the correct ports are open for traffic flow to and from your Catalyst Center Global Manager VA. You can open them using either the firewall settings or a proxy gateway. For information about the well-known network service ports that the appliance uses, see Required firewall ports and connectivity.
- **Site-to-Site VPN connection**: You can use TGW attachments and TGW route tables.

AWS region configuration requirements

You must meet these AWS region configuration requirements:

- Your AWS environment must be configured with one of these regions:
  - af-south-1 (Cape Town)
  - ap-east-1 (Hong Kong)
  - ap-northeast-1 (Tokyo)
  - ap-northeast-2 (Seoul)
  - ap-northeast-3 (Osaka)
  - ap-south-1 (Mumbai)
  - ap-south-2 (Hyderabad)
  - ap-southeast-1 (Singapore)
  - ap-southeast-2 (Sydney)
  - ap-southeast-3 (Jakarta)
  - ap-southeast-4 (Melbourne)
  - ca-central-1 (Canada Central)
  - ca-west-1 (Calgary)
  - eu-central-1 (Frankfurt)
  - eu-central-2 (Zurich)
  - eu-north-1 (Stockholm)
  - eu-south-1 (Milan)

- eu-south-2 (Spain)
- eu-west-1 (Ireland)
- eu-west-2 (London)
- eu-west-3 (Paris)
- il-central-1 (Tel Aviv)
- sa-east-1 (São Paulo)
- us-east-1 (Northern Virginia)
- us-east-2 (Ohio)
- us-gov-east-1 (AWS GovCloud US-East)
- us-gov-west-1 (AWS GovCloud US-West)
- us-west-1 (Northern California)
- us-west-2 (Oregon)

IAM user group requirement (optional)

If you want to enable multiple IAM users with the ability to configure Catalyst Center Global Manager using the same environment setup, you need to create a group with these policies and then add the required users to that group:

- IAMReadOnlyAccess
- AmazonEC2FullAccess
- AWSCloudFormationFullAccess

Catalyst Center Global Manager instance requirements

The Catalyst Center Global Manager instance size must meet these minimum resource requirements:

- c5.2xlarge

> **Note**
>
> Catalyst Center Global Manager supports only the c5.2xlarge instance size. Any changes to this configuration aren't supported.

- 8 virtual CPUs (vCPUs)
- 16-GB RAM
- 650-GB storage, provisioned as two separate EBS-gp3 disks:
  - 100-GiB disk
  - 550-GiB disk
- 2500 disk input and output operations per second (IOPS)
- 180-MBps disk bandwidth

Catalyst Center Global Manager backup instance requirements

The Catalyst Center Global Manager backup instance must meet these minimum resource requirements based on if you use a cloud server or an enterprise (on-premises) server:

- **Cloud backup**: t3.micro, 2 vCPUs, 1-GB RAM, and for storage, see Backup storage requirements.
- **Enterprise backup**: See Backup server requirements and Backup storage requirements.

AWS information requirements

You have this AWS information on hand:

- Subnet ID
- Security group ID
- Keypair ID
- Environment name
- CIDR reservation

Catalyst Center Global Manager environment requirements

You must meet these requirements for your Catalyst Center Global Manager environment:

- You have access to the Catalyst Center Global Manager GUI.
- You have this Catalyst Center Global Manager information on hand:
  - Default gateway setting
  - CLI password
  - FQDN for the Catalyst Center Global Manager VA IP address

Deploy Catalyst Center Global Manager on AWS using AWS CloudFormation

Provides step-by-step instructions for creating the stack and configuring the parameters to deploy Catalyst Center Global Manager on AWS.

Follow these steps to deploy Catalyst Center Global Manager on AWS using AWS CloudFormation. The provided AWS CloudFormation template contains the relevant details for all required parameters.

Before you begin

Ensure that

- the VPN tunnel is up, and
- the AWS environment is set up with all the required components.

  For information, see Prerequisites for deployment using AWS CloudFormation.

Procedure

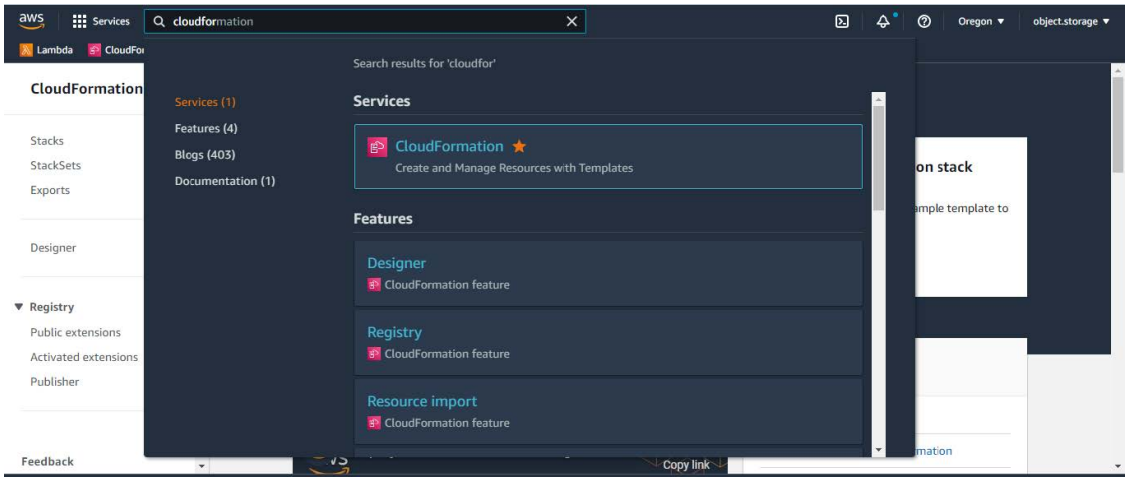
1. Verify that the TAR file is genuine and from Cisco Systems, Inc.

   For detailed steps, see Verify the Catalyst Center Global Manager VA TAR file.

2. Log in to the AWS console.

   The AWS console is displayed.

3. In the search bar, enter `cloudformation`.



4. From the drop-down menu, choose **CloudFormation**.
5. Click **Create stack** and choose **With new resources (standard)**.
6. Under **Specify template**, select **Upload a template file**, and choose the AWS CloudFormation template that you downloaded in Step 1.
7. Enter a stack name and review these parameters:
   - **EC2 Instance Configuration**
     - **Environment Name**: Assign a unique environment name.

       The environment name is used to differentiate the deployment and is prepended to your AWS resource names. If you use the same environment name as a previous deployment, the current deployment will fail.
     - **Private Subnet ID**: Enter the VPC subnet to be used for Catalyst Center Global Manager.
     - **Security Group**: Enter the security group to be attached to the Catalyst Center Global Manager VA that you are deploying.
     - **Keypair**: Enter the SSH keypair used to access the CLI of Catalyst Center Global Manager VA that you are deploying.
   - **Catalyst Center Global Manager Configuration**: Enter this information:
     - **CatalystCenterGlobal ManagerInstanceIP**: Catalyst Center Global ManagerIP address.
     - **CatalystCenterGlobal ManagerNetmask**: Catalyst Center Global Manager netmask.
     - **CatalystCenterGlobal ManagerGateway**: Catalyst Center Global Manager gateway address.
     - **CatalystCenterGlobal ManagerDnsServer**: Enterprise DNS Server.
     - **CatalystCenterGlobal ManagerPassword**: Catalyst Center Global Manager password.

> **Note**
>
> You can use the Catalyst Center Global Manager password to access the Catalyst Center Global Manager VA CLI through the AWS EC2 Serial Console.
>
> The password must
>
> - omit any tab or line breaks
> - have at least eight characters, and
> - contain characters from at least three of these categories.
>   - Lowercase letters (a-z)
>   - Uppercase letters (A-Z)
>   - Numbers (0-9)
>   - Special characters (for example, ! or #)

- **CatalystCenterGlobal ManagerFQDN**: Catalyst Center Global Manager FQDN.
- **CatalystCenterGlobal ManagerHttpsProxy**: (Optional) Enterprise HTTPS proxy.
- **CatalystCenterGlobal ManagerHttpsProxyUsername**: (Optional) HTTPS proxy username.
- **CatalystCenterGlobal ManagerHttpsProxyPassword**: (Optional) HTTPS proxy password.

8. Optional: Click **Next** to configure the stack options.
9. Click **Next** to review your stack information.
10. Click **Submit** when you are satisfied with the configuration.

    Stack creation usually takes 45 to 60 minutes.

Verify the Catalyst Center Global Manager VA TAR file

Details the Catalyst Center Global Manager VA TAR file verification process using Cisco public keys and signatures to ensure file integrity.

Before deploying the Catalyst Center Global Manager VA, we recommend that you verify that the TAR file that you downloaded is a genuine Cisco TAR file.

Before you begin

Ensure that you downloaded the Catalyst Center Global Manager VA TAR file from the Cisco Software Download site.

Procedure

---

1. Download the secure hash algorithm (SHA512) checksum file for the TAR file from the same location specified for downloading the Catalyst Center Global Manager OVA file, as specified by Cisco.
2. Obtain the signature file (.sig) for the TAR file from Cisco support through email or by download from the secure Cisco website (if available).

3. Optional: Perform an SHA verification to determine whether the TAR file is corrupted due to a partial download.

   Depending on your operating system, enter one of these commands:

   - On a Linux system: **sha512sum** <tar-file-filename>
   - On a macOS system: **shasum -a 512** <tar-file-filename>

   On Microsoft Windows, use the certutil tool because it does not include a built-in checksum utility:

   ```
   certutil -hashfile <filename> sha256
   ```

   For example:

   On Windows, you can also use Windows PowerShell to generate the digest. For example:

   Compare the command output to the SHA512 checksum file that you downloaded. If the command output does not match the SHA512 checksum file, download the TAR file again and run the appropriate command again. If the output still does not match, contact Cisco support.

4. Verify that the TAR file is genuine and from Cisco by verifying its signature:

   openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature <signature-filename> <tar-file-filename>

   > **Note**
   >
   > This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL (available on the OpenSSL Downloads site) if you have not already done so.

   If the TAR file is genuine, running this command displays a `Verified OK` message. If this message fails to appear, do not install the TAR file and contact Cisco support.

Validate the deployment

Explains how to verify a successful deployment, including network connectivity checks, system authentication, and Catalyst Center Global Manager GUI access testing.

Perform these validation checks to ensure that your environment setup and Catalyst Center Global Manager VA configuration work.

Before you begin

Ensure that your stack creation on AWS CloudFormation has no errors.

Procedure

---

1. From the Amazon EC2 console, validate the network and system configuration and verify that the Catalyst Center Global Manager IP address is correct.
2. Send a ping to the Catalyst Center Global Manager IP address to ensure that your host details and network connection are valid.
3. Establish an SSH connection with Catalyst Center Global Manager to verify that Catalyst Center Global Manager is authenticated.
4. Test HTTPS accessibility to the Catalyst Center Global Manager GUI using one of these methods:

- Use a browser.

  For more information about browser compatibility, see the *Release Notes for Cisco Catalyst Center Global Manager*.

- Use Telnet through the CLI.
- Use curl through the CLI.

Deployment using AWS Marketplace

Describes how to deploy Catalyst Center Global Manager on AWS using AWS Marketplace.

This chapter explains how to deploy Catalyst Center Global Manager on AWS using AWS Marketplace. It covers the required prerequisites, step-by-step deployment instructions, and procedures for the TAR file verification and Catalyst Center Global Manager VA deployment validation.

Prerequisites for deployment using AWS Marketplace

Lists the network, AWS infrastructure, and Catalyst Center Global Manager instance requirements–including VPC, security group, and region settings–needed to prepare for a Catalyst Center Global Manager on AWS deployment using AWS Marketplace.

Before deploying Catalyst Center Global Manager on AWS, ensure you meet these network, AWS, and Catalyst Center Global Manager requirements.

Network environment requirements

You have this information about your network environment on hand:

- Enterprise DNS server IP address
- (Optional) HTTPS network proxy details

AWS account requirements

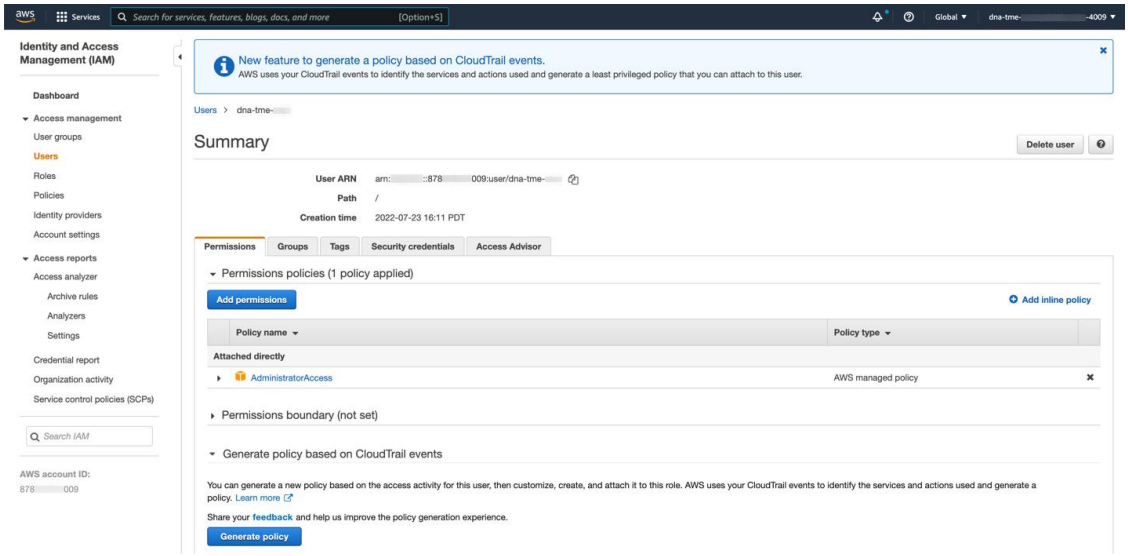
You must meet these AWS account requirements:

- You have valid credentials to access your AWS account.

  Tip

  We recommend that your Catalyst Center Global Manager account be a subaccount (a child account) to maintain resource independence and isolation. A subaccount ensures that the Catalyst Center Global Manager deployment does not impact your existing resources.

- **Important**: Your AWS account is subscribed to Cisco Catalyst Center Global Manager Virtual Appliance - Bring Your Own License (BYOL) in AWS Marketplace.
- You have administrator access permission for your AWS account. In AWS, the policy name is displayed as **AdministratorAccess**.



AWS network infrastructure requirements

You must set up these resources and services in AWS:

- **VPC**: The recommended CIDR range is /25. In IPv4 CIDR notation, the last octet (the fourth octet) of the IP address can only be 0 or 128. For example, x.x.x.0 or x.x.x.128 are valid options.
- **Subnets**: The recommended subnet range is /28, and it should not overlap with your corporate subnet.
- **Route tables**: Make sure that your VPC subnet is allowed to communicate with your enterprise network through your VPN Gateway (VPN GW) or Transit Gateway (TGW).
- **Security groups**: To ensure communication between the Catalyst Center Global Manager on AWS and the Catalyst Center in your enterprise network, the AWS security group attached to Catalyst Center Global Manager on AWS must allow TCP port 443.

  For more information about the ports that Catalyst Center Global Manager uses, see Required firewall ports and connectivity.
- **VPN GW or TGW**: You must have an existing connection to your enterprise network, which is your Customer Gateway (CGW).

  For your existing connection from the CGW to AWS, ensure that the correct ports are open for traffic flow to and from your Catalyst Center Global Manager VA. You can open them using either the firewall settings or a proxy gateway. For information about the well-known network service ports that the appliance uses, see Required firewall ports and connectivity.
- **Site-to-site VPN connection**: You can use TGW attachments and TGW route tables.

AWS region configuration requirements

You must meet these AWS region configuration requirements:

- Your AWS environment must be configured with one of these regions:
  - af-south-1 (Cape Town)
  - ap-east-1 (Hong Kong)
  - ap-northeast-1 (Tokyo)
  - ap-northeast-2 (Seoul)
  - ap-northeast-3 (Osaka)

- ap-south-1 (Mumbai)
- ap-south-2 (Hyderabad)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ap-southeast-3 (Jakarta)
- ap-southeast-4 (Melbourne)
- ca-central-1 (Canada Central)
- ca-west-1 (Calgary)
- eu-central-1 (Frankfurt)
- eu-central-2 (Zurich)
- eu-north-1 (Stockholm)
- eu-south-1 (Milan)
- eu-south-2 (Spain)
- eu-west-1 (Ireland)
- eu-west-2 (London)
- eu-west-3 (Paris)
- il-central-1 (Tel Aviv)
- sa-east-1 (São Paulo)
- us-east-1 (Northern Virginia)
- us-east-2 (Ohio)
- us-gov-east-1 (AWS GovCloud US-East)
- us-gov-west-1 (AWS GovCloud US-West)
- us-west-1 (Northern California)
- us-west-2 (Oregon)

- The Catalyst Center Global Manager c5.2xlarge instance size isn't supported in these availability zones:
  - The us-east-1e availability zone in the us-east-1 region
  - The ap-northeast-2b and ap-northeast-2d availability zones in the ap-northeast-2 region
  - The ca-central-1d availability zone in the ca-central-1 region

IAM user group requirement (optional)

If you want to enable multiple IAM users with the ability to configure Catalyst Center Global Manager using the same environment setup, you need to create a group with these policies and then add the required users to that group:

- IAMReadOnlyAccess
- AmazonEC2FullAccess
- AWSCloudFormationFullAccess

Catalyst Center Global Manager instance requirements

The Catalyst Center Global Manager instance size must meet these minimum resource requirements:

- c5.2xlarge

> **Note**
>
> Catalyst Center Global Manager supports only the c5.2xlarge instance size. Any changes to this configuration aren't supported.

- 8 virtual CPUs (vCPUs)
- 16-GB RAM
- 650-GB storage, provisioned as two separate EBS-gp3 disks:
  - 100-GB disk
  - 550-GB disk
- 2500 disk input and output operations per second (IOPS)
- 180-MBps disk bandwidth

Catalyst Center Global Manager backup instance requirements

The Catalyst Center Global Manager backup instance must meet these minimum resource requirements based on if you use a cloud server or an enterprise (on-premises) server:

- **Cloud backup**: t3.micro, 2 vCPUs, 1-GB RAM, and for storage, see Backup storage requirements.
- **Enterprise backup**: See Backup server requirements and Backup storage requirements.

AWS information requirements

You have this AWS information on hand:

- Subnet ID
- Security group ID
- Keypair ID
- Environment name
- CIDR reservation

Catalyst Center Global Manager environment requirements

You must meet these requirements for your Catalyst Center Global Manager environment:

- You have access to the Catalyst Center Global Manager GUI.
- You have this Catalyst Center Global Manager information on hand:
  - NTP setting
  - Default gateway setting

- CLI password
- UI username and password
- Static IP
- FQDN for the Catalyst Center Global Manager VA IP address

Deploy Catalyst Center Global Manager on AWS using AWS Marketplace

Provides the instructions for deploying Catalyst Center Global Manager on AWS via the AWS Marketplace, available for download through the Cisco Software Download site.

For instructions on how to deploy Catalyst Center Global Manager on AWS using AWS Marketplace, download the instructions file from the Cisco Software Download site.

Validate the deployment

Explains how to verify a successful deployment, including network connectivity checks, system authentication, and Catalyst Center Global Manager GUI access testing.

Perform these validation checks to ensure that your environment setup and Catalyst Center Global Manager VA configuration work.

Before you begin

Ensure that your stack creation on AWS Marketplace has no errors.

Procedure

1. From the Amazon EC2 console, validate the network and system configuration and then verify that the Catalyst Center Global Manager IP address is correct.
2. Send a ping to the Catalyst Center Global Manager IP address to ensure that your host details and network connection are valid.
3. Establish an SSH connection with Catalyst Center Global Manager to verify that Catalyst Center Global Manager is authenticated.
4. Test HTTPS accessibility to the Catalyst Center Global Manager GUI using one of these methods:
   - Use a browser.

     For more information about browser compatibility, see the *Release Notes for Cisco Catalyst Center Global Manager*.
   - Use Telnet through the CLI.
   - Use curl through the CLI.

6 Deploy Catalyst Center Global Manager on Azure

Topics:

- Deployment methods
- Deployment using an ARM template
- Deployment using Azure Marketplace

Deployment methods

Outlines the supported deployment methods for Catalyst Center Global Manager on Azure and summarizes the benefits and drawbacks of each method.

There are two ways to deploy Catalyst Center Global Manager on Microsoft Azure:

- Manual deployment using an Azure Resource Manager (ARM) template
- Manual deployment using Azure Marketplace

Manual deployment using an ARM template

You manually deploy the Catalyst Center Global Manager image on Azure using a custom ARM template. Then you manually configure Catalyst Center Global Manager by creating the Azure infrastructure, establishing a VPN tunnel, and deploying your Catalyst Center Global Manager VA.

Manual deployment using Azure Marketplace

You manually deploy the Catalyst Center Global Manager image on Azure using Azure Marketplace, an online software store. Then you manually configure Catalyst Center Global Manager by creating the Azure infrastructure, establishing a VPN tunnel, and deploying your Catalyst Center Global Manager VA.

Choosing a deployment method

Consider the benefits and drawbacks of each method using this table.

Table 4: Comparison Table

Manual deployment using an ARM template	Manual deployment using Azure Marketplace
The custom ARM file is required to create a Catalyst Center Global Manager VA on Azure.	The custom ARM file is *not* required to create a Catalyst Center Global Manager VA on Azure.
You will create the Azure infrastructure, such as VNets, resource groups, and tunnels, in your Azure account. Then you will establish a VPN tunnel.	
You will deploy Catalyst Center Global Manager.	
Deployment time is approximately 1 hour.	
You can configure either • an on-premises NFS for backups or • a cloud backup server if you create and manage it.	
You will manually configure monitoring through the Azure portal.	

Deployment using an ARM template

Describes how to deploy Catalyst Center Global Manager on Azure using an ARM template.

This chapter explains how to deploy Catalyst Center Global Manager on Azure using an ARM template. You will create the Azure infrastructure, establish a VPN tunnel, and deploy Catalyst Center Global Manager.

Prerequisites for deployment using an ARM template

Lists the requirements for your Azure account, disk size, network infrastructure, and region configuration, as well as the Catalyst Center Global Manager environment, before starting the deployment.

Before you deploy Catalyst Center Global Manager on Azure using an ARM template, you must meet these Azure and Catalyst Center Global Manager requirements.

Azure account requirement

You must download the ARM template for Catalyst Center Global Manager from the Cisco Software Download site.

Azure network infrastructure requirements

You must meet these Azure network infrastructure requirements:

- The ARM template deploys only the Catalyst Center Global Manager VA. Before you begin the Catalyst Center Global Manager VA deployment, you must manually deploy these required virtual machine resources:
  - Resource group
  - Virtual network name
  - Subnet name
  - Network security groups
  - SSH public key source
- Ensure that you establish a secure tunnel between your Azure resources and enterprise router or firewall for connectivity to the devices in your enterprise network. For example, Catalyst Center Global Manager on Azure can connect to your network using Azure ExpressRoute, Cisco SD-WAN, colocation services, or an IPsec tunnel.
- For your existing connection from the enterprise router or firewall to Azure, ensure that the correct ports are open for traffic to flow to and from the Catalyst Center Global Manager VA. You can open them using either the firewall settings or a proxy gateway. Make sure that the network security groups are configured to match the list of required ports. For information about the recommended communication ports, refer to Required firewall ports and connectivity.
- The ARM template you have downloaded from the Cisco Software Download site will configure the Azure cloud Network Time Protocol (NTP) server as 168.61.215.74 for time synchronization with the Catalyst Center Global Manager VA. NTP connectivity is required for a successful configuration of the Catalyst Center Global Manager VA. Ensure that the NTP connection is allowed in the network security group and any perimeter firewall.

Azure region configuration requirement

You must deploy Catalyst Center Global Manager in an Azure region that supports the Standard_F8s_v2 size.

Azure subscription requirement

You must use a supported Azure subscription type. Catalyst Center Global Manager on Azure is not supported on Cloud Solution Provider (CSP) plans. You must use a non-CSP plan, such as Pay-As-You-Go, Microsoft Customer Agreement (MCA), and Enterprise Agreement (EA).

Catalyst Center Global Manager environment requirements

You have this Catalyst Center Global Manager information and services on hand:

- IP address, netmask, and gateway that are created from the Azure subnet.
- Enterprise DNS server.

- Fully qualified domain name (FQDN) of Catalyst Center Global Manager, which is for the DNS resolution of Catalyst Center Global Manager on day one.

Configure a custom NTP server

Shows how to configure a custom NTP server in the Catalyst Center Global Manager ARM template using a text editor.

Use this procedure to configure a custom Network Time Protocol (NTP) server for your Catalyst Center Global Manager on Azure deployment.

When Catalyst Center Global Manager on Azure is deployed using the ARM template, the default NTP server for time synchronization is the Azure cloud NTP server at IP address 168.61.215.74.

Before you begin

The NTP server configuration plays a critical role during the initial configuration and ongoing functionality of the system. So, the custom NTP server must be reachable and meet these requirements:

- The NTP server must be low stratum, no more than four.
- Jitter and offset must not exceed these maximum values:
  - Maximum offset: 500 ms
  - Maximum jitter: 299 ms

You also must contact your Cisco sales representative to request the required files for this release.

Procedure

1. Open the downloaded file for the Catalyst Center Global Manager ARM template in a text editor.
2. Search for lines 123 and 124.

   Note

   Do not modify lines 123 and 124. Each line is long.

3. Search for the NTP server property in each line. Enter the custom IP address instead of the default IP address 168.61.215.74.

   You must keep the existing format, including the double quotes.

   For example, in this figure, you would need to replace the existing NTP IP address with the required value. Do not make any other modifications.

4. Save the updated file locally.

The Catalyst Center Global Manager ARM template is updated with the custom NTP server configuration.

What to do next

Deploy Catalyst Center Global Manager on Azure using the ARM template.

Deploy Catalyst Center Global Manager using an ARM template

Provides step-by-step instructions for deploying a Catalyst Center Global Manager on Azure using a custom ARM template and the Azure portal.

Use this procedure to manually deploy Catalyst Center Global Manager on Azure using a custom ARM template. The ARM template contains the relevant details for all required parameters.

Before you begin

If you want to use a custom NTP server instead of the default Azure cloud NTP server, configure a custom NTP server in the ARM template before following this procedure. For instructions, see Configure a custom NTP server.

Procedure

1. Log in to the Azure portal.
2. In the **Search** field, enter `Deploy a custom template` and press **Enter**.
3. In the **Custom deployment** window, click **Build your own template in the editor**.
4. In the **Edit template** window, create the custom template and then click **Save**.

   You can create the custom template by either

   - copying and pasting the contents of the template file into the open editor, or
   - clicking **Load file** and uploading the file.

   > **Note**
   >
   > If you configured a custom NTP server in the custom ARM template, make sure that you provide this updated version of the template.

5. In the **Custom deployment** window, under **Basics**, configure the template for the Catalyst Center Global Manager on Azure deployment.

   a. Under **Project details**, provide the required details.

      - From the **Subscription** drop-down list, choose the subscription.
      - From the **Resource group** drop-down list, choose the resource group.

   b. Under **Instance details**, provide the required details using this table.

Note

Choose the appropriate network and network security group (NSG) configurations for enabling secure access to your on-premises server. This process includes verifying the subnet routing and implementing the NSG rules to establish connectivity between Azure resources and the on-premises infrastructure.

Parameter	Description
Region	From this drop-down list, choose a region for the deployment.
Environment Name	Enter an environment name for the deployment.
Virtual Network Name	Enter the name of the virtual network where you want to deploy Catalyst Center Global Manager.
Subnet Name	Enter the subnet name for Catalyst Center Global Manager.
Network Security Group Name	Enter the name of the network security group for Catalyst Center Global Manager.
SSH public key source	From this drop-down list, choose the key that the enterprise network uses to establish an SSH connection with Catalyst Center Global Manager on Azure.
Stored Keys	From this drop-down list, choose the key that the enterprise network uses to establish an SSH connection with Catalyst Center Global Manager on Azure.
Catalyst Center Global Manager Instance IP	Enter an unused Catalyst Center Global Manager instance IP address from the subnet that's being used for Catalyst Center Global Manager.
Catalyst Center Global Manager Netmask	Enter the netmask for the subnet that's being used for Catalyst Center Global Manager.
Catalyst Center Global Manager Gateway	Enter the gateway IP address for the subnet that's being used for Catalyst Center Global Manager.
DNS Server	Enter the enterprise DNS server IP address that you want configured on Catalyst Center Global Manager.
Catalyst Center Global Manager FQDN	Enter the FQDN that you want configured on Catalyst Center Global Manager.
(Optional) **Catalyst Center Global Manager HTTPS Proxy**	Enter the enterprise proxy if needed.
(Optional) **Catalyst Center Global Manager HTTPS Proxy Username**	Enter the enterprise proxy username if needed.
(Optional) **Catalyst Center Global Manager HTTPS Proxy Password**	Enter the enterprise proxy password if needed.

Parameter	Description

Catalyst Center Global Manager Password	Enter the Catalyst Center Global Manager password that the Azure console uses to connect to the Catalyst Center Global Manager CLI.
	
	Note
	
	The password must
	• be 9 to 64 characters long, and
	• contain at least three of these categories:
	  • Uppercase letters (A through Z)
	  • Lowercase letters (a through z)
	  • Numbers (0 to 9)
	  • Special characters (for example, !, $, and #)
	
	The password must not include
	• the username or any two consecutive characters of the username
	• context-specific words, such as the service name, username, derivatives, Cisco, and maglev
	• four consecutive characters, except for special characters, and
	• any tabs or line breaks.

c. Click **Next** or **Review + Create**.

Azure performs a basic validation check of the template and displays any warnings or errors.

6. On the **Custom deployment** window, review the configuration and then click **Create** to approve the configuration and start the deployment.

When the deployment successfully completes, the resources display in the corresponding deployed resource group.

Verify the Catalyst Center Global Manager on Azure deployment

Outlines the steps to verify that the Catalyst Center Global Manager is functioning correctly by checking the IP address configurations and testing access to the management interfaces.

Use this procedure to verify that Catalyst Center Global Manager is functioning.

Before you begin

After you deploy Catalyst Center Global Manager on Azure, wait 1 hour before logging in to the Catalyst Center Global Manager UI.

Procedure

1. Verify that the IP address for the Catalyst Center Global Manager VA matches the corresponding configuration on the Azure network interface.
   a. Log in to the Azure portal.
   b. Navigate to the virtual machine page using the search bar.
   c. Select your virtual machine.
   d. Under **Network**, click **Network Settings**.
   e. Go to the network interface.
   f. Verify that the IP address for the Catalyst Center Global Manager VA matches the corresponding configuration on the Azure network interface.
2. Optional: Ping the Catalyst Center Global Manager IP address from an on-premises server.
3. Optional: After a successful deployment, wait 45 to 50 minutes and then establish an SSH connection with Catalyst Center Global Manager using port 2222.

   Use the SSH public key and stored key that you configured when you deployed Catalyst Center Global Manager.
4. Verify that the Catalyst Center Global Manager UI is accessible using the Catalyst Center Global Manager IP address and port 443.

   When you log in for the first time, use the default admin username (`admin`) and password (`P@ssword9`). After, create a new admin user with a new username and password.

   Important

   Changing this password is critical to network security, especially if the people who set up the Catalyst Center Global Manager VA on Azure are different from those who will serve as its administrators.

Deployment using Azure Marketplace

Describes how to deploy Catalyst Center Global Manager on Azure using Azure Marketplace.

This chapter explains how to deploy Catalyst Center Global Manager on Azure using Azure Marketplace. You will create the Azure infrastructure, establish a VPN tunnel, and deploy Catalyst Center Global Manager.

Prerequisites for deployment using Azure Marketplace

Lists the requirements for your Azure disk size, network infrastructure, and region configuration, as well as the Catalyst Center Global Manager environment, before starting the deployment.

Before you deploy Catalyst Center Global Manager on Azure using Azure Marketplace, you must meet these Azure and Catalyst Center Global Manager requirements.

Azure network infrastructure requirements

You must meet these Azure network infrastructure requirements:

- Before you begin the Catalyst Center Global Manager VA deployment, you must manually deploy these required virtual machine resources:
  - Resource group
  - Virtual network name
  - Subnet name
  - Network security groups
  - SSH public key source
- Ensure that you establish a secure tunnel between your Azure resources and enterprise router or firewall for connectivity to the devices in your enterprise network. For example, Catalyst Center Global Manager on Azure can connect to your network using Azure ExpressRoute, Cisco SD-WAN, colocation services, or an IPsec tunnel.
- For your existing connection from the enterprise router or firewall to Azure, ensure that the correct ports are open for traffic to flow to and from the Catalyst Center Global Manager VA. You can open them using either the firewall settings or a proxy gateway. Make sure that the network security groups are configured to match the list of required ports. For information about the recommended communication ports, refer to Required firewall ports and connectivity.

Azure region configuration requirement

You must deploy Catalyst Center Global Manager in an Azure region that supports the Standard_F8s_v2 size.

Azure subscription requirement

You must use a supported Azure subscription type. Catalyst Center Global Manager on Azure is not supported on Cloud Solution Provider (CSP) plans. You must use a non-CSP plan, such as Pay-As-You-Go, Microsoft Customer Agreement (MCA), and Enterprise Agreement (EA).

Catalyst Center Global Manager environment requirements

You have this Catalyst Center Global Manager information and services on hand:

- IP address, netmask, and gateway that are created from the Azure subnet.
- Enterprise DNS server.
- Fully qualified domain name (FQDN) of Catalyst Center Global Manager, which is for the DNS resolution of Catalyst Center Global Manager on day one.

Deploy Catalyst Center Global Manager using Azure Marketplace

Provides step-by-step instructions for deploying the Catalyst Center Global Manager VA on Azure using the Azure portal, Azure Marketplace, and a cloud-init script file.

Use this procedure to manually deploy Catalyst Center Global Manager on Azure using Azure Marketplace.

Before you begin

Ensure that you meet the prerequisites for this deployment method. For more information, see Prerequisites for manual deployment using Azure Marketplace.

Procedure

1. Log in to the Azure portal.
2. Create a new resource.
   a. In the left navigation pane, click **Create a resource**.
   b. In the **Search the Marketplace** field, type `Cisco Catalyst Center Global Manager` and press `Enter`.
   c. From the search results, click **Cisco Catalyst Center Global Manager**.
   d. Click **Create** to start the deployment wizard.
3. In the Azure deployment wizard, under **Basics**, configure your Catalyst Center Global Manager VA for deployment.
   a. Under **Project details**, provide the required details:
      - From the **Subscription** drop-down list, choose a subscription.
      - From the **Resource group** drop-down list, choose an existing resource group or create a new one.
   b. Under **Instance details**, provide the required details.

      This table lists the required fields, their descriptions, and input examples.

Field	Description	Example
Virtual machine name	Enter a unique name for the Catalyst Center Global Manager VA.	catalyst-center-va-eastus
Region	From this drop-down list, choose a region for the deployment.	(US) East US
Deploy to an Azure Extended Zone	Make sure that this check box is unchecked. Check this check box only if you need to deploy Catalyst Center Global Manager to an Azure extended zone.	–
Availability options	Choose a VM availability option.	Availability zone
Zone options	Indicate how you want the zone to be assigned.	Self-selected zone

Field	Description	Example
Availability zone	Choose one availability zone or multiple availability zones. **Note** One availability zone supports one VM. If you choose multiple availability zones, choose a VM for each zone.	Zone 1
Security type	Choose a VM security type.	Standard
Image	Choose the Catalyst Center Global Manager image in Azure Marketplace.	Cisco Catalyst Center Global Manager Virtual Appliance - x64 Gen1
VM architecture	Indicate the VM architecture. It must match the image architecture.	x64
Run with Azure Spot discount	Make sure that this check box is unchecked.	–
Size	Choose the VM size.	Standard_F8s_v2 - 8 vCPUs and 16GB
Enable Hibernation	Make sure that this check box is unchecked. **Note** This option is not supported for the selected image and size.	–

c. Under **Administer account**, provide the required details.

This table lists the required fields, their descriptions, and input examples.

Field	Description	Example
Authentication type	Choose the SSH public key login method.	SSH public key
Username	Enter the default admin username (maglev) for Catalyst Center Global Manager.	maglev

Field	Description	Example
SSH public key source	From this drop-down list, choose the key that the enterprise network uses to establish an SSH connection with Catalyst Center Global Manager on Azure.	Generate new key pair
SSH Key Type	From this drop-down list, choose the key type that the enterprise network uses to establish an SSH connection with Catalyst Center Global Manager on Azure. **Note** The RSA SSH format is the recommended key type.	RSA SSH Format
Key pair name	Enter a name for the SSH key pair. **Note** Azure automatically generates and stores the SSH key pair for secure access. You can also pass the existing key name.	catalyst-center-global-manager-ssh-key

d. Under **Disks**, verify that the disk configuration is configured by default.

The Catalyst Center Global Manager image in Azure Marketplace predetermines the disk configuration.

Note

Do not manually modify the existing disks or add new disks.

e. Under **Networking**, provide the required details:

- **Virtual Network (VNet)**: Choose an existing virtual network or create a new one.
- **Subnet**: Select a subnet within the virtual network.
- **Public IP**: Select **None**.

> **Caution**
>
> Ensure that the Catalyst Center Global Manager VA is not accessible on the public internet for security reasons.

- **NIC Network Security Group (NSG)**: Choose **Advanced**. Then select an existing security group or create one. Make sure that the security group contains the required inbound and outbound rules.

f. Under **Monitoring & Management**, enable boot diagnostics and other options if required.

g. Under **Advanced tab – Custom Data (cloud-init)**, pass a cloud-init script file into the VM user data during provisioning.

> **Caution**
>
> Azure does not allow the selection of private IP addresses during an Azure Marketplace deployment. You must use the next available IP address in the virtual network. Make sure to use this IP address in the cloud-init script.

If you are using a proxy, include the proxy details in the cloud-init script. For example:

```
#cloud-config
write_files:
  - path: /etc/cloud.json
    content: |
      {
        "mks_cloudinit_version": 1,
        "addressing_mode": "ipv4",
        "network": [
          {
            "address": "10.10.0.10",
            "netmask": "255.255.255.0",
            "gateway": "10.10.0.1",
            "routes": [],
            "name": "enterprise"
          }
        ],
        "upstream_dns_servers": ["10.0.0.2"],
        "proxy": {
          "server": "http://10.30.0.42:3128",
          "username": "proxyadmin",
          "password": "Proxypass"
        },
        "ntp": {
          "servers": ["168.61.215.74"]
        },
        "fqdn": "catalyst.center.example.com",
        "cli_password": "Public1@3"
      }
```

If you are not using a proxy, remove the proxy details from the cloud-init script. For example:

```
#cloud-config
write_files:
  - path: /etc/cloud.json
    permissions: '0644'
    content: |-
      {
        "mks_cloudinit_version": 1,
        "addressing_mode": "ipv4",
        "network": [
          {
            "name": "enterprise",
            "gateway": "10.30.0.1",
            "address": "10.30.0.6",
            "netmask": "255.255.255.0",
            "routes": []
          }
        ],
        "upstream_dns_servers": [
          "172.20.0.5"
        ],
        "ntp": {
          "servers": [
            "168.61.215.74"
          ]
        },
        "fqdn": "catalyst.center.example.com",
        "cli_password": "P@ssword10"
      }
```

Azure provisions the VM and automatically applies the configuration during the first boot.

This table lists the required cloud-init script keys and their descriptions.

Key	Description
`mks_cloudinit_version`	Ensure the cloud-init version is `1`.
`addressing_mode`	Ensure the addressing mode is `ipv4`.
Network configuration	
`address`	Enter the static IP address for Catalyst Center Global Manager.
`netmask`	Enter the netmask for Catalyst Center Global Manager.
`gateway`	Enter the gateway address for Catalyst Center Global Manager.
`routes`	Do not enter a route in this field.
`name`	Ensure the name is `enterprise`.
`upstream_dns_servers`	Enter the enterprise Domain Name System (DNS) server address.
Proxy configuration	

Key	Description
`server`	(Optional) Enter the enterprise HTTPS proxy server address.
`username`	(Optional) Enter the HTTPS proxy username.
`password`	(Optional) Enter the HTTPS proxy password.
Network Time Protocol (NTP) configuration	
`servers`	Enter a custom NTP server address that is reachable from the Catalyst Center Global Manager subnet. You can use the default NTP server address: 168.61.215.74.
Catalyst Center Global Manager configuration	
`fqdn`	Enter the fully-qualified domain name (FQDN) for Catalyst Center Global Manager.

Key	Description

`cli_password`	Enter the CLI password for Catalyst Center Global Manager.
	
	Note
	
	The password must
	• be 9 to 64 characters long, and
	• contain at least three of these categories:
	  • Uppercase letters (A through Z)
	  • Lowercase letters (a through z)
	  • Numbers (0 to 9)
	  • Special characters (for example, !, $, and #)
	
	The password must not include
	• the username or any two consecutive characters of the username
	• context-specific words, such as the service name, username, derivatives, Cisco, and maglev
	• four consecutive characters, except for special characters, and
	• any tabs or line breaks.

Note

- The Catalyst Center Global Manager image in Azure Marketplace uses cloud-init to process custom data.
- Each key in the user data script specifies a mandatory value that Catalyst Center Global Manager uses.
- Use the correct syntax for each key that you configure. Azure does not validate the syntax of the input. If the syntax or values are invalid, the Catalyst Center Global Manager VA may not boot.
- Use the same CLI password for `cli_password` and `echo "password"` in the script. The CLI password must be passed within the script.
- To verify the successful expansion of the Catalyst Center Global Manager instance storage on Azure, run:

```
xfs_quota -xc 'report -h -p /data/maglev/srv/ndp'
```

4. Under **Review + Create**, review and deploy the configuration.

a. Review the configuration.

   Azure validates the settings.

b. Click **Create** to deploy the Catalyst Center Global Manager VA.

   You can monitor the deployment progress under notifications by clicking the bell icon.

5. After successfully deploying Catalyst Center Global Manager on Azure, go to **Home** > **Virtual Machines** and verify the IP address, disk settings, and network settings.

   Remember

   Verify that the private IP address matches the IP address specified in the cloud-init script. If the IP addresses don't match, assign the private IP address as a static private IP address in the VM networking settings.

Verify the Catalyst Center Global Manager deployment

Outlines the steps to verify that the Catalyst Center Global Manager VA is functioning correctly by checking the IP address configurations and testing access to the management interfaces.

Use this procedure to verify that Catalyst Center Global Manager is functioning.

Before you begin

After you deploy Catalyst Center Global Manager on Azure, wait 1 hour before logging in to the Catalyst Center Global Manager UI.

Procedure

1. Verify that the IP address and cloud-init parameters for the Catalyst Center Global Manager VA match the corresponding configuration on the Azure network interface.

   a. Log in to the Azure portal.

   b. Navigate to the virtual machine page using the search bar.

   c. Select your virtual machine.

   d. Under **Network**, click **Network Settings**.

   e. Go to the network interface.

   f. Verify that the IP address and cloud-init parameters for the Catalyst Center Global Manager VA match the corresponding configuration on the Azure network interface.

2. Optional: Ping the Catalyst Center Global Manager IP address from an on-premises server.
3. Optional: After a successful deployment, wait 45 to 50 minutes and then establish an SSH connection with Catalyst Center Global Manager using port 2222.

   Use the SSH public key and stored key that you configured when you deployed Catalyst Center Global Manager.

4. Verify that the Catalyst Center Global Manager UI is accessible using the Catalyst Center Global Manager IP address and port 443.

   When you log in for the first time, use the default admin username (`admin`) and password (`P@ssword9`). After, create a new admin user with a new username and password.

Important

Changing this password is critical to network security, especially if the people who set up the Catalyst Center Global Manager VA on Azure are different from those who will serve as its administrators.

7 Deploy Catalyst Center Global Manager on Ubuntu KVM

Topics:

- Catalyst Center Global Manager on Ubuntu KVM
- Deploy Catalyst Center Global Manager on Ubuntu KVM
- Prepare for the Catalyst Center Global Manager virtual machine
- Deploy the Catalyst Center Global Manager virtual machine using Ubuntu Desktop
- Deploy the Catalyst Center Global Manager virtual machine using Ubuntu Server
- Configure a Catalyst Center Global Manager virtual appliance
- Verify the Catalyst Center Global Manager deployment

Catalyst Center Global Manager on Ubuntu KVM

Introduces Catalyst Center Global Manager on Ubuntu KVM as a virtual machine deployment in your on-premises environment.

Catalyst Center Global Manager on Ubuntu KVM is a deployment model that

- provides full functionality of Catalyst Center Global Manager in a virtual format
- allows rapid deployment of Catalyst Center Global Manager in your network environment, and
- allows you to evaluate Catalyst Center Global Manager without purchasing a physical appliance.

Catalyst Center Global Manager offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Catalyst Center Global Manager user interface provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

Deployment methods

Describes the supported deployment methods for Catalyst Center Global Manager on Ubuntu KVM.

You can manually deploy Catalyst Center Global Manager on Ubuntu KVM by usingUbuntu Desktop and Ubuntu Server.

Deploy using Ubuntu Desktop

You manually deploy Catalyst Center Global Manager on Ubuntu KVM on an Ubuntu host with a GUI installed. In this method, you create and manage the virtual machine by using locally installed desktop-based management tools.

Deploy using Ubuntu Server

You manually deploy Catalyst Center Global Manager on Ubuntu KVM on an Ubuntu host without a GUI installed. In this method, you create and manage the virtual machine by using server-based management tools.

Deployment requirements

Lists the minimum platform, processors, memory, storage, and performance requirements for the virtual machine.

Before you deploy Catalyst Center Global Manager on Ubuntu KVM, make sure that the virtual machine meets these minimum requirements.

Table 5: Virtual machine minimum requirements

Feature	Description
Virtualization platform and hypervisor	Kernel-based Virtual Machine (KVM) on Ubuntu 22.04 LTS or Ubuntu 24.04 LTS.
Processors	Intel Xeon Scalable server processor (Cascade Lake or newer) or AMD EPYC Gen2 with 2.1 GHz or better clock speed. Dedicate 8 virtual CPUs (vCPUs) with a 16 GHz reservation to the virtual machine (VM).
Hard Disk Drive (HDD)	100 GB + 550 GB (2 HDDs).
Memory	16 GB RAM.
I/O bandwidth	180 MB/sec.

Feature	Description
Input/output operations per second (IOPS) rate	2,000 to 2,500, with less than 5 ms of I/O completion latency.
Latency	Catalyst Center Global Manager to Catalyst Center connectivity: ≤ 350 ms (less than or equal to 350 ms).

> ⚠ **Caution**
>
> Any changes to the resource allocation or reservation of the Catalyst Center Global Manager virtual machine may adversely affect its operations and could result in failure.

Deployment prerequisites

Provides the Catalyst Center environment, network, and internet access prerequisites for deploying Catalyst Center Global Manager on Ubuntu KVM.

Meet these prerequisites to deploy Catalyst Center Global Manager on Ubuntu KVM.

Enterprise interface reservations

Describes the enterprise interface reservation requirements for deploying Catalyst Center Global Manager on Ubuntu KVM.

An enterprise interface reservation is a network configuration requirement that

- dedicates an interface on the VA for enterprise network connectivity,
- requires recording the assigned IP address for later use during appliance setup, and
- may support management interfaces and additional network interfaces for appliance administration.

Before setting up the VA:

- Reserve at least one 1-Gbps or 10-Gbps Enterprise interface to connect to your enterprise network.
- Note the IP address for this interface. You will enter it later during appliance configuration.
- Optionally, reserve a 1-Gbps or 10-Gbps Management interface for accessing the Catalyst Center Global Manager on Ubuntu KVM GUI. Note its IP address if you plan to configure it.

Note:

- The IP address of the intracluster interface is predefined. You do not need to enter it when you complete either the Maglev Configuration wizard with default mode selected or the browser-based Install Configuration wizard.
- Catalyst Center Global Manager on Ubuntu KVM supports configuring one additional interface for use by the VA. If your deployment requires an additional interface, add and connect it before you configure the VA.

DNS, NTP, and proxy server settings

Describes how to prepare the DNS, NTP, and proxy servers your VA will use.

Before you configure your VA, do these tasks:

- Obtain the IP address or host name of the NTP server.

- If you use a proxy server, obtain its URL or host name and login credentials.

While you configure your VA, you will be prompted to specify these settings:

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

Required internet URLs and fully qualified domain names

Lists the internet addresses Catalyst Center Global Manager must be able to access.

You must provide secure access to the required URLs and Fully Qualified Domain Names (FQDNs) for the appliance to function.

This table describes the features that make use of each URL and FQDN. You must configure either your network firewall or a proxy server so that IP traffic can travel to and from the appliance and these resources.

Caution

If you do not provide access to the listed URLs and FQDNs, the associated features will not work as intended.

Note

Table 6: Required URLs and FQDN access

In order to...	...Catalyst Center Global Manager must access these URLs and FQDNs
Download updates for system software and application packages.	Recommended: https://*.ciscoconnectdna.com/* [1] To avoid wildcards, specify these URLs instead.
Authenticate with the cloud domain.	https://dnaservices.cisco.com
Integrate with Webex.	• http://analytics.webexapis.com • https://webexapis.com

[1] Cisco owns and maintains ciscoconnectdna.com and its subdomains. The Cisco Connect DNA infrastructure meets Cisco Security and Trust guidelines. It is tested for security on a continuous basis. This infrastructure is robust, with built-in load balancing and automation capabilities. A cloud operations team monitors and maintains the infrastructure to ensure continuous availability.

In order to...	...Catalyst Center Global Manager must access these URLs and FQDNs
Connectivity with Cisco Catalyst Cloud and apps hosted there (e.g. AppX MS Teams Integration, Talos integration).	*.cisco.com:443 Otherwise, specific FQDNs are: • neoffers.cisco.com • neoffers-de.cisco.com • neoffers-sg.cisco.com • dnaservices.cisco.com
Access a menu of interactive help flows that let you complete specific tasks from the GUI.	https://ec.walkme.com

Catalyst Center Global Manager environment requirements

Lists environment requirements for deploying Catalyst Center Global Manager on Ubuntu KVM.

Before you deploy Catalyst Center Global Manager on Ubuntu KVM, make sure that your deployment has the required network interfaces and required image files.

Have this information on hand:

- IP address information for the correct interfaces
- Proxy server settings
- DNS server settings
- NTP server settings
- Password for the `maglev` user
- Username and password for a new Catalyst Center Global Manager GUI user

Deploy Catalyst Center Global Manager on Ubuntu KVM

Outlines the workflow for preparing the image files, creating the virtual machine, and configuring the Catalyst Center Global Manager virtual appliance on a Ubuntu host.

Use this workflow to deploy Catalyst Center Global Manager on a Ubuntu Kernel-based Virtual Machine (KVM) host.

Before you begin

Ensure that you meet the prerequisites. Refer to Deployment prerequisites.

Procedure

1. Prepare the Catalyst Center Global Manager qcow2 files for deployment.

   Complete Prepare for the Catalyst Center Global Manager virtual machine.

2. Create the Catalyst Center Global Manager virtual machine by using one of these methods:
   - Create the Catalyst Center Global Manager virtual machine using Ubuntu Desktop.
   - Create the Catalyst Center Global Manager virtual machine using Ubuntu Server.

3. Configure the Catalyst Center Global Manager virtual appliance after the virtual machine boots.

   Complete the Configure a Catalyst Center Global Manager virtual appliance.

4. Verify the Catalyst Center Global Manager deployment.

Catalyst Center Global Manager on Ubuntu KVM is successfully deployed and ready for use.

What to do next

Get started using the Catalyst Center Global Manager.

Prepare for the Catalyst Center Global Manager virtual machine

Describes how to download, copy, and extract the Catalyst Center Global Manager qcow2 package and identify the disk files before you create the virtual machine.

Use this task to prepare the Catalyst Center Global Manager qcow2 files for deployment on the Ubuntu KVM host.

After you extract the package, identify qcow2 disk 1, and disk 2 so that you can select the correct files when you create the virtual machine.

Before you begin

Ensure that you meet the deployment prerequisites and have access to the Catalyst Center Global Manager qcow2 TAR package. If you need access to the package, contact your Cisco sales representative. Refer to Deployment prerequisites.

Procedure

1. Download the Catalyst Center Global Manager qcow2 TAR package.
2. Copy the package to the Ubuntu server where KVM is installed.
3. Extract the package to the images folder.
4. Identify the location of qcow2 disk 1, and disk 2 in the extracted files.

The Catalyst Center Global Manager qcow2 files are ready to use when you create the virtual machine.

Deploy the Catalyst Center Global Manager virtual machine using Ubuntu Desktop

Covers how to use Virtual Machine Manager to import qcow2 disk 1, configure the virtual machine hardware, add the remaining disks, and start the virtual machine.

Use this task to deploy the Catalyst Center Global Manager virtual machine from the extracted qcow2 image files.

Before you begin

Ensure that you completed Prepare for the virtual machine.

Procedure

1. From the KVM console, open Virtual Machine Manager.
2. In Virtual Machine Manager, create a new virtual machine.
   a) From the **File** menu, click **New Virtual Machine**.
   b) In the **New VM** dialog box, click **Import existing disk image** on the **Step 1 of 4** page.

c) On the **Step 2 of 4** page, select disk 1 and the appropriate OS:

1. Click **Browse** and select qcow2 disk 1 from the extraction location.
2. In the **Choose the operating system you are installing** field, enter `Ubuntu 22`, and then click **Ubuntu 22.04 LTS**.
3. Click **Forward**.

d) On the **Step 3 of 4** page, allocate 8 vCPUs and 16 GB RAM for the Catalyst Center VA.

For more information, refer to Deployment requirements.

e) On the **Step 4 of 4** page, do these steps:

1. Check the **Customize configuration before install** check box.
2. Click **Network selection** and choose the network that you want to connect to from the drop-down list.
3. Verify the installation selections.
4. Click **Finish**.

3. Change the disk 1 bus type to SCSI.
   a) On the installation page, click **VirtIO Disk 1** in the left pane.
   b) Under **Details**, change the **Disk bus** type to **SCSI**.
   c) Click **Apply**.
4. Attach qcow2 disk 2.
   a) Click **Add Hardware**.

   The **Add New Virtual Hardware** dialog box displays the **Storage** details by default.

   b) Under **Details**, click **Select or create custom storage** and then click **Manage**.
   c) In the **Volumes** pane, select qcow2 disk 2 and click **Choose Volume**.
   d) Under **Details**, verify that the **Bus type** is **SCSI**.
   e) Click **Finish**.
5. Attach qcow2 disk 3.

> **Note**
>
> Disk 3 is not included in the default deployment and is optional.

   a) Click **Add Hardware**.

   The **Add New Virtual Hardware** dialog box displays the **Storage** details by default.

   b) Under **Details**, click **Select or create custom storage** and then click **Manage**.
   c) In the **Volumes** pane, select qcow2 disk 3 and click **Choose Volume**.
   d) Under **Details**, verify that the **Bus type** is **SCSI**.
   e) Click **Finish**.
6. Configure the destination network for the enterprise interface.
   a) In the left pane, click **NIC*<unique value>***.
   b) From the **Network source** drop-down list, choose the network that will connect to the Catalyst Center Global Manager on Ubuntu KVM enterprise interface.

To add and configure additional NICs, refer to Configure additional NICs.

7. Click **Begin Installation** to start the virtual machine.

   The virtual machine begins to boot.

The Catalyst Center Global Manager virtual machine is created in Virtual Machine Manager and booted. Then the Maglev Configuration Wizard automatically opens.

Configure additional NICs

Describes how to add additional network interface cards (NICs) in Virtual Machine Manager and configure the Management interface.

Use this procedure to add additional network interface cards (NICs), configure the networks that connect to them, and configure the Management interface on the virtual appliance.

Procedure

---

1. In Virtual Machine Manager, open the virtual machine hardware customization settings.
2. Power off the virtual machine.
3. Add a NIC:
   a) Click **Add Hardware**.
   b) In the **Add New Virtual Hardware** dialog box, click **Network** in the left pane.
   c) Under **Details**, define the **Network source**, such as Network Address Translation (NAT) or Bridge, and the **Device name**, such as `br1`.
4. Configure the NIC:
   a) In the left pane, click the new NIC, displayed as **NIC*<unique value>***.
   b) From the **Network source** drop-down list, choose the network that this NIC will use.
5. Repeat Step 3 and Step 4 for each additional NIC that your deployment requires.
6. Power on the virtual machine.
7. Do one of these tasks:
   - If you have not already configured the virtual appliance, configure it by using one of the methods described in "Configure a virtual appliance".
   - If you have already configured the virtual appliance, continue to the next step.
8. After Catalyst Center Global Manager Ubuntu KVM comes up, run the Configuration wizard to configure the Management interface:
   a) Open a terminal window to the virtual machine.
   b) Run the `sudo maglev-config update` command.
   c) In the Configuration wizard, review the settings for the Enterprise interface, and then click **next>>**.
   d) Review the settings for the Intracluster interface, and then click **next>>**.
   e) For the Management interface (**NETWORK ADAPTER 3**), enter these values, and then click **next>>**:
      - **Host IPv4 Address** field: Enter the IP address for the Management interface.
      - **IPv4 Netmask/IPv6 Prefix Length** field: Enter the netmask for the interface IP address.
      - **Default Gateway IPv4/IPv6 Address** field: Enter the default gateway IP address to use for the interface.

- **IPv4 Static Routes** field: Enter one or more static routes in this format, separated by spaces: *<network>|<netmask>|<gateway>*.

The additional NICs are added to the virtual machine, connected to the chosen networks, and configured for the Management interface.

Deploy the Catalyst Center Global Manager virtual machine using Ubuntu Server

Covers how to use Cockpit to import qcow2 disk 1, configure the virtual machine hardware, add the remaining disks, configure networking, and start the virtual machine.

Use this task to deploy the Catalyst Center Global Manager virtual machine from the extracted qcow2 image files on an Ubuntu Server host.

Before you begin

Ensure that you have administrative access.

Procedure

1. Open Cockpit.
   a) Open a supported browser.

      For supported browser information, refer to the Cisco Catalyst Center Global Manager Release Notes.

   b) Go to:

      `https://<Ubuntu_Server_IP_Address>:9090`

   c) Log in using your server credentials.
2. In Cockpit, import qcow2 disk 1.
   a) From the left pane, click **Virtual machines**.
   b) On the **Virtual machines** page, click **Import VM**.
   c) In the Import a virtual machine dialog box, provide these details:
      - **Name**: Enter a unique name for your virtual machine.
      - **Connection**: Ensure **System** is selected.
      - **Disk image**: Enter the path where the disk images are stored and choose disk 1.
      - **Operating System**: Enter `Ubuntu 22.04 LTS` or `Ubuntu 24.04 LTS`.

        For more information, refer to Deployment requirements.
      - **Memory**: Enter `16` and choose **GB** from the drop-down list.

        To use MB instead, enter `16384` and choose **MB** from the drop-down list.

   d) Click **Import and edit**.
3. Update the virtual machine CPU and memory as needed based on the Deployment requirements.
   a) Under **Overview**, click **edit** next to **CPU**.
   b) In the dialog box, update the vCPU allocation and then click **Apply**:
      - **vCPU maximum**: Enter `8`.

- **vCPU count**: Enter `8`.

> **Note**
>
> Ensure that you allocate 8 virtual CPUs (vCPU) for the Catalyst Center Global Manager VA.

c) If you want to update the memory, click **edit** next to **Memory**.
d) In the dialog box, update the memory allocation and then click **Apply**.

> **Note**
>
> Ensure that you allocate 16 GB (or 16384 MB) of memory (RAM) for the Catalyst Center Global Manager VA.

4. Reconfigure qcow2 disk 1.
   a) From the **Disks** table, click **Edit** for disk 1.
   b) In the **Edit** dialog box, under **Bus**, select **scsi** and click **Save**.
5. Add qcow2 disk 2.
   a) Under **Disks**, click **Add Disk**.
   b) In the **Add disk** dialog box, provide these details and then click **Add**.
      - **Source**: Select **Custom Path**.
      - **Custom path**: Enter the path where the disk images are stored and choose the next disk.
      - **Device**: Ensure **Disk image file** is selected.
      - Under **Show additional options**, **Bus**: From the drop-down list, choose **scsi**.
   c) Repeat this step to add qcow2 disk 3.

> **Note**
>
> Disk 3 is not included in the default deployment and is optional.

6. Configure networking.
   a) Configure the destination network for the enterprise interface.
   b) Add interfaces as needed for your deployment.
7. Click **Run** to start the virtual machine.

   Under **Console**, the virtual machine console boots.

The Catalyst Center Global Manager virtual machine is created and booted. The Maglev Configuration wizard automatically opens.

Configure a Catalyst Center Global Manager virtual appliance

Describes the methods for configuring the Catalyst Center Global Manager virtual appliance after the virtual machine starts.

Before you begin, complete Prepare for the Catalyst Center Global Manager virtual machine on page 82 and create a Catalyst Center Global Manager virtual machine.

Use one of these methods to configure the virtual appliance:

- Complete Configure a virtual appliance using the maglev configuration wizard (default mode).
- Complete Configure a virtual appliance using the maglev configuration wizard (advanced mode).
- Complete Configure a virtual appliance using the web install configuration wizard.
- Complete Configure a virtual appliance using the advanced web install configuration wizard.

Each method requires values for IP address configuration, proxy, Domain Name System (DNS), Network Time Protocol (NTP), username, and password.

Verify the Catalyst Center Global Manager deployment

Presents how to verify that the Catalyst Center Global Manager is functioning correctly by checking IP connectivity and access to the management interfaces.

Use this task to verify a successful deployment of Catalyst Center Global Manager on Ubuntu KVM.

Before you begin

After you manually deploy Catalyst Center Global Manager on Ubuntu KVM, wait 1 hour before logging in to the Catalyst Center Global Manager UI.

Procedure

1. Optional: Ping the Catalyst Center Global Manager IP address from an on-premises server.
2. Optional: After a successful deployment, wait 45 to 50 minutes and then establish an SSH connection with Catalyst Center Global Manager using port 2222.

   Use the SSH public key and stored key that you configured when you manually deployed Catalyst Center Global Manager.
3. Verify that the Catalyst Center Global Manager UI is accessible using the Catalyst Center Global Manager IP address and port 443.
4. When you log in for the first time, use the default admin username (`admin`) and password (`P@ssword9`).

   After you log in, create a new admin user with a new username and password.

   Important

   Changing this password is critical to network security, especially if the people who set up the Catalyst Center Global Manager VA are different from those who will administer it.

The deployment is verified successfully.

What to do next

Get started using the Catalyst Center Global Manager.

8 Get Started

Topics:

- Log in to Catalyst Center Global Manager and run it
- Enable an air-gapped deployment on Catalyst Center Global Manager
- Enroll Catalyst Centers to Catalyst Center Global Manager
- Enroll Catalyst Centers to Catalyst Center Global Manager in air gap mode
- Site Hierarchy
- Monitor from the overview dashboard
- Alerts
- Device infrastructure
- Endpoints
- Situational dashboard
- Controllers
- Controller backups
- Controller upgrades
- Controller certificates
- Global search
- Workflows
- Platform
- Activities
- System

Log in to Catalyst Center Global Manager and run it

Provides instructions for accessing the Catalyst Center Global Manager GUI, logging in with default credentials, creating a new user account, accepting terms, activating the device, and launching the dashboard.

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.

Follow these steps to log in and access Catalyst Center Global Manager:

Procedure

1. Access the Catalyst Center Global Manager GUI by entering HTTPS:// URL and the IP address of the Catalyst Center Global Manager GUI displayed at the end of the configuration process.

   The Catalyst Center Global Manager login page appears.

   > **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 Additional deployment requirements section.

2. Log in to Catalyst Center Global Manager using 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 to access the GUI for the first time. The system deletes them after you create a new user account in step 3.

3. Create a new user account for Catalyst Center Global Manager after the password is authenticated.
   - Catalyst Center Global Manager logs you out. Log back in using the newly created user account.
   - Each of the controllers managed by Catalyst Center Global Manager should have an identical user account created on it.

4. Click **Log In** after creating the Catalyst Center Global Manager account to complete the first-time set up.

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

5. Click **Next** to accept the terms and conditions.

   The **Login to Cisco.com** window appears.

Ensure that you:

- use the valid cisco.com user id for completing the registration workflow.
- enable the pop-ups for the page in the browser.

6. Click **Next**.

   The **Activate your device** window appears.

7. Click **Next** to get the activation code and activate the Catalyst Center Global Manager to Cisco Catalyst Cloud.

   The **Device activated** window appears.

   Then the **Registration to Catalyst cloud completed** window appears.

   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**
   >
   > If you cannot log in, a failure message appears indicating that registration with Cisco Catalyst Cloud could not be completed due to an authentication issue. In this case, wait a few minutes and sign in again, or check your browser pop-up settings.

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

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

   > **Note**
   >
   > - The menu displays only a few options, such as **Overview**, **Activities**, and **System**, when there are no controllers enrolled on day-0 or after all controllers are deleted on day-n.
   > - The **Overview** page displays a standard message regarding controller registration.

Enable an air-gapped deployment on Catalyst Center Global Manager

Explains the process for isolating the network and performing manual data transfers for air-gapped deployments.

An air gap is a security measure that involves isolating a network and preventing it from establishing external connections. Transfer data into an air-gapped network by inserting removable media, such as a USB drive, or by connecting a laptop. To enable an air gap for your Catalyst Center Global Manager on ESXi deployment, complete these steps.

Procedure

1. Deploy a virtual appliance.

2. Contact the Cisco Technical Assistance Center (TAC) to enable an air gap for your network.

Enroll Catalyst Centers to Catalyst Center Global Manager

Details the process of registering Catalyst Center controllers with Catalyst Center Global Manager, requiring integration with Cisco Catalyst Cloud and specifying controller details like IP address and Member ID.

To register Catalyst Center with Catalyst Center Global Manager, it's necessary to integrate Catalyst Center with the Cisco Catalyst Cloud. Log in to Catalyst Center to start the process.

Note

- The minimum supported versions of the Catalyst Center are 2.3.7.9, 2.3.7.10, 2.3.7.11, 3.1.3, 3.1.5, 3.1.6, 3.2.1, and 3.2.3.
- Use this procedure for cloud-connected deployments. For deployments where Catalyst Center Global Manager is configured in air gap mode, see **Enroll Catalyst Center to Catalyst Center Global Manager in air gap mode**.
- You can enroll a Catalyst Center 3.2.3 and later that is configured for Disaster Recovery (DR) with Catalyst Center Global Manager. DR-enabled Catalyst Centers support both single-node and 3-node deployments.
- Before you enroll a DR-enabled Catalyst Center, ensure that:
  - The Catalyst Center DR setup is complete and stable.
  - The active Catalyst Center site is reachable from Catalyst Center Global Manager.
  - For a 3-node Catalyst Center cluster, use the cluster Management or Enterprise VIP or FQDN, or the IP address of an individual node.
  - For a single-node Catalyst Center, use the reachable enterprise interface IP address or FQDN of the active node.
  - The same user account exists on Catalyst Center Global Manager and the Catalyst Center that you are enrolling.

Procedure

1. From the **Overview** menu, click **+ Controller** to enroll a new Catalyst Center controller.

   You are redirected to the **Controllers** page to add a controller.

   The **Add Controller** window appears.

2. Enter these details:
   - **Controller Name**: Enter the name of controller. This is optional.
   - **Controller IP Address or FQDN**: Enter the reachable IP address or FQDN.

> **Note**
>
> This address is only used for initial enrollment setup completion.

- **Controller Member ID**: Enter member ID of the Catalyst Center.

> **Note**
>
> **Member ID** is a global unique identifier for each instance of the controller that gets assigned when it gets created and is registered with the Catalyst Center Global Manager Cloud.

To obtain the member ID of the Catalyst Center:

a. Log into your Catalyst Center dashboard.

b. Click the **?** icon in the Catalyst Center product header, then select **About** > **Member ID** to view your member ID.

> **Note**
>
> - For a DR-enabled Catalyst Center, enter the Management or Enterprise VIP IP address or FQDN of the currently active Catalyst Center. If you use an FQDN, ensure that DNS resolves to the active DR site during enrollment.
> - For a 3-node DR deployment, enter the Enterprise VIP or FQDN of the active cluster or enter the IP address of an individual cluster node that is reachable to global manager.
> - Enter the **Controller Member ID** from the same active Catalyst Center you are enrolling. To view the Member ID, log in to the active Catalyst Center dashboard and click **? About > Member ID**.
> - For DR-enabled Catalyst Center enrollment, enroll only the active setup IP address along with **Member ID**s once. During a DR failover, the Global Manager automatically updates these details and continues to manage the system seamlessly.

3. Click **Add**.

   The controller gets added to the Catalyst Center Global Manager. The **Connect to controller** window appears.

4. Click **Sign in to controller** to complete the enrollment of Catalyst Center Global Manager from the controller side.

   You will be prompted to login to the controller to finish enrollment.

   The Catalyst Center page appears.

   You need to finish enrollment in Catalyst Center in the **Settings** > **External Services** > **Global Manager Integration** page. Once you successfully authenticate, it will show the **Global Manager Integration** page of the Catalyst Center to complete the enrollment.

5. Click **Enroll** to link the Catalyst Center with Catalyst Center Global Manager.

Note

- You can enroll a controller later when it appears as **pending connection** on the **System** > **Controllers** page. Select the controller and follow the instructions to enroll in the **Controller Details** window.

  Alternatively, you can enroll or delete a controller from the **System** > **Controllers** page. Click the ellipses (...) adjacent to the controller you want to manage, then select the appropriate option to view, edit the controller name, enroll, or delete the controller.

- For a DR-enabled Catalyst Center, the **Controllers Details** window includes:
  - **DR Enterprise VIP**: The floating enterprise-network IP that moves to whichever DR site is active, preserving device and user connectivity after failover.
  - **DR Management VIP**: The optional floating management-network IP that moves to the active DR site for administrative access.
  - **SR System Status**: Shows the overall operational state of the site-recovery/DR system, such as active, paused, degraded, or unconfigured.
  - **Main site**: The first DR site configured—initially active by default and normally the primary source of network services and replicated data.
  - **Witness site**: An independent VM/server that monitors site availability and provides quorum for safe automatic failover; it does not replicate application data.
  - **Recovery site**: The second Catalyst Center site—initially standby and continuously synchronized so it can become active after a failure.
  - **Active Enterprise VIP**: The site-specific enterprise VIP belonging to the Catalyst Center cluster currently serving the network.
  - **Active Management VIP**: The site-specific management VIP belonging to the currently active Catalyst Center cluster.

- In the event of a DR failover while the controller is in Pending connection state, wait until the DR failover is complete and ensure the new active Catalyst Center is reachable. Then, go to **System > Controllers**, select the pending controller, and update the controller's IP address or FQDN and Member ID, if required, before completing enrollment.

Deleting a controller is a two-step process:

a. Unenroll the controller. This action changes the controller status from **Reachable** to **Pending** connection.

b. Select the controller to delete from Catalyst Center Global Manager.

You can delete only the pending controllers from the **System** > **Controller** page section

You cannot delete an unreachable controller from Catalyst Center Global Manager. You must wait until the controller comes online before deleting it.

Note

You must add a unique controller Member ID in the Catalyst Center Global Manager. The same controller Member ID cannot be added to multiple Catalyst Center Global Manager setups.

What to do next

Go to the Catalyst Center Global Manager dashboard. A toast notification will appear for the newly enrolled controller. This notification includes a **Refresh** link for you to update the page and view data from the controller.

Once the menu options are updated, go to the **Controllers** page to:

- View the new Catalyst Center added to the Catalyst Center Global Manager.
- Edit the pending controllers.
- Enroll or add a new controller.

Note

For a DR-enabled Catalyst Center only: After enrollment, go to **System > Controllers** page and verify that the newly enrolled DR-enabled Catalyst Center is displayed as reachable. For 3-node deployments, verify that the DR Enterprise VIP, DR Management VIP, DR system status, and cluster configuration show the expected values.

Enroll Catalyst Centers to Catalyst Center Global Manager in air gap mode

Enroll supported Catalyst Centers with Catalyst Center Global Manager in an air-gapped environment.

Use this procedure to enroll supported Catalyst Centers with Catalyst Center Global Manager when air gap mode is enabled.

The existing cloud-connected enrollment workflow uses Cisco Catalyst Cloud. In air gap mode, controller enrollment uses the offline registration profiles prepared for Catalyst Center Global Manager and each supported Catalyst Center.

Before you begin

Before you begin, ensure that these requirements are met:

- Catalyst Center version is 3.3.1 and later.
- Catalyst Center Global Manager version is 1.5.1 and later.
- Both Catalyst Center and Catalyst Center Global Manager are required to be deployed in air gap mode.

> **Note**
>
> Mixed mode deployment, where one is in the cloud and the other in air gap, is not supported.

- Catalyst Center Global Manager and the Catalyst Centers can reach each other over the required internal network paths.
- The updated Catalyst Center Global Manager registration profile is uploaded to Catalyst Center Global Manager.
- The updated controller registration profile is uploaded to each Catalyst Center.

Procedure

1. Launch the controller enrollment wizard.
   a. Log in to Catalyst Center Global Manager, and navigate to the **Controllers** page.
   b. Click **+ Controller** button in the upper-right corner.

      The **Add Controller** window is displayed which includes three steps.

      - Add the Catalyst Center.
      - Download enrollment file.
      - Enroll in Catalyst Center.

   c. Enter these information:

      - **Controller name** (optional): A name for the controller.
      - **IP Address or FQDN**: The IP address or FQDN of the Catalyst Center.
      - **Member ID**: The 24-character hex identifier from the Catalyst Center.

   a) Obtain the **Member ID** of the Catalyst Center.

      1. Log into your Catalyst Center dashboard.
      2. Click the **?** icon in the Catalyst Center product header, then select **About > Member ID** to view your member ID.
      3. Copy the 24-character hex value.

      > **Note**
      >
      > - In air gap mode, this Member ID is generated locally from the cluster ID. It is not a cloud-issued identifier.
      > - The Member ID field is required. If you leave it blank, a validation error appears: **This field is required**.

2. After you add the controller, the wizard advances to the **Download enrollment file** step. Download the enrollment file to proceed.

a. Click the **Enrollment file** button to download.

b. Save the downloaded file.

This enrollment file applies to all controllers, so you only need to download it once.

> **Note**
>
> The downloaded enrollment file contains the discovery data (FQDN and certificates) that Catalyst Center needs to establish a trusted connection with Catalyst Center Global Manager.

3. After you download the enrollment file, the wizard advances to the **Enroll in Catalyst Center** step. Click the **Enroll in Catalyst Center** to proceed.

This action opens a new browser tab and redirects you to the Catalyst Center's **Global Manager Integration** page (**System > Settings > External Services > Global Manager Integration**).

> **Note**
>
> To complete the enrollment from Catalyst Center, you must have Catalyst Center administrator access.

4. Initiate the enrollment on Catalyst Center and upload the enrollment file on Catalyst Center.

a. Navigate to the Catalyst Center dashboard and click **System > Settings > External Services > Global Manager Integration**.

The **Global Manager Integration** window displays:

- **Connected To**: Updated once connection is established.
- **Enrollment Status**: Updated once connection is initiated.

b. Click the **Enroll** button to begin the enrollment process.

The **Global Manager enrollment** upload window appears with a file upload area.

c. Click or drag the enrollment file downloaded from Catalyst Center Global Manager in Step 2 into the upload area.

d. Click the **Enroll** button to validate the file and initiate the connection to Catalyst Center Global Manager.

The Catalyst Center validates the enrollment file and establishes a secure connection to the Catalyst Center Global Manager cluster.

After successful enrollment, the **Global Manager Integration** page updates to show:

- **Connected To**: The Catalyst Center Global Manager IP address.
- **Enrollment Status**: Green checkmark with "Enrolled".
- **Enrollment File**: Option to "Upload a new file" (for re-enrollment scenarios).

The connection between the Catalyst Center and Catalyst Center Global Manager is now established in air gap mode.

> **Note**
>
> For a DR-enabled Catalyst Center, the **Controllers Details** window includes:
>
> - **DR Enterprise VIP**: The floating enterprise-network IP that moves to whichever DR site is active, preserving device and user connectivity after failover.
> - **DR Management VIP**: The optional floating management-network IP that moves to the active DR site for administrative access.
> - **SR System Status**: Shows the overall operational state of the site-recovery/DR system, such as active, paused, degraded, or unconfigured.
> - **Main site**: The first DR site configured—initially active by default and normally the primary source of network services and replicated data.
> - **Witness site**: An independent VM/server that monitors site availability and provides quorum for safe automatic failover; it does not replicate application data.
> - **Recovery site**: The second Catalyst Center site—initially standby and continuously synchronized so it can become active after a failure.
> - **Active Enterprise VIP**: The site-specific enterprise VIP belonging to the Catalyst Center cluster currently serving the network.
> - **Active Management VIP**: The site-specific management VIP belonging to the currently active Catalyst Center cluster.

> **Note**
>
> The **Unenroll** button is now available to disconnect from Catalyst Center Global Manager if needed.

5. Return to Catalyst Center Global Manager and verify that the controller status is reachable.
   a. Log in to Catalyst Center Global Manager, and navigate to the **Controllers** page.

      The newly enrolled controller now appears with:

      - **Connectivity**: Reachable with green checkmark.
      - **System version**: Displays the system version.
      - **Cluster configuration**: Displays the node of cluster configuration.

      The controller enrollment in air gap mode is complete. Catalyst Center Global Manager can now manage this Catalyst Center without any cloud connectivity.

      Air gap mode only changes "how" controllers are enrolled (file-based instead of cloud-based). Once enrolled, the management experience is identical to cloud mode.

What to do next

Go to the Catalyst Center Global Manager dashboard. A toast notification will appear for the newly enrolled controller. This notification includes a **Refresh** link for you to update the page and view data from the controller.

Once the menu options are updated, go to the **Controllers** page to:

- View the new Catalyst Center added to the Catalyst Center Global Manager.
- Edit the pending controllers.
- Enroll or add a new controller.

> **Note**
>
> **For a DR-enabled Catalyst Center only**: After enrollment, go to **System > Controllers** page and verify that the newly enrolled DR-enabled Catalyst Center is displayed as reachable. For 3-node deployments, verify that the DR Enterprise VIP, DR Management VIP, DR system status, and cluster configuration show the expected values.

Site Hierarchy

Explains the aggregated view of sites across multiple controllers, how sites are combined into a single node, and the process for refreshing and searching within the 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.

> **Note**
>
> Catalyst Center Global Manager does not support non-global site-based RBAC for Catalyst Center sites; however, it displays globally scoped site-based RBAC sites in the site selector.

Rename a site

Describes how to rename buildings and areas within the Site Hierarchy from Site management, with changes configured on the Catalyst Centers.

You can rename sites in the **Site Hierarchy** from **Site management** for all related controllers. These modifications are 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.

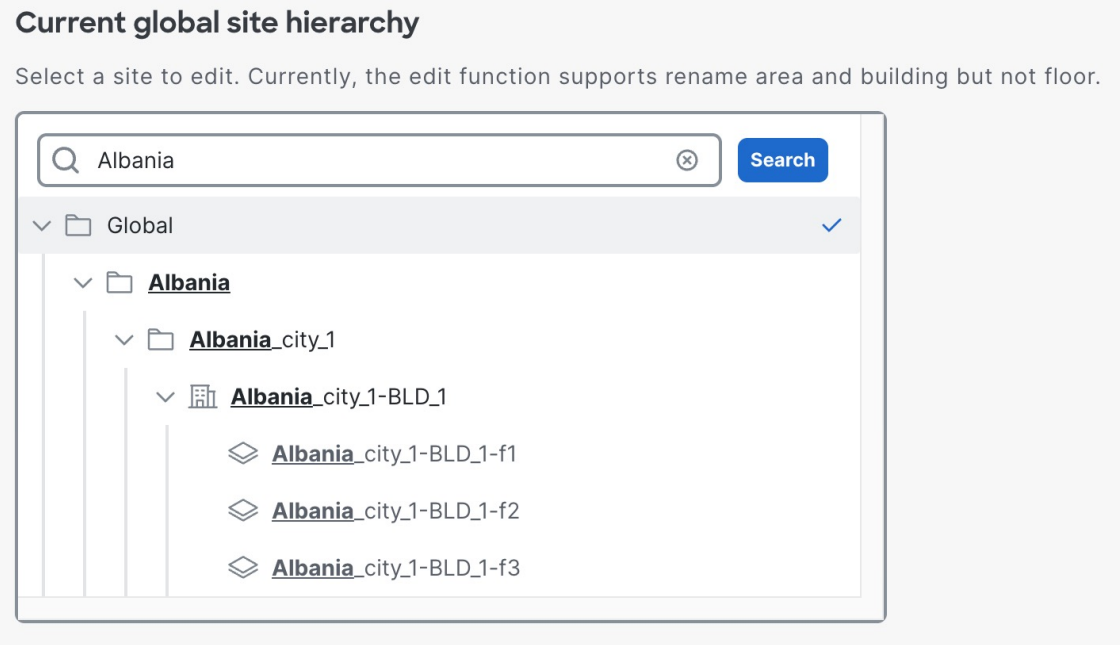
Procedure

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.

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

   A pop-up window appears showing the impacted controllers for this site.



4. On the **Edit** page, update the site name or other relevant details you want to change.
5. Click **Save**.

   The site is renamed successfully, and the updated site name appears in the site selector.

> **Note**
>
> In the site selector, the updated site name appears immediately. On other second-level pages such as **Alerts**, **Endpoints**, **Health**, and **Software-Defined Access**, the new site name appears after about 15 to 30 minutes.
>
> If any errors occur, they are displayed in the final status of the operation.

Monitor from the overview dashboard

Explains how to use the Overview page to progressively load and display data from enrolled controllers, showing controller health, network status changes, and providing options to refresh and customize dashlets.

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

After you log in to Catalyst Center Global Manager and add controllers, the Catalyst Center Global Manager starts rendering 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.

Data refresh and caching

Catalyst Center Global Manager retrieves current data from the enrolled controllers when a page loads. If a controller's status changes, a subsequent page load displays the updated data.

Note

The total loading time of a page depends on the response time of each controller.

When all enrolled controllers respond with data, the progress bar turns green. The progress bar disappears within 5 seconds after the data load is complete.

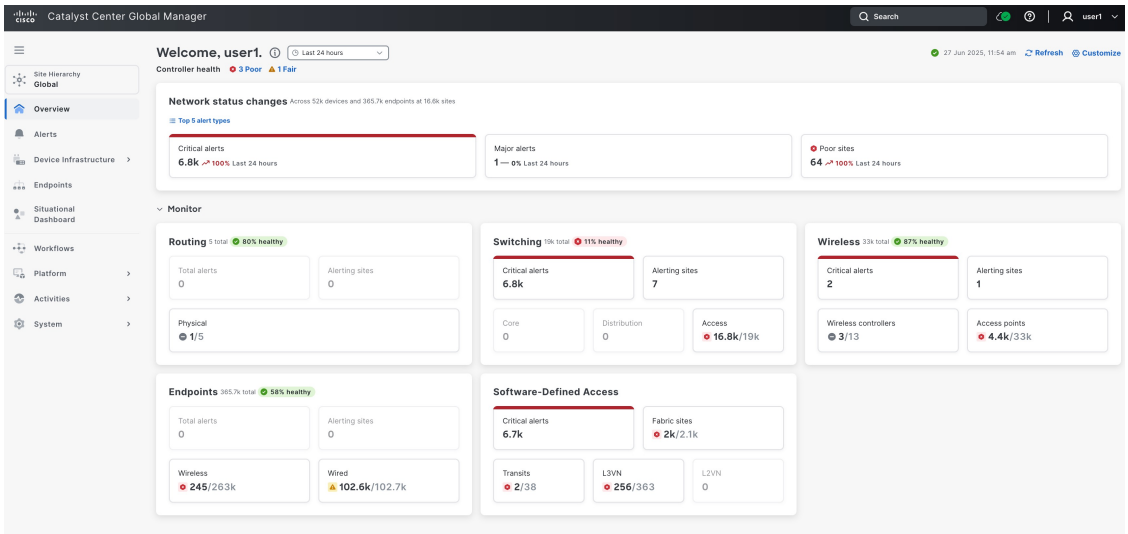
All the second-level pages, including **Alerts**, **Device infrastructure**, **Endpoints**, and **Situational Dashboards** display a **Loading complete** progress indicator.

If the progess bar is:

- Green- If the loading is success and it will vanish in five seconds.
- Blue- While the loading is in progress.
- Red- If the loading fails, and it will give you the loading error.

Note

If an error occurs while fetching data from enrolled controllers, the page displays a progress bar with error alerts. Hover over the bar to see how many controllers have responded. Click the loading status icon near the date and time to view detailed information about each failure for every dashlet in the **Overview** page.



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

Details how to view individual controller health status from the Overview page or System > Controllers, and how to cross-launch to specific controller health details for troubleshooting.

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

1. On the Catalyst Center Global Manager dashboard, go to the **Overview** page and click the controller health status to view the health of the number of displayed controllers shown. Alternatively, go to **System** > **Controllers** to view the same information.
2. Click one of the controller names to view the details. Use the cross-launch feature to access the respective controller's **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

Explains how to view network status changes on the Overview page, including critical/major alerts and poor sites, providing an overview of network health across devices and endpoints.

Network status changes provides an overview of networks across all devices and endpoints at multiple sites managed by all the Catalyst Centers. Use this information to identify potential issues that may require attention.

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

Describes how to monitor summaries and health of devices across routing, switching, wireless, endpoints, and Software-Defined Access, with options to drill down into specific alerts or health categories.

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

Alerts

Explains the Alerts feature for viewing and exploring details about alerts categorized by critical, major, minor, and informational levels, including analytics for top site groups and segment types.

The **Alerts** feature in Catalyst Center Global Manager helps you view and explore details about alerts that require your attention. You can see different alert types and analytics, including the top site groups and segment types for each alert.

To view the alerts, navigate to the Catalyst Center Global Manager dashboard and click **Alerts**. The page progressively loads data as information is received 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 provides these details.

- Loading error: Displays a loading error if there are any issues with the controller, such as 401, 403, or if it is unreachable.
- 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

Describes the Device Infrastructure section for viewing filtered details of device health and fabric sites, ensuring security and proper functioning.

The **Device Infrastructure** in Catalyst Center Global Managershows filtered details of each device health and fabric site. Use it to ensure your devices and fabric sites are secure and working well.

Device health

Details how to view the health status of devices (Poor, Fair, No Health Data, Good) under Device Infrastructure > Health, including summary, analytics, and a table of devices with export functionality.

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

The health status categories are:

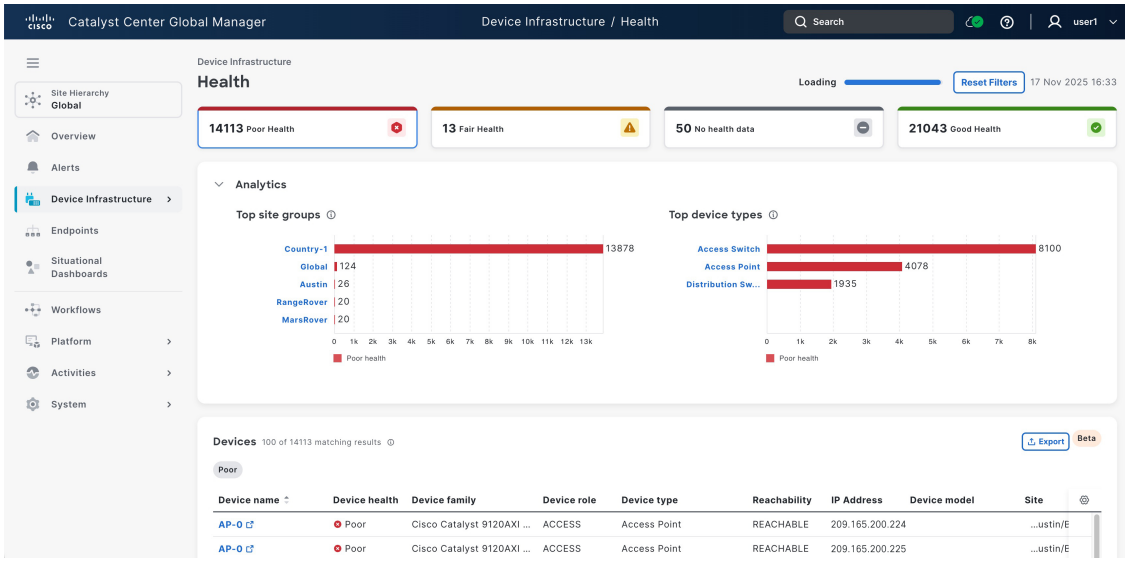
- Poor Health: Devices with a health score range from 1 to 3.
- Fair Health: Devices with a health score range from 4 to 7.
- No Health Data: Devices with no data.
- Good Health: Devices with a health score range from 8 to 10.

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:

- Loading error: Displays a loading error if there are any issues with the controller, such as 401, 403, or if it is unreachable.
- 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: Displays a table of all devices, including device name, controller, device health, and device family, based on your selection.

  The devices table displays only 100 entries.

Data export allows you to export all the matching results from the table on the device **Health** page in CSV format.

You can apply filters to tables in Catalyst Center Global Manager; however, they are limited to display first 100 records of all the matching records in the list.

To export the device health:

1. From the main menu, choose **Device Infrastructure** > **Health**.
2. From the **Devices** section, click **Export**.

   The **Device health export** window appears.
3. Click **Export** to export all results that match the applied filter.

   You will receive a toaster notification when the export completes.

   You can track the progress in the **Download** report tab.
4. Click **Download** to see the exported data with the respective filter showing the health status.

Note

- The data export process may take up to 30 minutes to complete because it progressively retrieves all matching results from the enrolled controller.
- Each exported file has a unique name.
- You can view the latest five exported reports, which are retained on the **Download** page for three days.

Software-Defined Access health

Explains how to view the health status of fabric sites, transits, L3 VNs, and L2 VNs under Device Infrastructure > Software-Defined Access, categorized by health scores.

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 page loads data progressively as it receives information 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:

- Loading error: Displays a loading error if there are any issues with the controller, such as 401, 403, or if it is unreachable.
- 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.

End-of-Life Devices

Describes the beta feature for viewing End-of-Life (EoL) information for Cisco devices (routers, switches, wireless, accessories), including expiration dates, summaries, analytics, and detailed device tables.

To view the End-of-Life (EoL) of each device, navigate to the Catalyst Center Global Manager dashboard and click **Device Infrastructure** > **End-of-life Devices**. Then the page loads data progressively as it receives information from the enrolled controllers.

The End-of-Life devices feature gives you an aggregate view of your Cisco devices that have reached or are nearing their End-of-Life (EoL) status, including key hardware and software expiration dates. This feature is similar to the EoX (End-of-life) feature in Catalyst Center, offering detailed reports on device lifecycle milestones to help with product upgrade and substitution planning.

Unified hardware refresh for End-of-Life devices is supported only on Catalyst Centers running software versions 2.3.7.10, 3.1.5, or later.

The EoL devices display counts for these categories:

- Routers
- Switches
- Wireless
- Accessories (can be part of router/switches/wireless)

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

The **End-of-life Devices** page also gives information on:

- Loading error: Displays a loading error if there are any issues with the controller, such as 401, 403, or if it is unreachable.
- Summary: Summary of EOL devices based on each device category.
- Analytics: Analytics shows the top five site groups and top device series, along with their individual counts.

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

  For example: When a site group is selected from the **Top site groups** chart, the **Top device series** chart will highlight the device types associated with that selected site group. Conversely, selecting a device type from the **Top device series** 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 series** analytics sections simultaneously. The **Devices** table below will then show devices filtered by the selected criteria, with active filters visually highlighted. The filters correspond to your selections for routers, switches, wireless devices, and accessories at the top. Unselecting a site group or device type selection from the analytics charts will clear the corresponding filter and update the **Devices** table accordingly.
- Devices: Displays a table of all devices, including device name, controller, IP address, site, device type, device model, chassis + modules, accessories, last date of support, and next milestone, based on your selection. Additional data may be selected via table settings.

  You can edit the table settings.

  You can decide what to display or hide by adjusting the table settings for the **End-of-life Devices** page. Click the gear icon in the table header. The **Table settings** window appears. You can check or uncheck the items under **Table density** and **Table columns** as needed, then click **Apply**.

  Click on **Chassis+ modules** counts to view the EOL details for each hardware component, including accessories and software EOL data.

  Click the **Accessories** counts to view the EOL details for accessories components, such as fans and power supplies.

  Click **Advanced** filter to do further filters based on the columns selected in the **Devices** table.

  Click **Controller** to view the controller name.

  You can cross-launch to the Catalyst Center to view inventory information, alerts, and device end-of-life status.

Endpoints

Explains how to view health details for wireless and wired endpoints under the Endpoints section, including top site groups and metrics, with cross-launch capabilities to Device 360 pages.

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

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

The **Endpoints** page provides additional health categories for both the wireless and wired endpoints, which include:

- 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 **Endpoints** page also gives information for both the wireless and wired endpoints on:

- Loading error: Displays a loading error if there are any issues with the controller, such as 401, 403, or if it is unreachable.
- Analytics: Analytics shows the top site groups and top metrics.

To see more information about **Connected AP**, click the Access Point (AP) name on the **Endpoints** page for wireless endpoints. This action cross-launches to the corresponding controller's **Device 360** page for the specific AP page. Similarly, to see more information about **Connected Switch**, click the connected switch name on the **Endpoints** page for wired endpoints. This cross-launches to the related controller's **Device 360** page for that specific controller switch page.

Situational dashboard

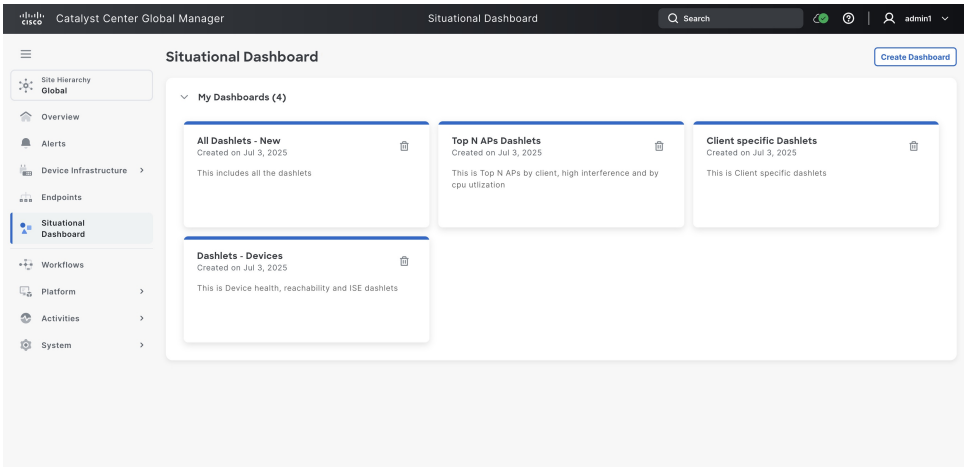
Describes the feature for creating customized dashboards using pre-built dashlets to display aggregated views of client and device health, connectivity, and performance metrics.

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.

You can select a maximum 15 dashlets on a single dashboard.

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

The image here shows the situational dashboard page with different dashlets.



Create a dashboard

Provides steps to create a new situational dashboard by entering a title, description, and selecting desired dashlets related to endpoint performance, AP metrics, network health, and network services (ISE, AAA, DHCP, DNS, PoE).

Procedure

1. From the Catalyst Center Global Manager dashboard, navigate to **Situational Dashboard** > **Create Dashboard** to create a customised page using the 32 available pre-defined dashlets.

   The **Create New Dashboard** window appears.

2. Enter the **Dashboard Title**, and the **Description**. Then, choose the views you want to enable in your dashboard from the available dashlets. These dashlets display various widgets categorized into separate sections.

   Endpoint Performance

   - Endpoint onboarding times
   - Endpoint roaming times
   - Endpoint connectivity Received Signal Strength Indicator (RSSI)
   - Endpoint connectivity Signal-to-Noise Ratio (SNR)
   - Endpoint count per Service Set Identifier (SSID)
   - Endpoint physical link connectivity
   - Endpoint count per band

   Access Point Metrics

   - Top N Access Points (APs) by endpoint count

     Here, **N** refers to the number of APs displayed.
   - Top N APs by high interference (2.4 Ghz)
   - Top N APs by CPU utilization
   - Total APs up/down

   > **Note**
   >
   > For each of the **Top N APs**, the cross-launch link is enabled that takes you to the APs respective controller **Device 360** page.

   Network Health

   - Device health count
   - Total network reachability

   Network Services

   - Authentication, Authorization and Accounting (AAA)
     a. AAA transactions

b. AAA summary

c. AAA servers top transactions by WLC

d. Top AAA latency sites

e. Top AAA failure sites

- Dynamic Host Configuration Protocol (DHCP)

a. DHCP transactions

b. DHCP summary

c. DHCP servers top transactions by device

d. Top DHCP latency sites

e. Top DHCP failure sites

- Domain Name System (DNS)

a. DNS transactions

b. DNS summary

c. DNS servers top transactions by device

d. Top DNS server latency

e. Top DNS failure sites

> **Note**
>
> Each **controller IP** has a cross-launch link enabled that takes you to the respective controller home page.

Power over Ethernet (PoE)

a. Power usage

b. PoE powered device distribution

c. PoE operational state distribution

Integrations

- Identity Services Engine (ISE)

3. Click **Save**.

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

> **Note**
>
> This dashboard is specific to your user account and is not visible to other users.

4. Click the page you have created to view aggregated data from multiple controllers.

> **Note**
>
> - Click **Refresh** to update the information displayed, ensuring you have the most current status.
> - Select the dashlet and choose **Edit** to modify the dashboard. You can then toggle off the view from the list in a window to remove dashlets from the dashboard.
> - You can switch between the created dashboard using the drop-down menu in the dashboard title's arrow icon.
> - If you select the site under **Site Hierarchy**, the dashlets will reflect the specific site data.
> - You can see the progressive loading on the **Situational Dashboard** page when the data loads. If an error occurs while fetching the data, an error alert appears on this page.
> - You can use the selector drop-down to switch from the selected situational dashboard.

Controllers

Explains how to view all enrolled Catalyst Centers on the Controllers page, displaying details like controller name, IP address, connectivity, health status, type, and system version, with options to edit names and cross-launch.

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 to view 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:

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 **Controller**s to view the controller details. The **Controller Details** window appears, and you can click any link to cross-launch to the controller page for further information.

The **Controller Details** include:

- **Controller name**: Shows the controller name, which is displayed as an IP address.
- By default, the controller name is populated during enrollment using the configured hostname, VIP address, management IP address, or Enterprise interface IP address for the Catalyst Center controller. 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 for enrolled controllers 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.

    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 GUI setting and does not affect the configuration of the controller. 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 **Controller**s name that you want to edit. The **Controller Details** window is displayed. Click **Edit** and change the name of the controller and then save.
  - All the fields are editable for the Pending controllers only.

- **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, an alert or a description of any system health event for 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 the table settings.

You can decide what to display or hide by adjusting the table settings for the **Controllers** page. Click the gear icon in the table header. The **Table Settings** window appears. You can check or uncheck the items under **Table Density** and **Table Columns** as needed, then click **Apply**.

For information about adding and deleting a controller, see Enroll Catalyst Center to Catalyst Center Global Manager.

Once a controller is added to the controller page, it appears in the list as a "Pending connection" controller. You can edit any fields of a controller when it is in pending controller status.

Pending controllers

Once a controller is added to the controller page, it appears in the list as a **Pending connection** controller. Catalyst Center Global Manager helps you manage these controllers more efficiently. You can now easily identify pending connection controllers through new warning indicators. You can now select the **View pending controller(s)** option to filter the table, allowing you to focus exclusively on pending connections.

When a controller is in the **Pending connection** status, you now have the capability to edit all fields associated with a controller. If no modifications are made to the fields, the system enables the **Complete enrollment** option, which directs you to the Catalyst Center to complete the enrollment process. If changes are made to the fields, the **Save** button is enabled. You must save your changes before you can proceed with enrollment, or cancel the changes.

The system displays a direct pop-up alert to guide you during the edit process. The **You have unsaved changes** window is displayed as the system ensures that enrollment cannot be completed until the changes have been saved, preventing configuration errors.

Cross-launch to controllers

Describes the single sign-on capability to seamlessly navigate from Catalyst Center Global Manager to registered controllers for detailed views like System 360, System Health, and Software Management.

The **Controllers** page displays various types of cross-launches in the **Controller Details** for each controller. These include 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

Explains how to access System 360 from the Controllers page to view detailed information about app stacks and services running on a selected Catalyst Center, including node and service status, with tools for monitoring (Grafana) and logging (Kibana).

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

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

   The **Controller Details** window is displayed.

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

Describes how clicking System Health in the Controller Details window cross-launches to the corresponding Catalyst Center page for detailed health information.

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

Explains how clicking Software Management in the Controller Details window cross-launches to the corresponding controller page to view installed applications or system updates.

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.

Controller backups

Explains the Controller backups page, a centralized dashboard for monitoring, troubleshooting, and managing backup statuses and configurations for all enrolled controllers.

A **Controller backups** is a feature that provides a centralized, aggregate view of your environment, allowing you to monitor statuses, troubleshoot failures, and manage backup configurations or schedules.

> **Note**
>
> - The **Controller backups** page displays enrolled controllers only; pending controllers are not shown.
> - Catalyst Center Global Manager does not store controller backup files. Each controller stores its backups in the configured storage location.

After the Catalyst Centers have been enrolled to Catalyst Center Global Manager, you can monitor the backup status of all enrolled controllers on the **Controller backups** page.

To view the backup status of all enrolled controllers, navigate to **System** > **Controller backups** page.

Key features are:

- Centralized monitoring: View the backup status of all enrolled controllers in one location.
- Status-based filtering: Filter controllers by their current backup state, including Failed, Not configured, No backup data, In progress, and Success. The **Last backup status** displays only Success, Failed, or In progress, and excluding secondary statuses such as Canceled or Deleting.
- Progressive loading: Displays data as controllers respond, ensuring you receive updates as they become available.
- Error reporting: View detailed error reports in the loading error list for any controllers that fail to retrieve the backup details.
- Cross-launch capabilities: Easily navigate to specific controller interfaces to perform advanced management tasks, such as configuring backups, restoring selected backups, and deleting or canceling any backup.

By default, the table displays all controllers and their backup status details sorted by **Last backup status** column. You can add optional table columns, such as **Scheduled scope** through the **Table settings**.

Monitoring and filtering

- **Status cards**: Select a status card (Failed, Not configured, No backup data, In progress, or Success) to filter the list of controllers.
- **Reset filters**: Click **Reset Filters** to clear all active filters and display the full list of controllers.
- **Loading errors**: Click **Loading error** to view details regarding controllers that failed to load.

Troubleshooting failures

If a controller status has failed, perform the following steps to investigate:

1. Click the controller name to view specific failure error.
2. Click **Learn more** to cross-launch the controller **Backup & Restore** page, where you can review connectivity status, backup names, and historical attempt data.

> **Note**
>
> For a failed backup status, the "Learn more" option will be available to cross-launch to the controller for troubleshooting.

Managing backup configurations and schedules

- **Configure backups**: If a controller backup is not configured, follow these steps:
  - Click the **Configure backups** link located in the **Last backup status** column of the table directly, or
  - Click the controller name on the table first, then click **Configure backup** link in the **Last backup status** column.

  This action will cross-launch you to the controller **Backup Configuration** page, where you can set up the backup settings, including specifying the backup path (NFS, physical disk, or SSH (Remote Server)).
- **View backup details**: Click controller name in the table, then click **Backup details** to view the controller backup details.

  To access advanced backup details, click **Backup details** link which will cross-launch to Catalyst Center to view the backup history and their advanced actions such as backup & restore, schedule backup or delete.

- **Schedule backups**: Select one or more controllers using the checkboxes and click **Schedule backup** to schedule the backups. You can update the backup name, schedule type, and data scope of one or more controllers.

  Note

  For virtual appliance-based controllers, any new backup schedule will overwrite the existing one. However, for on-premises controllers, if a backup schedule already exists, it must first be deleted from the controller through cross-launch before scheduling a new backup from the Catalyst Center Global Manager.

- **Additional actions**: Click the **(...)** icon in the table to cross-launch to the respective Catalyst Center to perform these actions:
  - Backup & Restore: For restore or delete backups.
  - Backup configuration: For any non-configured or new backups.

Note

- **Time zone**: All timestamps are converted to UTC to ensure consistency across controllers.
- **Platform-specific configurations**:
  - **On-premises controllers (physical appliance)**: Catalyst Center Global Manager supports configurations for both remote hosts and NFS servers.

    Limitations of On-premises controllers

    - The controller backup details, including last backup scope, scheduled scope, retained backups, and available space, are marked as N/A. This occurs because the APIs of on-premises or older controller versions do not include this data. This data is available only in the VA or 3.x version controllers.
    - You cannot edit a backup schedule that already exists on the controller. An error message appears prompting you to delete the existing schedule before creating a new one.
    - The backup names on the Catalyst Centers must meet these requirements:
      - Contain only: Lowercase letters (a-z), numbers (0-9), hyphens (-), or periods (.).
      - Start and end with: A lowercase letter or a number.

      The Catalyst Center Global Manager will convert the provided backup name into a compatible controller name that is accepted by the on-premises-based controller during scheduling.

  - **VA-based controllers**: The interface displays information about the physical disk, NFS server, and SSH (Remote Server), and the destination path.

Controller upgrades

Explains the centralized management of controller software upgrades, including monitoring upgrade process, view upgrade status, release downloads, upgrade initiation or scheduling, edit or delete an upgrade status, and handle upgrade failures within Cisco Catalyst Center Global Manager and controller GUI environments.

The Controller upgrades feature provides a centralized view of the software upgrade status for Catalyst Center controllers that are registered with Cisco Catalyst Center Global Manager. Use **Controller Upgrades** to view controller upgrade status, review upgrade activity and failure details, download a release, and start or schedule supported controller upgrades.

Catalyst Center Global Manager supports single-node and 3-node controller upgrade operations for reachable Catalyst Center 3.x controllers that are not configured for disaster recovery (DR). For Catalyst Center 2.x controllers and disaster recovery (DR)-enabled controllers, Catalyst Center Global Manager provides status visibility and a link to the controller GUI, where you can perform upgrade tasks.

Note

- Controller upgrades is not available when Catalyst Center Global Manager is deployed in air-gapped mode.
- Catalyst Center Global Manager only orchestrates the operation, while the controller downloads and installs the release, and identify where the release catalog and optional packages originate.

Workflow overview: Upgrade available → download release → Ready for upgrade → Now or Scheduled → monitor activity → handle success or failure

Prerequisites for all controller upgrades procedures:

- Before you upgrade a Catalyst Center controller, refer to the supported upgrade paths for hotfixes in the Cisco Catalyst Center Upgrade Guide, and confirm that the installed and target release builds support the upgrade:
  - Catalyst Center 3.1.6 to 3.2.x
  - Catalyst Center 3.1.x or 3.2.x to 3.3.x
- Enroll the Catalyst Center controllers that you want to manage in Catalyst Center Global Manager.
- Catalyst Center Global Manager displays registered controllers when inventory data is available, including unreachable controllers and controllers that do not support upgrade actions from Catalyst Center Global Manager.
- For controller upgrade actions, use a Super Admin account. Network Admin and Observer users can view the page and its details but cannot perform modifying operations.
- Confirm that the target controller is reachable. Catalyst Center Global Manager cannot perform an upgrade operation on an unreachable controller.
- Catalyst Center Global Manager supports upgrade actions for one controller at a time. Bulk operations are not supported.
- To perform an upgrade action from Catalyst Center Global Manager, the controller must meet all the following requirements:
  - Runs Catalyst Center 3.x.
  - Is not configured for DR.
  - Is reachable from Catalyst Center Global Manager.
  - Is in a state that supports the requested action.
- For Catalyst Center 2.3.7.x and DR-enabled controllers, use **Navigate to controller** to perform upgrade actions from the Catalyst Center GUI.
- You can select optional packages during a supported download or upgrade workflow. After the controller is up to date, Catalyst Center Global Manager does not support installing or uninstalling optional packages. To perform these operations, use the Catalyst Center GUI for the controller.

View controller upgrade status

Explains how to view controller upgrade status, interpret summary cards, search and filter controllers, review upgrade details, use **Go to Controller** to access a controller GUI, and identify available actions based on controller state and eligibility.

Use this procedure to view controller upgrade status.

Procedure

1. From the Catalyst Center Global Manager navigation pane, choose **System > Controller Upgrades**.

   The **Controller Upgrades** page opens and displays all the registered controllers, including the unreachable controllers.

2. Review the summary cards and controller table.

   The summary cards display the number of visible controllers in the following states:

   - Download failed
   - Upgrade failed
   - Upgrade available
   - Ready for upgrade

3. To display controllers in a specific state, select a summary card.

   ### Summary cards

   Summary cards count visible controllers that map to the corresponding status. A controller contributes to a card even when its version or DR configuration makes it read-only in Catalyst Center Global Manager. Controllers with an unknown status, an unavailable status, or only an API error are not counted.

   Table 7: Summary cards count

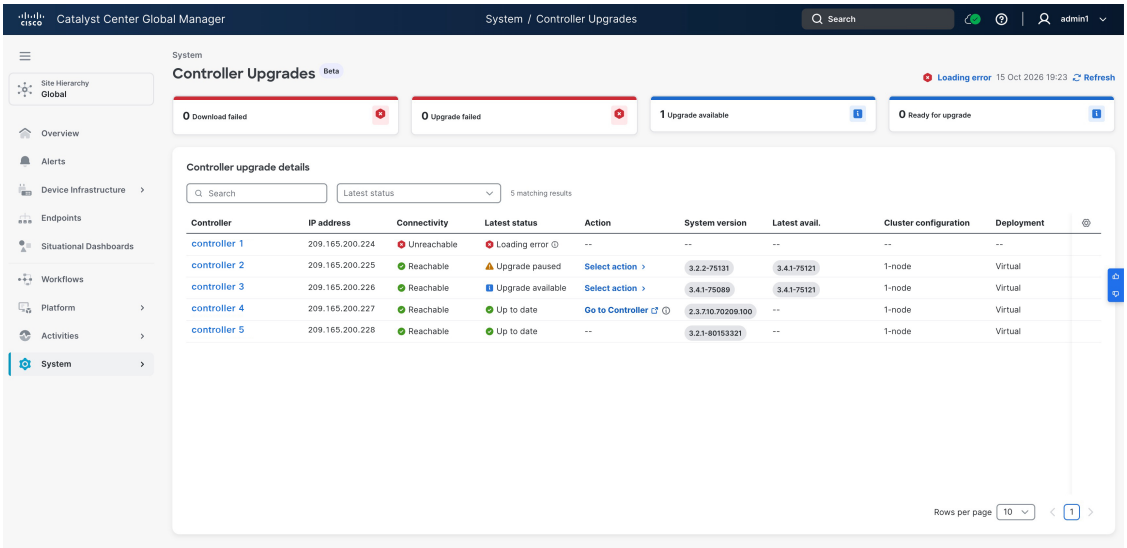
Summary cards	Controllers counted
Download failed	Controllers with the Download failed status.
Upgrade failed	Controllers with the Upgrade failed status.
Upgrade available	Controllers with the Upgrade available status.
Ready for upgrade	Controllers with the Ready for upgrade status.

4. To find a controller, use the search, filter, and sort controls.

   Use search to find a controller by name or IP address. Use status filters to focus on a normalized upgrade state and sort the displayed fields that support sorting.

5. To retrieve the latest available information, click **Refresh**.

   Refresh the page to request the latest status from the registered controllers. If a refresh fails for one controller, Catalyst Center Global Manager keeps the controller row and displays the data that remains available.



Note

A controller can appear in a summary-card count even if it is not eligible for upgrade actions in Catalyst Center Global Manager. Eligibility controls the available actions, not controller visibility.

If Catalyst Center Global Manager cannot retrieve upgrade data from a controller but inventory data is available, Catalyst Center Global Manager continues to display the controller. Fields that depend on unavailable data display two hyphens (**--**). Catalyst Center Global Manager displays available error details for the affected controller.

6. Review the controller **Upgrade Details** drawer and activity information.

   The **Controller Upgrades** details table displays the following information when it is available.

Table 8: View Controller information

Field	Description
Controller	Controller name from Catalyst Center Global Manager inventory.
IP address	Controller IP address from Catalyst Center Global Manager inventory.
Connectivity	Connectivity status between Catalyst Center Global Manager and the controller. Whether the controller is reachable or unreachable.
Latest status	Current controller upgrade status.
Action	Primary action available for the controller–**Download & Upgrade** and **Download only**.
System version	Software version currently installed on the controller.
Latest avail.	Latest release available for the controller.

Field	Description
Cluster configuration	Single-node, 3-node, or DR-enabled configuration, when available.
Deployment	Whether the deployment type is virtual or physical appliance, when available.
Last successful upgrade	Date and time of the latest successful upgrade.

- **Review a failed download**

  If you filter the table by **Download failed**, the table displays controllers whose downloads failed. Click a controller name to open the **Upgrade Details** drawer. Review the failure details, including the latest download activity and the reason for the failure. From the drawer, select **Retry download** to retry the download or **Delete download** to remove the failed download.

  You can also perform these actions from the **Controller upgrades** table. Open **Actions**, and select **Retry download** or **Delete download**.

- **Review a failed upgrade**

  If you filter the table by **Upgrade failed**, the table displays controllers whose upgrade failed. Click a controller name to open the **Upgrade Details** drawer. Review the failure details to see the workflow stage where the upgrade failed, such as the pre check step or some other step.

  From the drawer:

  - Select **Retry upgrade** to retry the upgrade.
  - Click **View activities** to cross-launch to the related controller release activity.
  - Click **View available applications** to view the applications available for the controller.

- **Review an available upgrade**

  If you filter the table by **Upgrade available**, the table displays controllers with the new releases available. Open **Actions**, and select one of these options:

  - **Download & Upgrade**: to view and select an available release and optional packages, then download and upgrade the controller.
  - **Download only**: to view and select an available release and optional packages, then download the release without upgrading the controller.

- **Ready to start upgrade**

  If you filter the table by **Ready for upgrade**, the table displays controllers that are ready to upgrade. Open **Actions**, and select one of these options:

  - **Upgrade**: Select this option if you already have downloaded the target release. You can either start the upgrade immediately or do the scheduled upgrade.

    Click a controller name to open the **Upgrade Details** drawer to view the upgrading status progress.

  - **Delete download**: Select this option to delete any downloaded release.

7. To open the Catalyst Center GUI for the controller, click **Go to controller**.

   Catalyst Center Global Managerprovides **Go to controller** only when the controller is reachable and Catalyst Center Global Manager can create the controller link.

> **Note**
>
> Catalyst Center Global Manager does not display **Go to controller** for unreachable controllers.

Controller eligibility

Catalyst Center Global Manager displays controllers regardless of whether they support upgrade actions. Catalyst Center Global Manager enables an action only when the controller, user role, and current controller state support the action.

Table 9: Controller category

Controller category	Catalyst Center Global Manager behavior
Reachable Catalyst Center 3.x (single-node or 3-node), non-DR	Upgrade actions are available according to role and current state.
Reachable Catalyst Center 3.x (single-node or 3-node), DR-enabled	Read-only in Catalyst Center Global Manager. Upgrades must be managed locally to preserve synchronized state and service continuity
Reachable Catalyst Center 2.3.7.x, non-DR	Read-only in Catalyst Center Global Manager. Upgrades from 2.3.7.x to 2.3.7.x or 3.x must be performed directly on the controller because of underlying architectural changes.
Unreachable controller	Displayed when inventory data is available; upgrade actions and Go to Controller may be unavailable.

For 2.3.7.x and DR-enabled controllers, Catalyst Center Global Manager displays upgrade information when available. Use **Go to controller** to perform upgrade tasks in the Catalyst Center GUI.

Upgrade actions by status

The available actions depend on the controller version, DR configuration, reachability, user role, and current upgrade state. Catalyst Center Global Manager supports only one mutating controller operation at a time. If the state changes before an action is submitted and the controller rejects the request, Catalyst Center Global Manager displays the backend error and keeps the controller visible.

Table 10: Upgrade actions

Display state	Available Catalyst Center Global Manager actions for an eligible controller
Up to date	Displays the status in Catalyst Center Global Manager and perform actions through Catalyst Center.
Upgrade available	Download, Upgrade now, or Schedule upgrade.
Downloading	Cancel download.
Download failed	Retry download or Delete download.
Ready for upgrade	Upgrade now, Schedule upgrade, or Delete download.

Display state	Available Catalyst Center Global Manager actions for an eligible controller
Upgrade scheduled	Upgrade now, Edit schedule, or Delete schedule.
Upgrading	Displays the status in Catalyst Center Global Manager and perform actions through Catalyst Center.
Upgrade paused	Retry or Cancel upgrade, when supported by the controller.
Upgrade failed	Retry upgrade.
Canceling download	Displays the status in Catalyst Center Global Manager and perform actions through Catalyst Center.
Download canceled	Delete download.
Cancel download failed	Delete download.
Deleting download	Displays the status in Catalyst Center Global Manager and perform actions through Catalyst Center.
Delete download failed	Retry delete, when supported by the controller.
Installing applications	Displays the status in Catalyst Center Global Manager and perform actions through Catalyst Center.
Uninstalling applications	Displays the status in Catalyst Center Global Manager and perform actions through Catalyst Center.

Upgrade a Controller

Outlines how to upgrade an eligible controller immediately or schedule the upgrade for a maintenance window, with important considerations regarding controller availability during the process.

Catalyst Center Global Manager allows you to upgrade an eligible controller immediately or schedule the upgrade for a maintenance window.

Caution: An upgrade can make the Catalyst Center controller temporarily unavailable. Schedule upgrades during an approved maintenance window.

During the maintenance window, the controller may temporarily become unreachable. It becomes reachable again near the end of the upgrade process, while Catalyst Center Global Manager continues to display its status.

When a controller has the **Upgrade available** status, you can download and upgrade a release in one workflow, or download a release without upgrading. When you choose **Download** only, it will show list of available releases to choose the latest release and proceed the download workflow.

Upgrade a controller immediately

Provides instructions for immediately upgrading a controller, including selecting an eligible device, scheduling the upgrade, viewing upgrade details, and monitoring progress through the **Controller Upgrades** page.

Use this task to upgrade a controller immediately.

Procedure

1. Locate an eligible controller with the **Upgrade available** or **Ready for upgrade** status.

   Ready for upgrade refers to the already downloaded release, which may not be the latest available release.

2. From the **Actions** menu, choose **Schedule** upgrade.

   The **Controller Upgrades** window appears with these details:

   - Controller name
   - Installed version
   - Target version
   - Notes about maintenance warning

3. Select the **Now** radio button for immediate upgrade.
4. Click **Upgrade**.

Catalyst Center Global Manager starts the upgrade workflow. Refresh the **Controller Upgrades** page to view the current status and progress.

If you start an upgrade when a release is not already downloaded, Catalyst Center Global Manager downloads the selected release before starting the upgrade.

Upgrade a controller on schedule

Shows you how to schedule a controller upgrade by selecting an eligible controller, reviewing upgrade details, setting the upgrade time, meeting scheduling requirements, and submitting the schedule.

Use this task to upgrade a controller on schedule.

Procedure

1. Locate an eligible controller with the **Upgrade available** or **Ready for upgrade** status.
2. From the **Actions** menu, choose **Schedule** upgrade.

   The **Controller Upgrades** window appears with these details:

   - Controller name
   - Installed version
   - Target version
   - Notes about maintenance warning

3. Select the **Scheduled** radio button for any scheduled upgrade.
   a) Specify the upgrade date and time.

      Catalyst Center Global Manager displays the time in your browser local time and sends the schedule to the controller in UTC.

      Ensure that the scheduled time meets the following requirements:

      - Is exactly 3 hours ahead.
      - Is within 30 days of the current date.

- Review the maintenance information.

4. Click **Schedule**.

When you schedule an upgrade for a controller with the **Upgrade available** status, Catalyst Center Global Manager starts the release download immediately and starts the upgrade at the scheduled time.

Pre-upgrade checks

Outlines the pre-upgrade check process as part of the upgrade workflow.

When you start an upgrade, the controller runs pre-upgrade checks as part of the upgrade workflow. If a pre-upgrade check fails, Catalyst Center Global Manager marks the workflow as failed and displays the available failure information.

Correct the issue and select **Retry upgrade** when the option is available.

> **Note**
>
> Catalyst Center Global Manager does not support running a pre-upgrade check independently before you start the upgrade workflow.

Cancel or delete a downloaded release

Shows you how to cancel an active release download when the controller status is in **Downloading** state and the controller supports cancellation.

Use this task to cancel or delete a downloaded release.

Procedure

1. Locate an eligible controller with the **Upgrade scheduled** or **Ready for upgrade** status.
2. From the **Actions** menu, choose **Delete download**.

   The **Cancel download** action is shown only for controllers in the **Downloading** state.

   While Catalyst Center Global Manager processes the cancellation request, the controller status is **Canceling download**. No upgrade actions are available until the operation completes.

Edit or delete an upgrade schedule

Shows you how to modify or remove an upgrade schedule when the controller status is **Upgrade scheduled**.

Use this task to edit or delete an upgrade schedule.

Procedure

1. Locate the controller with the **Upgrade scheduled**.
2. From the **Actions** menu, choose one of these options:
   - Edit schedule–Changes the scheduled upgrade date or time.

- Delete schedule—Cancels the scheduled upgrade.

3. Confirm the action.

Monitor download or upgrade progress

Shows you how to monitor download or upgrade progress.

Cisco Catalyst Center Global Manager displays the current upgrade progress or the latest upgrade activity and lets you monitor the release download.

Select a controller to view the current or latest upgrade activity.

Catalyst Center Global Manager can display these upgrade information:

- Download or upgrade status
- Progress percentage
- Workflow steps
- Start and end times
- Workflow duration
- Error and failure details

During an upgrade, the controller can become temporarily unreachable while controller services restart. Catalyst Center Global Manager retains the controller in the **Controller Upgrade** table and displays the latest available status and error information.

Handle upgrade failures

Guides you through handling upgrade failures by viewing workflow details and error information.

When a download or upgrade fails, select the controller to view the workflow details and error information.

The action that Catalyst Center Global Manager provides depends on the controller status and controller support. If the controller state changes after Catalyst Center Global Manager displays the page and the controller does not accept the requested action, Catalyst Center Global Manager displays the controller error message.

Controllers that are unreachable or return an API error remain in the table with a **Loading error** status with appropriate error message in the tool tip, or click **Loading error** in the upper-right corner to view the affected controllers.

Controller certificates

Explains how controller certificates in Catalyst Center Global Manager centralize monitoring and management of security certificates across enrolled controllers.

A controller certificate is a security credential that

- enables centralized visibility and monitoring of certificate status across multiple Catalyst Center controller clusters,
- supports tracking and proactive management for both system and trusted (Cisco Trusted External Root Bundle) certificates, and
- allows integrated remediation actions such as certificate replacement or updates directly through cross-launch to the Catalyst Center.

Controller Certificates in Catalyst Center Global Manager provide a centralized dashboard for monitoring the security and validity of certificates for all enrolled Catalyst Center controllers. You can review **Trusted** (Cisco Trusted External Root Bundle and Third party) status and **System certificate integrity** for all controllers in one location. You can reduce operational effort and ensure uninterrupted service with this approach.

Key capabilities:

- Centralized visibility: Monitor certificate status (valid, expiring, or expired) across multiple controller clusters.
- System and trusted certificate management: Track system certificates (required for cluster management and operations) and manage trusted third-party certificates.
- Integrated remediation: Use deep links to launch directly into the appropriate controller interface to take actions such as replacing or updating certificates.
- Overview card: The **Overview** page includes a **Controller Certificates** card that displays the **Expired** and **Expiring** counts. Select the card to open the **Controller Certificates** page.

Certificate categories

Describes the main categories of certificates, including their purposes and how they support security architecture.

A certificate category is a grouping of digital certificates that

- defines the purpose and scope for certificate usage in a system,
- determines how certificates are managed and validated, and
- influences security controls, trust relationships, and operational continuity.

You can group certificates into two main categories.

- **System certificates**: used for internal cluster operations, backend communications, disaster recovery, and integrations such as RADIUS or TACACS+. If your cluster's system certificate expires, you cannot manage the cluster.
- **Trusted certificates**: include third-party and certificate authority trust stores. These maintain a uniform trust chain across the global estate and prevent trust-chain drift between regions. Cisco-trusted certificates are excluded to focus on user-managed security.

Cisco Trusted External Root Bundle

Cisco Catalyst Center stores and updates the **Cisco Trusted External Root Bundle** (`ios.p7b`) from the Cisco PKI website. The bundle enables supported Cisco networking devices to authenticate the controller and applications such as Network Plug and Play when they present valid third-party vendor certificates. Catalyst Center includes a preinstalled **Cisco Trusted External Root Bundle**.

Certificate statuses

This section explains the different certificate statuses used to indicate certificate validity and expiration.

Certificates are grouped by status:

- **Expired** – the certificate has expired and is no longer valid.
- **Expiring** – the certificate is approaching its expiration date.

  Certificates are labeled **Expiring** when the threshold is less than 90 to 100 days remaining. The threshold varies by Catalyst Center platform version.
- **Valid** – the certificate is currently valid.

Monitor system certificates

Monitor the status of system controller certificates to ensure secure and uninterrupted operation of your Catalyst Center.

Identify expired or expiring certificates so that you can proactively manage renewals and maintain security compliance.

Use the page to monitor the health and status of certificates across your controllers. You can identify expired or expiring certificates, view third-party trusted certificates, and troubleshoot connectivity issues.

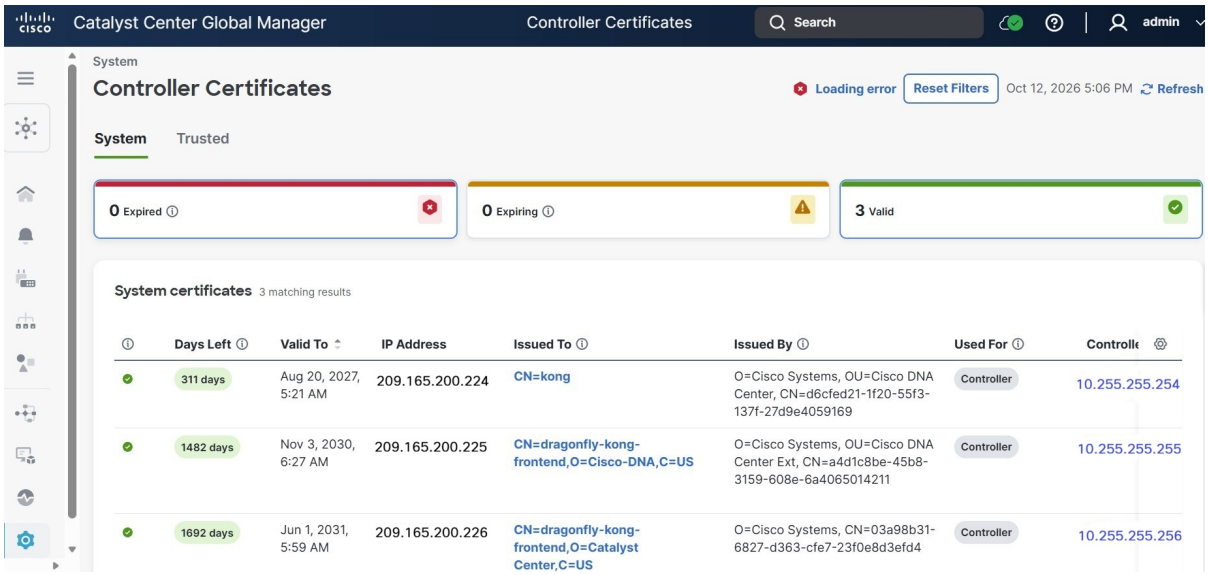
Before you begin

Ensure you have administrative privileges for viewing and managing system certificates.

Procedure

1. From the Catalyst Center Global Manager **Overview** page, select the **Controller Certificates** card, or choose **System** > **Controller Certificates** from the main menu to view the **Controller Certificate** dashboard.

   Figure 1: Controller Certificates Dashboard



2. Click the **System** tab to view system controller certificates.

   If one controller fails, data from other controllers can remain available. If a system certificate prevents a controller from communicating with Catalyst Center Global Manager, you may not see that controller in the certificate table. To review reported connectivity issues, click **Loading errors**.

3. Review the summary to quickly identify the state of your certificates:
   - **Status cards**: Select a status card (Expired, Expiring, or Valid) to filter the list of controllers.
   - **Reset filters**: Click **Reset Filters** to clear all active filters and display the full list of controller certificates.
   - **Loading errors**: Click **Loading error** to view details regarding controllers that failed to load.

4. In the **System** certificates table, review details for each certificate.
   - **Days Left**: Days until expiration.
   - **Valid To**: The certificate expiration date and time.
   - **Controller**: Corresponding controller IP address.

- **Issued To/By**: The entity to which the certificate was issued. The value must contain the FQDN or IP address that belongs to the server.
- **Certificate Serial Number**: Identifier for the certificate.

> **Note**
>
> You can edit the table settings. You can decide what to display or hide by adjusting the table settings for the Controller Certificates page. Click the gear icon in the table header. The **Table Settings** window appears. You can check or uncheck the items under **Table Density** and **Table Columns** as needed, then click Apply.

5. If you notice outdated data on the dashboard, click **Refresh** to update the data.

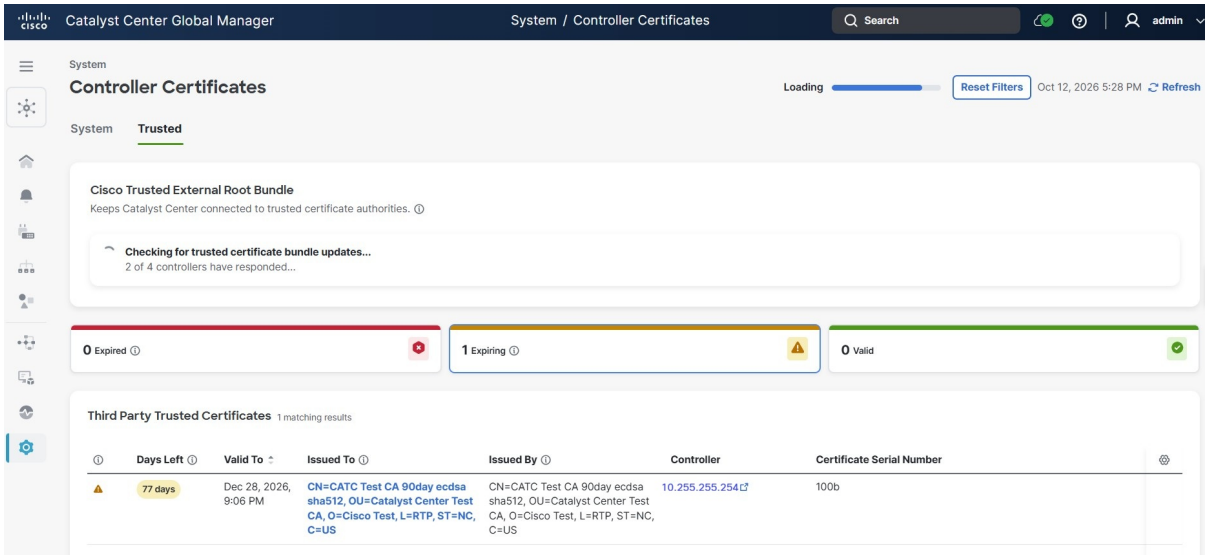
Monitor trusted certificates

Monitor the status of third-party controller certificates to ensure secure and uninterrupted operation of your Catalyst Center instances.

Procedure

1. From the Catalyst Center Global Manager **Overview** page, select the **Controller Certificates** card, or choose **System** > **Controller Certificates** from the main menu to view the **Controller Certificate** dashboard.

Figure 2: Trusted controller certificate



2. Click the **Trusted** tab to view certificates from connected third-party authorities.

   Review the **Cisco Trusted External Root Bundle** status for each controller. The status identifies controllers that require an update and controllers for which the bundle is up to date.

3. If you detect a connectivity failure notification, click **Review failures** and resolve any reported issues.
4. Review the summary to quickly identify the state of your certificates:
   - **Status cards**: Select a status card (Expired, Expiring, or Valid) to filter the list of controllers.

- **Reset filters**: Click **Reset Filters** to clear all active filters and display the full list of controller certificates.
- **Loading errors**: Click **Loading error** to view details regarding controllers that failed to load.

5. In the **Third Party Trusted Certificates** table, review details for each trusted certificate:
   - **Days Left**: The number of days remaining until the certificate expires.
   - **Valid To**: The certificate expiration date and time.
   - **Controller**: Shows the IP address associated with the controller.
   - **Issued To/By**: The entity to which the certificate was issued. It must contain the FQDN or IP address of the server.
   - **Certificate Serial Number**: Shows the identifier for the certificate.

> **Note**
>
> You can modify the table settings for the **Controller Certificates** page. Click the gear icon in the table header to open the **Table Settings** window. In **Table Settings**, check or uncheck the items under **Table Density** and **Table Columns** as needed, then click **Apply**.

6. If the dashboard data appears outdated, click **Refresh** to update the data.

Global search

Describes the global search box on the Catalyst Center Global Manager home page, supporting searches by MAC address, platform, software version, and IP address for devices, endpoints, applications, sites, and users, with cross-launch to detailed views.

The global search box is available on 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 to search across the controllers.

You do not 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. Press the **Return** or **Enter** key to initiate the search, because the autosearch feature is not supported. 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

Explains support for triggering notifications for events, with supported channels including EMAIL, PAGERDUTY, REST, SNMP, SYSLOG, and WEBEX.

Catalyst Center Global Manager provides support to trigger notifications when certain events occur. You can choose 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.

Platform

Introduces the extensible platform for creating value-added applications, leveraging Intent APIs for policy-based abstraction, Integration Flows for data center operations, and Events and Notifications Services.

Catalyst Center Global Manager provides an extensible platform that Cisco customers and partners can use to create value-added applications that can be built on top of its native capabilities. You can leverage the platform features to enhance the overall network experience by optimizing end-to-end IT processes, reducing the Total Cost of Ownership (TCO), and developing new value networks:

- Intent APIs: The Intent APIs are northbound REST APIs that expose specific capabilities of Catalyst Center Global Manager platform. The Intent APIs provide policy-based abstraction of business intent, allowing you to focus on an outcome to achieve instead of struggling with the mechanisms that implement that outcome. The APIs conform to the REST API architectural style. The APIs are simple, extensible, secure to use, and support the standard REST methods, which include the GET, POST, PUT, and DELETE operations through HTTPS.
- Integration Flows: Integration capabilities are part of westbound interfaces. To meet the need to scale and accelerate operations in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs.
- Events and Notifications Services: Supported services are available for Catalyst Center Global Manager events.

Overview

Describes the Platform Overview window, accessible to SUPER-ADMIN-ROLE users, displaying summaries and links to Bundles and Developer Toolkit, and platform notifications.

To access the **Platform** window, navigate to the Catalyst Center Global Manager dashboard and click **Platform** > **Overview**.

The platform **Overview** window supports these features:

- Displays brief summaries and direct links to the Catalyst Center Global Manager platform GUI features, including:
  - **Bundles**: Provides access to bundles that you can use to integrate your own applications to Catalyst Center Global Manager with or to enhance the performance of Catalyst Center Global Manager itself. Bundles are defined as groupings of APIs, events, integration flows, data services, or applications. Additionally, provides access to a GUI (**Configurations**) where you can configure general or event global settings or settings for multiple bundles.
  - **Developer Toolkit**: Provides tools (APIs and integration flows) for accessing Catalyst Center Global Manager and integrating Catalyst Center Global Manager with other applications.
- Accesses the **Notifications** slide-in pane that presents any current Catalyst Center Global Manager platform notifications, including bundle updates. Click **View Details** to view detailed data about the bundle under the **Bundles** tab. Click **Dismiss** to dismiss the bundle notification.

Manage

Explains the Platform Manage window, providing access to Bundles for integrating applications or enhancing performance, showing bundle status (NEW, ENABLED, DISABLED, ACTIVE, UPDATE, ERROR).

The Catalyst Center Global Manager platform **Manage** window provides access to these features:

To access the **Manage** window, navigate to the Catalyst Center Global Manager dashboard and click **Platform** > **Manage**.

- **Bundles**: Access to bundles that you can use to integrate Catalyst Center Global Manager with your own applications or to enhance the performance of Catalyst Center Global Manager itself. Bundles are comprised of groupings of APIs, events, data services, or applications.

Bundles

Describes bundles as groupings of APIs, events, data services, or applications, and their various statuses (NEW, ENABLED, DISABLED, ACTIVE, UPDATE, ERROR) for integration and performance enhancement.

Catalyst Center Global Manager platform provides access to bundles that you can use to integrate Catalyst Center Global Manager with your own applications or to enhance the performance of Catalyst Center Global Manager itself.

This Catalyst Center Global Manager platform information is accessible using the GUI:

- Bundle name, vendor, version, version release date, tags, and description.
- Status of the bundle:
  - **NEW**: Bundle that is available through Catalyst Center Global Manager platform, but has not yet been enabled. Click **Enable** to enable the bundle for configuration and subsequent activation.
  - **ENABLED**: Bundle that has been enabled, but not yet configured. Once enabled, the bundle's API code can be viewed under the **Contents** tab. Click **Configure** to configure at the bundle level.

    The enablement and configuration of bundles are two separate steps, because a business manager will usually enable a particular bundle as a business decision. The follow-up configuration of the bundle will usually be performed by an IT or network administrator.

- **DISABLED**: The bundle has been stopped from executing any further.
- **ACTIVE**: After either reviewing and/or configuring the bundle (configuring bundle-specific values), you can activate the bundle in your network by clicking **Activate**.
- **UPDATE**: When you upgrade from one version of Catalyst Center Global Manager platform to a later version of Catalyst Center Global Manager platform.
- **ERROR**: There is an issue with the bundle and it cannot be activated within your network.

Developer toolkit

Outlines the software developer tools provided, including APIs organized by functionality (Authentication, Event Management, Know Your Network, Site Management, System) and Event Notifications for subscribing to network events.

The Catalyst Center Global Manager platform provides you with these software developer tools to access and program with Catalyst Center Global Manager, as well as to integrate Catalyst Center Global Manager with other applications:

- **APIs**: Available APIs organized within categories by functionality (for example, **Operational Tasks** or **Site Management** APIs).
- **Event Notifications**: Lets you view and subscribe to specific events that may occur in your network.

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 the **Swagger docs** from the **APIs** GUI.

Activities

Explains the Activities page for viewing audit log details of Catalyst Center Global Manager, capturing user actions, system changes, and controller operations, with filtering options by period and severity.

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 these details:

- Created date and time
- Description
- Category
- Severity

- User

Note

- You can refine the search summary for these 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 these 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

Introduces the System page for viewing basic details of Catalyst Center Global Manager, including System 360, Software Management, and Backup & Restore information.

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

Use System 360

Explains how to access System 360 from the Controllers page to view detailed information about app stacks and services running on a selected Catalyst Center, including node and service status, with tools for monitoring (Grafana) and logging (Kibana).

The **System 360** tab provides at-a-glance information about Catalyst Center Global Manager.

Procedure

1. From the main menu, choose **System** > **System 360**.
2. On the **System 360** dashboard, review these displayed data metrics:

   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.

   Cluster

   - **Hosts**: Displays information about the Catalyst Center Global Manager hosts. The displayed information includes the hosts IP addresses and detailed data about the services running on the host. Click the **View Services** link to view detailed data about the services running on the hosts.

     > **Note**
     >
     > The host IP address has a color badge next to it. A green badge indicates that the host is healthy. A red badge indicates that the host is unhealthy.

     The side panel displays these information:

     - **Node Status**: Displays the health status of the node.

       If the node health is unhealthy, hover over the status to view additional information for troubleshooting.

     - **Services Status**: Displays the health status of the services. Even if one service is down, the status is **Unhealthy**.
     - **Name**: Service name.
     - **Appstack**: App stack name.

       An app stack is a loosely coupled collection of services. In this environment, a service is a horizontally scalable application that adds instances when demand increases and removes instances when demand decreases.

     - **Health**: Status of the service.
     - **Version**: Version of the service.
     - **Tools**: Displays metrics and logs for the service. Click the **Metrics** link to view service monitoring data in Grafana. Grafana is an open-source metric analytics and visualization suite. You can troubleshoot issues by reviewing the service monitoring data. For information about Grafana, see https://grafana.com/. Click the **Logs** link to view service logs in Kibana. Kibana is an open-source analytics and visualization platform. You can troubleshoot issues by reviewing the service logs. For information about Kibana, see https://www.elastic.co/products/kibana.

   - **Cluster Tools**: Lets you access only the monitoring tool.
     - **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. For information about Grafana, see https://grafana.com/.

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

System Management

- **Software Management**: Displays the status of application or system updates.

  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 & Restore**: Displays the status of the most recent backup. Catalyst Center Global Manager supports configuring backups using Network File System (NFS), physical disk, or SSH (Remote Server) as backup storage options within the backup configuration settings. It schedules a backup with 2 options: **Now** or **Daily**.

  > **Note**
  >
  > A backup has a color badge next to it. A green badge indicates a successful backup with a timestamp. A yellow badge indicates that the next backup is not yet scheduled.

  Click **Configure Settings** to configure backup settings, including adding or updating NFS configurations for storing backups. Additionally, you can restore the system using these backups through the interface.

3. Click **System Health** to view 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

Explains how clicking Software Management in the Controller Details window cross-launches to the corresponding controller page to view installed applications or system updates.

The Catalyst Center Global Manager provides many of its functions as individual applications, packaged separately from the core infrastructure. This enables you to view installed applications or system updates and uninstall those you are not using, depending on your preferences.

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

Some applications are basic that they are required on nearly every Catalyst Center Global Manager deployment.

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

The **Software Management** page provides you a view of these details.

- **Installed applications**

  To view the description of a package, click the **View Installed Applications** and place your cursor over its name.

- **Upgrade summary report**

  Click the **View Upgrade Summary** to view the results of the latest upgrade of Catalyst Center Global Manager and its applications. This report allows you to:

  - Identify the current and previous Catalyst Center Global Manager version that was installed on your appliance.
  - Determine when the upgrade took place.
  - In the **Activity** tab, view the application packages that were upgraded and their current version number.
  - In the **Timeline** tab, see whether the post-upgrade checks performed by Catalyst Center Global Manager were completed successfully.

- **Release activities**

  Click the **View Release Activities** to view all installed applications that are in progress, success, or failed state.

About backup and restore

Explains the backup and restore functions for Catalyst Center Global Manager data, including enrolled controllers, users, roles, situational dashboards, and system settings, emphasizing the importance of not modifying backup files.

The backup and restore functions enable you to create backup files and restore them on a different appliance if necessary for your network configuration.

Backup

- You can back up Catalyst Center Global Manager data only.
- Catalyst Center Global Manager backup consists of database backups which includes:
  - All the enrolled controllers
  - Users and roles
  - Situational dashboards created by the users
  - All the system settings saved by the users
  - Device health export file
- **Important**

  Do not modify or delete the backup files. If you do, you might not be able to restore the backup files to Catalyst Center Global Manager.

- Catalyst Center Global Manager creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see Backup server requirements.
- Only a single backup can be performed at a time. Performing multiple backups at once is not supported.
- When a backup is being performed, you cannot delete the files that have been uploaded to the file service, and changes that you make to these files might not be captured by the backup process.
- Options available are:
  - Perform a daily backup to maintain a current version of your database and files.

  - Perform a backup after making changes to your configuration. For example, when changing or creating a new policy on a device.
  - Perform a backup only during a low-impact or maintenance period.
- You can schedule weekly backups on a specific day of the week and time.

Restore

- You can restore the backup files from the remote server using Catalyst Center Global Manager.
- When you restore the backup files, Catalyst Center Global Manager removes and replaces the existing database and files with the backup database and files. While a restore is being performed, Catalyst Center Global Manager is unavailable.
- You can restore a backup to a Catalyst Center Global Manager with a different IP address. This situation could happen if the IP address is changed on Catalyst Center Global Manager and you need to restore from an older system.

Backup server requirements

Details the operating system, SSH/rsync, Linux rsync utility, C.UTF-8 locale, destination folder permissions, SFTP subsystem, and multiple Catalyst Center Global Manager deployment requirements for the backup server.

The backup server must run one of the supported operating systems:

- Red Hat Enterprise 8 or later
- Ubuntu 16.04 (or Mint, etc) or later

Server requirements for data backup

To support data backups, the server must meet these requirements:

- Must use SSH (port22)/remote sync (rsync). Catalyst Center Global Manager does not support using FTP (port 21) when performing a backup.
- The Linux rsync utility must be installed.
- The C.UTF-8 locale must be installed. To confirm whether C.UTF-8 is installed, enter:

```
# localectl  list-locales | grep -i c.utf
C.utf8
en_SC.utf8
```

- The backup user must own the destination folder for the backup or have read-write permissions for the user's group. For example, assuming the backup user is *backup* and the user's group is *staff*, this sample outputs show the required permissions for the backup directory:
  - Example 1: Backup directory is owned by *backup* user:

```
$ ls -l /srv/
drwxr-xr-x  4 backup     root  4096 Apr 10 15:57 acme
```

  - Example 2: *backup* user's group has required permissions:

```
$ ls -l /srv/
drwxrwxr-x. 7 root   staff  4096 Jul 24  2017 acme
```

- SFTP subsystem must be enabled. The SFTP subsystem path depends on which Ubuntu or Red Hat release is installed. For the latest release, these lines below must be uncommented and present in the SSHD configuration:
  - Ubuntu-based Linux: `Subsystem sftp /usr/lib/openssh/sftp-server`
  - Red Hat-based Linux: `Subsystem sftp /usr/libexec/openssh/sftp-server`

  The file where you need to uncomment the preceding line is usually located in `/etc/ssh/sshd_config`.

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

Requirements for multiple Catalyst Center Global Manager deployments

If your network includes multiple Catalyst Center Global Manager clusters, you cannot use the same backup location. For multiple Catalyst Center Global Manager deployments, the best practice is to separate the backup directory structure for each Catalyst Center Global Manager cluster. This example configuration shows how to separate your backup directory structure.

Resource	Example configuration
Catalyst Center Global Manager clusters	1. *cluster1* 2. *cluster2*
Backup server hosting backups	The example directory is `/data/`, which has ample space to host the Catalyst Center Global Manager backups.
Directory ownership and permissions	Earlier in this section, see "Server Requirements for Data Backup."
NFS export configuration	The content of the `/etc/exports` file: `/data/cluster1 *(rw,sync,no_subtree_check,all_squash)`

Backup storage requirements

Specifies the need for external NFS storage for backup copies, recommending a daily limit of 1 GB and a maximum retention capacity of 60 GB for disk backups.

Catalyst Center Global Manager stores backup copies of data on an external NFS device on an external target location. Refer to Backup to view the types of database backups.

You must allocate enough external storage for your backups to cover the required retention. We recommend that the daily NFS storage backup size be limited to a maximum of 1 GB, with a maximum retention capacity of 60 GB for disk backups.

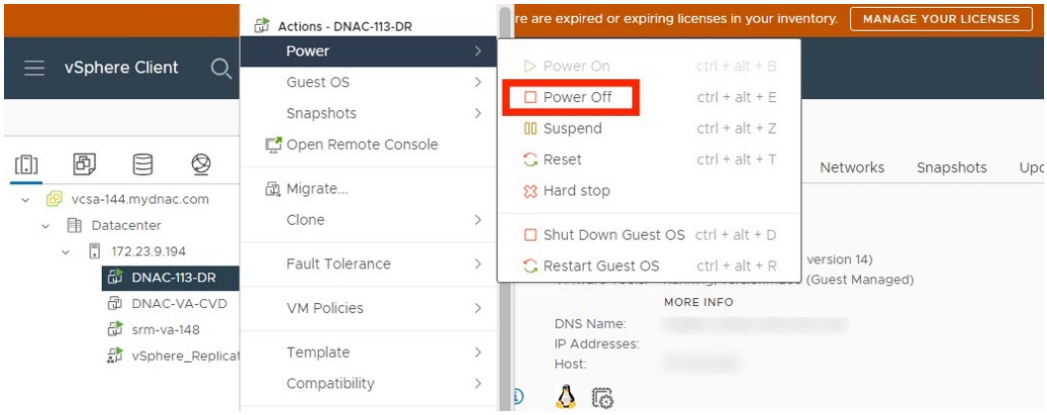
Add a physical disk for backup and restore

Provides a procedure for adding a physical disk to a VMware ESXi virtual machine to be used specifically for Catalyst Center Global Manager backup and restore operations.

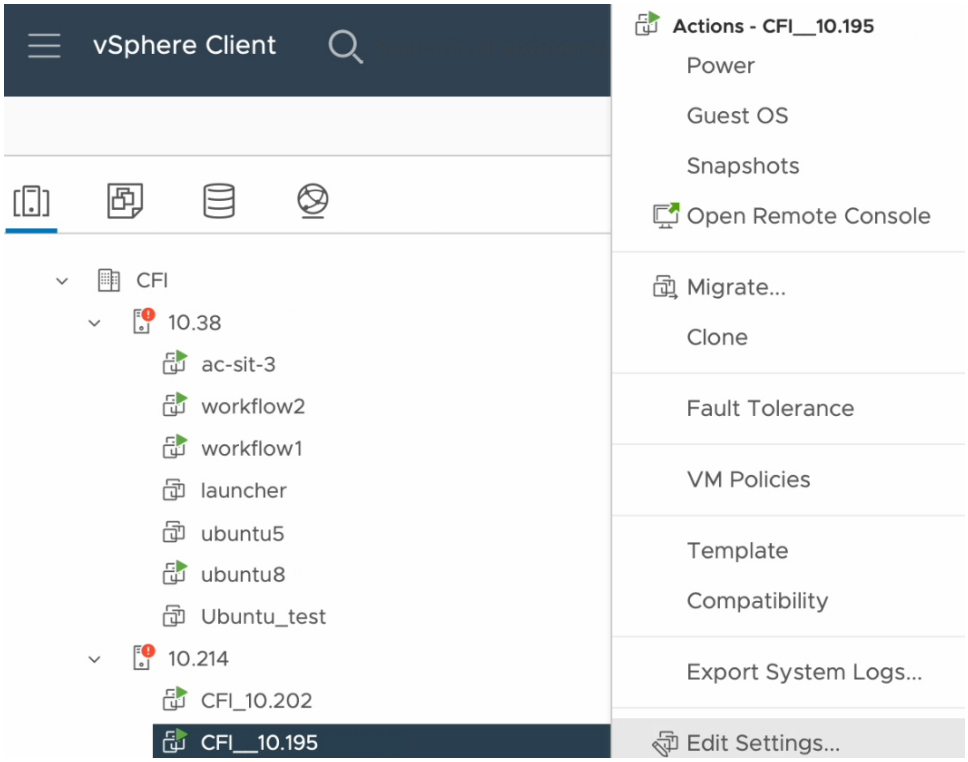
Use this procedure to add a physical disk that can be used for only Catalyst Center Global Manager on ESXi backup and restore operations.

Procedure

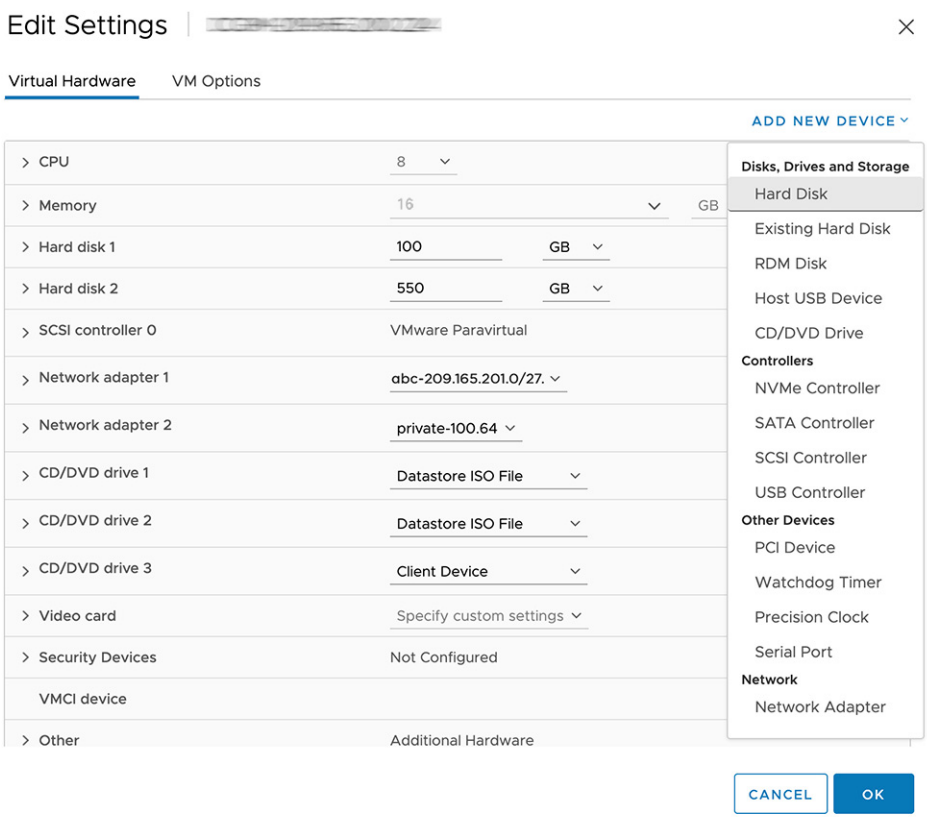
1. If your appliance is running on the machine that's hosting Catalyst Center Global Manager on ESXi, power off the appliance's virtual machine.



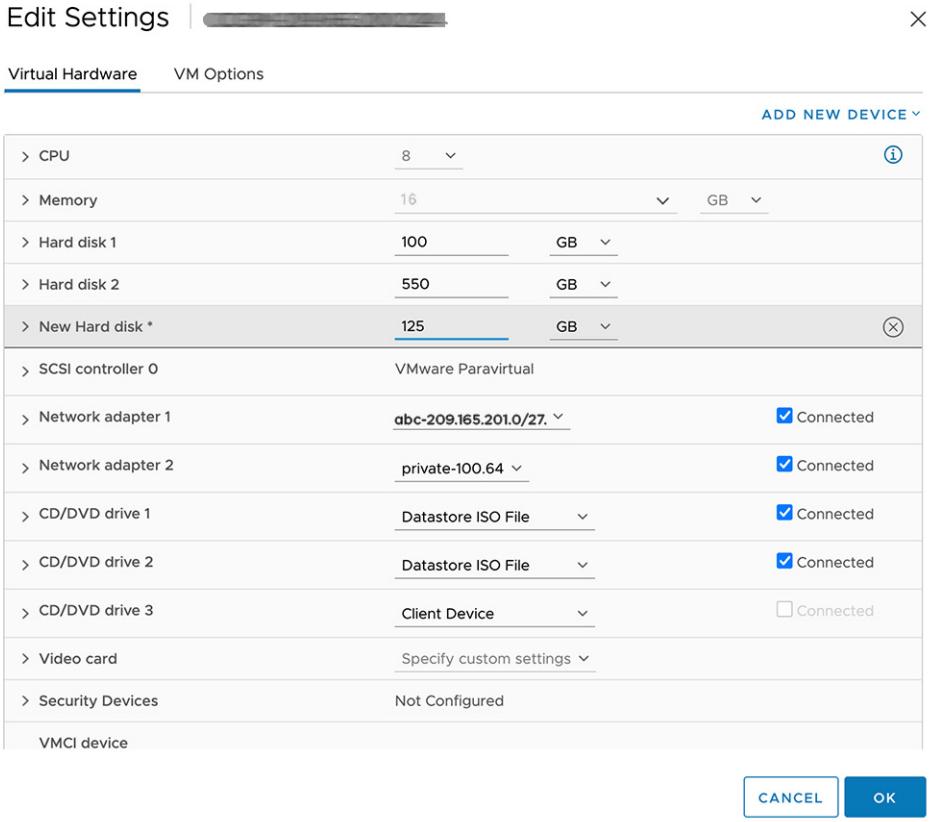
2. Log in to VMware vSphere.
3. From the vSphere client left pane, right-click the ESXi host and then choose **Edit Settings**.



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

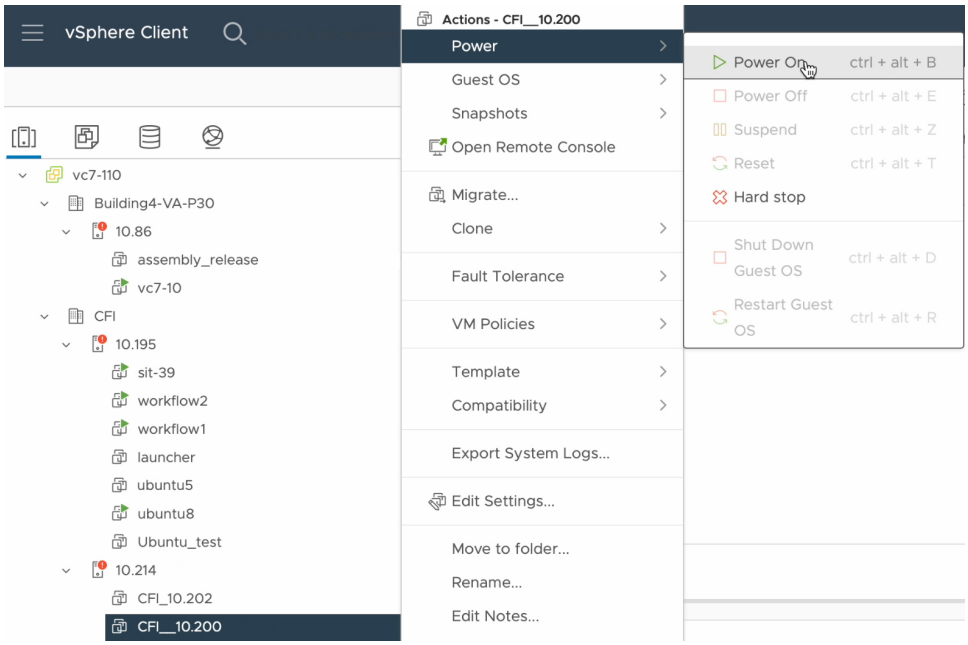


5. In the **New Hard disk** field, enter the desired storage size.



> **Note**
>
> For information on the recommended storage space for backup, see Backup storage requirements.

6. Click **OK**.
7. Power on the appliance's virtual machine.



What to do next

You can now configure the added physical disk for backup. For information on how to configure the physical disk, see Configure the location to store backup files.

Add the NFS server

Details the procedure for adding multiple Network File System (NFS) servers to Catalyst Center Global Manager for backup purposes, including server host, source path, NFS version, and port mapper.

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

Procedure

1. From the main menu, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

   Alternatively, choose **System** > **Backup and Restore** > **Configure Settings**.
2. Click **Add NFS**.
3. In the **Add NFS** slide-in pane, complete these steps:
   a) Enter the **Server Host** and **Source Path** in the respective fields.
   b) Choose **NFS Version** from the drop-down list.

c) The **Port** is added by default. You can leave the field empty.
d) (Optional) Enter the **Port Mapper** number.
e) Click **Save**.

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

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

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

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

What to do next

Configure the added NFS server for backup. For more information, see Configure the location to store backup files.

Add a remote SSH server

Add a remote SSH server for backups.

Use this procedure to configure a remote server for backups.

Procedure

1. From the main menu, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

   Alternatively, choose **System** > **Backup and Restore** > **Configure Settings**.

2. On the **Backup Configuration** page, select **SSH (Remote Server)**, and then click **Add SSH**.
3. In the **Add SSH** slide-in pane, enter the remote SSH server details, and then click **Save**.
   a) In the **SSH IP Address** field, enter the IP address of the server.
   b) In the **SSH Port** field, enter the SSH port number.
   c) In the **Username** field, enter the user name for the server.
   d) In the **Password** field, enter the password for the server.
   e) In the **Server Path** field, enter the backup directory path.
4. On the **Backup Configuration** page, click **View SSH List** to confirm the server is successfully added.

   The **SSH List** slide-in pane displays the added server and its details.

5. On the **Backup Configuration** page, configure the server path for backup storage:
   a) Click **Refresh**.
   b) From the **Server Path** drop-down list, choose the server path.
   c) Click **Submit**.

The remote SSH server is configured and available for backups.

Configure the location to store backup files

Guides users on configuring the storage location for backup files, offering options for physical disk or NFS server or SSH (Remote Server), and defining mount path, encryption passphrase, and backup retention.

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

Before you begin

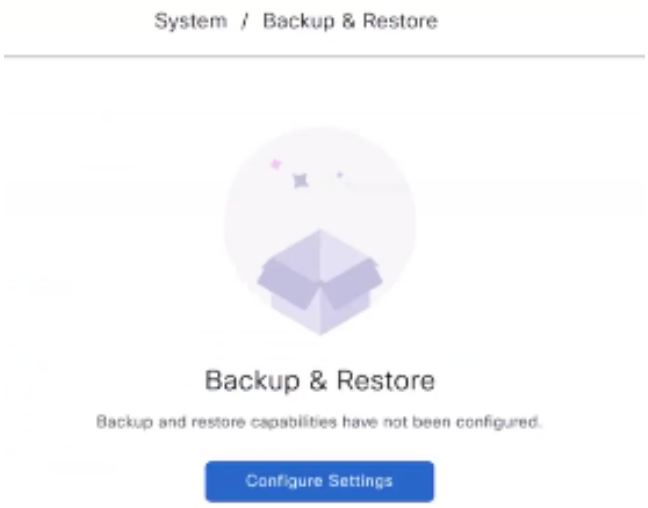
Make sure that these requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in Backup server requirements.

Procedure

1. From the main menu, choose **System** > **Backup and Restore**.

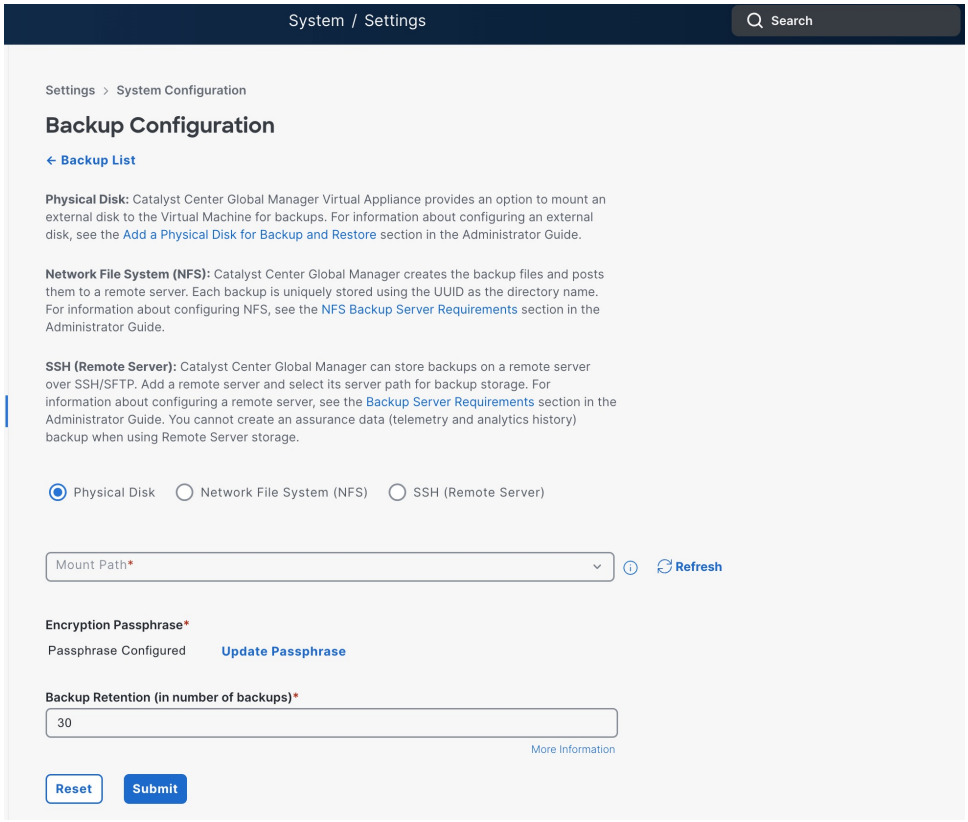
   You can view this window:



2. Click **Configure Settings**.

   Alternatively, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

3. Choose the **Physical Disk** or **NFS** server or **SSH (Remote Server)** option.



4. **Physical Disk**: Catalyst Center Global Manager provides an option to mount an external disk to the virtual machine, to store a backup copy of data. To configure a physical disk, click the **Physical Disk** radio button and define these settings:

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

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

5. **NFS**: Catalyst Center Global Manager creates the backup files and posts them to a remote NFS server. For information about the remote server requirements, see Backup server requirements. To configure an NFS backup server, click the **NFS** radio button and define these settings:

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

6. **SSH (Remote Server)**: Catalyst Center Global Manager can store backups on a remote server over SSH/SFTP. Add a remote server and select its server path for backup storage. For information about configuring a remote server, see the Backup server requirements. To configure the SSH backup server, click the **SSH (Remote Server)** radio button.
7. Click **Submit**.

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

Create a backup

Outlines the procedure for creating a backup of Catalyst Center Global Manager, including naming the backup, choosing a schedule type (now, daily, weekly), and monitoring its progress.

Use this procedure to create a backup of your Catalyst Center Global Manager.

Before you begin

You must configure the backup location. For more information, see Configure the location to store backup files.

Procedure

---

1. From the main menu, choose **System** > **Backup & Restore**.
2. Click **Schedule Backup**.

   The **Schedule Backup** slide-in pane opens.

   Complete these steps in the **Schedule Backup** slide-in pane:

   a. Enter a unique name for the backup.

   b. In the **Schedule Type** area, choose one of these options:

      - **Backup now**: To immediately create a backup.
      - **Schedule backup daily**: To schedule the backup on a daily basis.
      - **Schedule backup weekly**: To schedule the backup on a weekly basis.

   c. Click **Save**.

3. Catalyst Center Global Manager begins the backup process. An entry for the backup is added to the **Backup & Restore** window.

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

Schedule data backup

Explains how to schedule recurring backups for Catalyst Center Global Manager data, specifying the day of the week and time, and providing options to view, edit, or delete upcoming schedules.

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

Before you begin

Make sure that these requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in Backup server requirements.
- Backup servers have been configured in Catalyst Center. For more information, see Configure the location to store backup files.

Procedure

---

1. From the main menu, choose **System** > **Backup & Restore**.
   The **Backup & Restore** window is displayed.
2. Click **Schedule Backup**.

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

3. In the **Schedule Backup** slide-in pane, complete these steps:
   a. In the **Backup Name** field, enter a unique name for the backup.
   b. Choose a schedule option:
      - **Schedule backup daily**: To schedule a daily backup job, choose the time of day when you want the backup to occur.
      - **Schedule backup weekly**: To schedule a weekly backup job, choose the days of the week and time of day when you want the backup to occur.
   c. Click **Save**.

   The **Backup & Restore** window displays a banner message that shows the day and time for which the backup is scheduled.
4. Optional: Click **View Upcoming Backups** to make any changes to the upcoming schedules. If you don't want the backup to occur on a scheduled date and time, in the **Upcoming Schedules** slide-in pane, click the toggle button to disable a particular schedule.
5. Optional: Click **Edit Schedule** to edit the schedule.

6. Optional: Click **Delete Schedule** to delete the schedule.
7. After the backup starts, it appears in the **Backup & Restore** window. Click the backup name to view the lists of steps executed.

   Alternatively, you can click **View Activities** at the top left of the **Backup & Restore** window and click the **Execution ID**. The **Create Backup Details** slide-in pane opens and shows the list of steps executed.
8. In the **Backup & Restore** window, click the **In Progress**, **Success**, or **Failure** tab to filter the list of backups to show only those tasks with a status of In Progress, Success, or Failure.

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

   Note

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

Restore data from backups

Provides instructions for restoring backup data to Catalyst Center Global Manager, emphasizing that the process replaces existing data and requires the encryption passphrase, making the system unavailable during restoration.

Use this procedure to restore backup data from your Catalyst Center Global Manager.

Caution

The Catalyst Center Global Manager restore process restores only the database and files. The restore process does not reflect any changes made since the last backup. This mean that any changes made after the last backup, including adding or deleting controllers, may be lost.

Before you begin

Make sure that these requirements are met:

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

When you restore data, Catalyst Center Global Manager enters maintenance mode and is unavailable until the restore process completes. Make sure that you restore data at a time when Catalyst Center Global Manager can be unavailable.

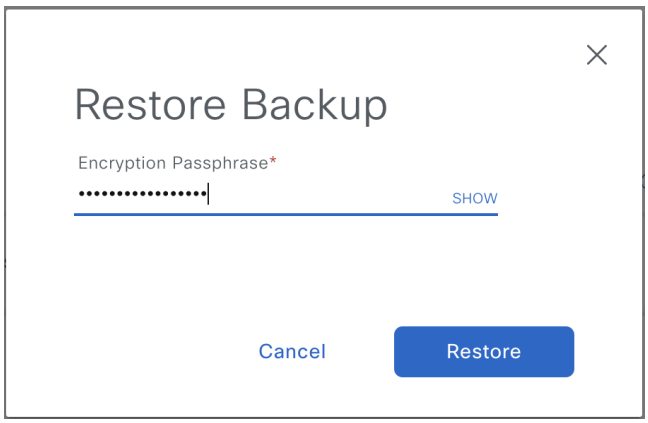
Procedure

---

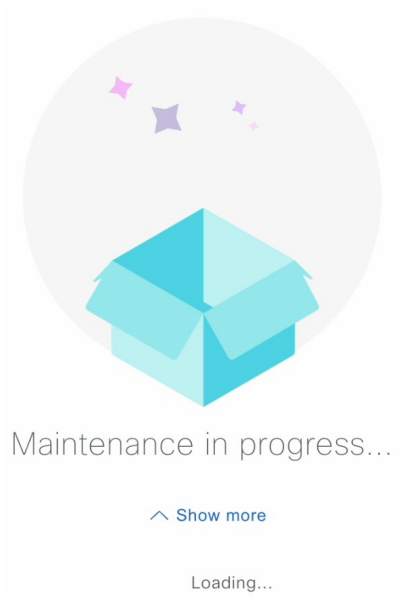
1. From the main menu, choose **System** > **Backup & Restore**.

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

2. In the **Backup Name** column, locate the backup that you want to restore.
3. In the **Actions** column, click the ellipsis and choose **Restore**.
4. In the **Restore Backup** dialog box, enter the **Encryption Passphrase** that you used while configuring the backup location and click **Restore**.



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



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

5. After the restore operation completes, click **Log In** to log back in to Catalyst Center Global Manager.
6. Enter the admin user's username and password, then click **Login**.

System settings

Describes the System Settings page, which allows configuration of certificates, external services (destinations, Cisco Catalyst Cloud), system configuration (health, proxy, debugging logs, backup, authentication API encryption, integration settings), login messages, terms and conditions, and trust and privacy settings.

To start using Catalyst Center Global Manager, you must first configure the system settings. This allows the server to communicate outside the network, ensures secure communications, authenticates users, and supports other key tasks. Use the procedures in this chapter to configure the system settings.

Note

- Any changes that you make to the Catalyst Center Global Manager configuration–including changes to the proxy server settings–must be done from the Catalyst Center Global Manager GUI.
- Any changes to your Catalyst Center Global Manager virtual appliance's configuration settings must be done with the `sudo maglev-config update` command. Run this command in a KVM console opened from Cisco IMC.
  - Change the **maglev** user password by specifying a new one in the **Linux Password** and **Re-enter Linux Password** fields. Leave these fields blank to continue using the current password.
  - You can make the other configuration setting changes without entering the **maglev** user password.
- By default, the Catalyst Center Global Manager system time zone is set to UTC. Do not change this time zone because the Catalyst Center Global Manager GUI works with your browser time zone.
- Restricted or secure shell is enabled for enhanced security. However, if you want to access the root shell using the `_shell` command, or use any of the restricted commands, you must contact Cisco TAC for assistance.

The Catalyst Center Global Manager **Settings** page 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.

    For more information on security best practices and managing certificates in Catalyst Center Global Manager, see Cisco Catalyst Center Security Best Practices Guide.

- **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.

    To configure REST Endpoint, email settings, syslog server, or SNMP trap server, go to the main menu, choose **System** > **Settings** > **External Services** > **Destinations**.
  - **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. After this, the Catalyst Center Global Manager will display the menus for controllers that are absent.

- **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 the Host Name or IP Address that will be used in the Integration Callback URLs.
- **Login Message**: shows a message for users when they log in.

- **Terms and Conditions**
  - **Product Offer**: 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 and roles

Explains how Catalyst Center Global Manager manages access using users, roles (super-admin, observer, network-admin), and access groups, detailing RBAC limitations and support for external authentication (AAA-RADIUS/TACACS or Cisco ISE).

The Catalyst Center Global Manager uses both users and roles to manage access. Each user is assigned roles to access controller functionality.

- **User Management**: The Catalyst Center Global Manager uses users, roles and access groups to manage access. A user is mapped to an access group to determine the scope and permission(s).
- **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.

  > **Note**
  >
  > If external authentication is enabled on a specific Catalyst Center and it is integrated with Catalyst Center Global Manager, data specific to this controller is not fetched if the user has not logged in at least once using their external authentication credentials. Consequently, any cross-launch to that Catalyst Center fails. Users must log in to Catalyst Center at least once before they can view any controller-specific data in Catalyst Center Global Manager or perform a cross-launch to that Catalyst Center.