Cisco Catalyst Center Administrator Guide, Release 3.1.3

First Published: 2025-06-16

Last Modified: 2025-07-15

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

CONTENTS

CHAPTER 3

CHAPTER 4

CHAPTER 1

New and Changed Information

New and changed information

This table summarizes the new and changed features in Catalyst Center 3.1.3 and tells you where they are documented.

Table 1: New and changed features in Catalyst Center 3.1.3

Feature	Description
Site-based, role-based access control	Catalyst Center supports site-based, role-based access control (SRBAC), which enables you to create an access group that limits access to certain network sites. Access group is a combination of the role and site. See Configure site-based, role-based access control, on page 134, and Impact of SRBAC on Catalyst Center features, on page 138.

CHAPTER 2

Configure System Settings

About system settings

To start using Catalyst Center, you must first configure the system settings so that the server can communicate outside the network, ensure secure communications, authenticate users, and perform other key tasks. Use the procedures described in this chapter to configure the system settings.

Note

- Any changes that you make to the Catalyst Center configuration—including changes to the proxy server settings—must be done from the Catalyst Center GUI.
- Any changes to your Catalyst Center 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.

  In Catalyst Center 2.3.7.7 onwards:

  - 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 system time zone is set to UTC. Do not change this time zone in settings because the Catalyst Center GUI works with your browser time zone.
- 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.

User profile roles and permissions

Catalyst Center supports role-based access control (RBAC). Your permissions are defined by your user role. Catalyst Center has three main default user roles:

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE, and
- OBSERVER-ROLE.

The SUPER-ADMIN-ROLE allows comprehensive access and supports creating and assigning custom roles in the Catalyst Center GUI. The NETWORK-ADMIN-ROLE and the OBSERVER-ROLE provide limited access.

You can create access groups that limits access to certain network sites. Access group is a combination of the role and site. At any point, you can log in to one specific access group.

Catalyst Center supports these default access groups:

- **NW-ADMIN_Global** - Access group for global access to the role NW-ADMIN
- **OBSERVER_Global** - Access group for global access to the role OBSERVER, and
- **SUPER-ADMIN_Global** - Access group for global access to the role SUPER-ADMIN.

The behavior of Catalyst Center features depends on the user role and site specified in the access group. For more information, see *Configure site-based, role-based access control* in the *Cisco Catalyst Center Administrator Guide*.

Use System 360

The **System 360** tab provides at-a-glance information about Catalyst Center.

Procedure

Step 1 From the main menu, choose **System** > **System 360**.

Step 2 On the **System 360** dashboard, review the following displayed data metrics:

Cluster

- **Hosts**: Displays information about the Catalyst Center hosts. The information that is displayed includes the IP address of the hosts and detailed data about the services running on the hosts. Click the **View Services** link to view detailed data about the services running on the hosts.

  Note
  The host IP address has a color badge next to it. A green badge indicates that the host is healthy. A red badge indicates that the host is unhealthy.

  The side panel displays the following information:

  - **Node Status**: Displays the health status of the node.

  If the node health is unhealthy, hover 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. A service in this environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.
  - **Health**: Status of the service.
  - **Version**: Version of the service.
  - **Tools**: Displays metrics and logs for the service. Click the **Metrics** link to view service monitoring data in Grafana. Grafana is an open-source metric analytics and visualization suite. You can troubleshoot issues by reviewing the service monitoring data. For information about Grafana, see https://grafana.com/. Click the **Logs** link to view service logs in Kibana. Kibana is an open-source analytics and visualization platform. You can troubleshoot issues by reviewing the service logs. For information about Kibana, see https://www.elastic.co/products/kibana.
  - **Actions**: Option available to restart the service. For some of the internal and system specific services, the **Actions** option is disabled.

- **High Availability**: Displays whether HA is enabled and active.

  For instructions on how to activate HA on your cluster, see Activate high availability, on page 82.

  Important

  Three or more hosts are required for HA to work in Catalyst Center.

  The three-node HA is not supported for Catalyst Center running on ESXi.

- **Cluster Tools**: Lets you access the following tools:
  - **Service Explorer**: Access the app stack and the associated services.
  - **Monitoring**: Access multiple dashboards of Catalyst Center components using Grafana, which is an open-source metric analytics and visualization suite. Use the **Monitoring** tool to review and analyze key Catalyst Center metrics, such as memory and CPU usage. For information about Grafana, see https://grafana.com/.

    Note

    In a multihost Catalyst Center environment, expect duplication in the Grafana data due to the multiple hosts.
  - **Log Explorer**: Access Catalyst Center activity and system logs using Kibana. Kibana is an open-source analytics and visualization platform designed to work with Elasticsearch. Use the **Log Explorer** tool to review detailed activity and system logs. In the Kibana left navigation pane, click **Dashboard**. Then, click **System Overview** and view all of the system logs. For information about Kibana, see https://www.elastic.co/products/kibana.

    Note

    All logging in Catalyst Center is enabled, by default.

System Management

- **Software Updates**: Displays the status of application or system updates. Click the **View** link 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.

- **Backups**: Displays the status of the most recent backup. Click the **View** link to view all backup details.

  Additionally, it displays the status of the next scheduled backup (or indicates that no backup is scheduled).

  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.

- **Application Health**: Displays the health of automation and Assurance.

  Note
  Application health has a color badge next to it. A green badge indicates a healthy application. A red badge indicates that the application is unhealthy. Click the **View** link to troubleshoot.

Externally Connected Systems

Displays information about external network services used by Catalyst Center.

- **Identity Services Engine (ISE)**: Displays Cisco ISE configuration data, including the IP address and status of the primary and secondary Cisco ISE servers. Click the **Configure** link to configure Catalyst Center for integration with Cisco ISE.
- **IP Address Manager (IPAM)**: Displays IP address manager configuration data and the integration status. Click the **Configure** link to configure the IP Address Manager.

Step 3 Click **System Health** and review the topology of your Catalyst Center appliances and the external systems that are connected to your network.

For more information about the **System Health** window, see View the system topology, on page 19.

View the services in System 360

The **System 360** tab provides detailed information about the app stacks and services running on Catalyst Center. You can use this information to assist in troubleshooting issues with specific applications or services. For example, if you are having issues with Assurance, you can view monitoring data and logs for the NDP app stack and its component services.

Procedure

Step 1 From the main menu, choose **System** > **System 360**.

Step 2 In **System 360** window, click **Service Explorer** tab.

The node clusters and the associated services are displayed in a tree-like structure in a new browser window.

- Hover your cursor over the node to view the details like, serial number, product ID, and interface.
- The Services table shows all the services associated with the node. The managed services are marked as (M).
- In the Service table, click the global filter icon to filter services by app stack name, service health status (Up, Down, or In Progress), or managed services.
- Enter a service name in the Global Search field to find a service. Click the service name to view the service in its associated node.

Step 3 Click the service to launch the Service 360 view, which displays the following details:

- **Metrics**: Click the link to view the services monitoring data in Grafana.
- **Logs**: Click the link to view the service logs in Kibana.
- **Name**: Service name.
- **Appstack**: App stack name.
- **Version**: Version of the service.
- **Health**: Status of the service.
- **Required Healthy Instances**: Shows the number of healthy instances and indicates whether the service is managed.
- **Instances**: Click the instances to view details.

Step 4 Enter the service name in the Search field to search the services listed in the table.

Step 5 Click the filter icon in the services table to filter services based on app stack name, service status (Up, Down, or In Progress), or managed service.

Monitor system health

From the **System Health** page, you can monitor the health of the physical components on your Catalyst Center appliances and keep tabs on any issues that may occur. Refer to the included topics, which describe how to enable this functionality and use it in your production environment.

Establish Cisco IMC connectivity

To enable the **System Health** page, you must establish connectivity with Cisco Integrated Management Controller (Cisco IMC), which collects health information for your appliances' hardware. Complete this procedure.

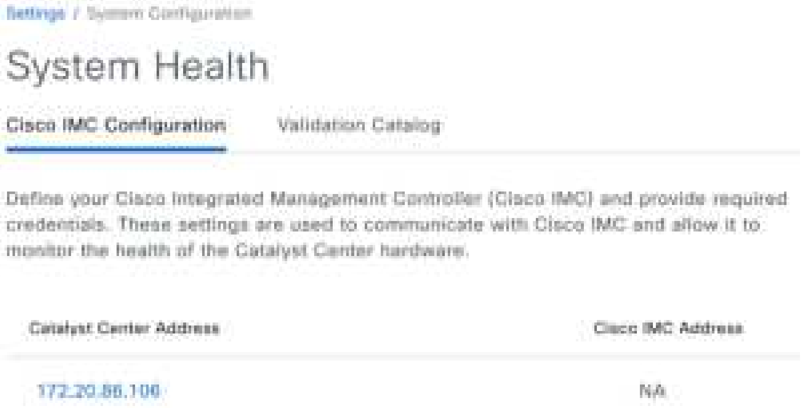
Before you begin

Only users with SUPER-ADMIN-ROLE permissions or CUSTOM-ROLE with "Write" permission to System Settings can configure Cisco IMC connectivity settings for an appliance.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration** > **System Health**.

The IP address of each appliance in your cluster is listed in the **Catalyst Center Address** column.



System Health

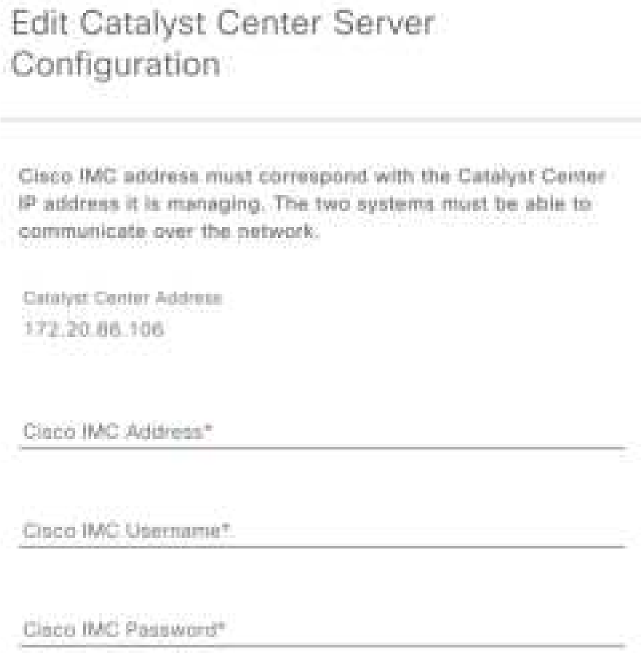
Define your Cisco Integrated Management Controller (Cisco IMC) and provide required credentials. These settings are used to communicate with Cisco IMC and allow it to monitor the health of the Catalyst Center hardware.

Catalyst Center Address	Cisco IMC Address
172.20.86.106	NA

Step 2 Configure the information required to log in to Cisco IMC:

a) Click the IP address for an appliance.

The **Edit Catalyst Center Server Configuration** slide-in pane is displayed.



Edit Catalyst Center Server Configuration

Cisco IMC address must correspond with the Catalyst Center IP address it is managing. The two systems must be able to communicate over the network.

Catalyst Center Address
172.20.86.106

Cisco IMC Address*

Cisco IMC Username*

Cisco IMC Password*

b) Enter this information and then click **Save**:

- The IP address configured for the appliance's Cisco IMC port.
- The username and password required to log in to Cisco IMC.

c) Repeat this step for the other appliances in your cluster, if necessary.

Delete Cisco IMC settings

To delete the Cisco IMC connectivity settings that have been configured previously for a particular appliance, complete these procedure.

Before you begin

Only users with SUPER-ADMIN-ROLE permissions or CUSTOM-ROLE with "Write" permission to System Settings can delete these settings.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration** > **System Health**.

Step 2 For the appliance you want to delete settings for, click the corresponding delete icon (🗑) in the **Actions** column.

Step 3 In the confirmation window, click **OK**.

Subscribe to system event notifications

After you have established connectivity with Cisco IMC, Catalyst Center collects event information from Cisco IMC and stores this information as raw system events. The rules engine then processes these raw events and converts them into system event notifications that are displayed in the System Health topology. By completing the procedure described in the "Work with Event Notifications" topic of the *Cisco Catalyst Center Platform User Guide*, you can also receive these notifications in one of the available formats. When completing this procedure, select and subscribe to these events:

Table 2: System notification events in Catalyst Center

Event name	Event ID	Domain	Sub domain	Description
System Backup v2	SYSTEM-BACKUP-v2	System	System Backup	A notification is sent when the backup operation fails.
System Restore v2	SYSTEM-RESTORE-v2	System	System Restore	The event is generated on failure during restore operation.
System Software Upgrade v2	SYSTEM-SOFTWARE-UPGRADE-v2	System	System Software Upgrade	A notification is sent when the software upgrade operation fails.

Event name	Event ID	Domain	Sub domain	Description
Disaster Recovery health status v2	SYSTEM-DISASTER-RECOVERY-v2	System	Disaster Recovery	A notification is sent when the state of the disaster recovery system changes.
CMX connectivity failure v2	SYSTEM-EXTERNAL-CMX-v2	External Integrations	CMX Connectivity	A notification is sent when there's no connectivity with CMX.
External IPAM provider connectivity failure v2	SYSTEM-EXTERNAL-IPAM-v2	External Integrations	IPAM Integration	A notification is sent when there's no connectivity with an external IPAM provider.
ISE AAA trust establishment failure v2	SYSTEM-EXTERNAL-ISE-AAA-TRUST-v2	External Integrations	Cisco ISE AAA Trust Establishment	A notification is sent when the ISE AAA trust establishment fails.
ISE PAN ERS connectivity failure v2	SYSTEM-EXTERNAL-ISE-PAN-ERS-v2	External Integrations	Cisco ISE PAN ERS Connectivity	A notification is sent when there's no connectivity with the Cisco ISE primary and secondary PAN ERS.
ISE PxGrid health state change notification v2	SYSTEM-EXTERNAL-ISE-PXGRID-v2	External Integrations	Cisco pxGrid	A notification is sent when the health state of Cisco ISE PxGrid connections change.
External ITSM provider connectivity failure v2	SYSTEM-EXTERNAL-ITSM-v2	External Integrations	ITSM Integration	A notification is sent when there's no connectivity with an external ITSM provider.
Certificate Status Notification v2	SYSTEM-CERTIFICATE-v2	System	System Certificate	A notification is sent when a system certificate, built-in certificate, proxy certificate, disaster recovery certificate, or a third-party trusted certificate has expired, been revoked, or will expire in less than 90 days.

Event name	Event ID	Domain	Sub domain	Description
Cisco IMC Certificate Status Notification v2	CISCO-IMC-CERTIFICATE-v2	Appliance	Cisco IMC Certificate	A notification is sent when the Cisco IMC certificate has expired, been revoked, or will expire in less than 90 days.
Cisco IMC Connectivity status v2	CISCO-IMC-v2	Appliance	Cisco IMC	A notification is sent whenever Cisco IMC's connectivity status changes.
System Appliance Configuration Status Notification v2	CISCO-IMC-CONFIGURATION-v2	Appliance	Cisco IMC Configuration	A notification is sent when the Cisco IMC hardware configurations are not compliant with the Cisco standards.
System Hardware health status v2	CISCO-IMC-HARDWARE-v2	Appliance	Cisco IMC Hardware Health Status	A notification is sent when the health status of any hardware component changes. Supported hardware components include: • CPU • Memory • Disk • NIC • Fan • Power Supply • RAID controller

Event name	Event ID	Domain	Sub domain	Description
System managed services v2	SYSTEM-MANAGED-SERVICES-v2	System	System Managed Services	A notification is sent when the status of a platform-provided managed service changes. **Note** For managed services, the probe interval (the time it takes for Catalyst Center to delete stale events from its database) is 60 minutes. When managed services that have been down become active again, it takes this long for the System Health GUI to reflect that the services have been restored.
System Performance: Filesystem Utilization v2	SYSTEM-PERFORMANCE-v2	System	System Performance: Filesystem Utilization	A notification is sent when filesystem (partition) utilization is approaching capacity.
System Scale Limits v2	SYSTEM-SCALE-LIMITS-v2	System	System Scale Limits	A notification is sent when scale limits have been exceeded.
Application Health v2	SYSTEM-APPLICATION-HEALTH-v2	System	Application Health	A notification is sent when the health state of an application registered for monitoring changes.
Cisco Trusted Certificate Update Notifications v2	CISCO-TRUSTED-CERTIFICATE-BUNDLE-v2	System	Cisco Trusted Certificates	A notification is sent when a newer Cisco-trusted certificate bundle is available.

Event name	Event ID	Domain	Sub domain	Description
Internet URL Accessible Notifications v2	INTERNET-URL-ACCESS-v2	System	Internet Access	A notification is sent when Catalyst Center is unable to reach any of the URLs listed in Check required URLs access, on page 32.

Event notification information

This table lists the key information that Catalyst Center provides when it generates a system health notification message.

Subdomain	Tag	Instance	State	Message
Domain: System				
CPU	CPU	*<node-hostname>*:CPU-1	OK	Catalyst Center CPU-1 is working as expected on *<node-hostname>*
			NotOk	Catalyst Center CPU-1 has failed on *<node-hostname>*
			Disabled	Catalyst Center CPU-1 is disabled on *<node-hostname>*
Memory	Memory	*<node-hostname>*:DIMM_A1	Ok	Catalyst Center RAM DIMM_A1 is working as expected on *<node-hostname>*
			NotOk	Catalyst Center RAM DIMM_A1 has failed on *<node-hostname>*
Disk	Disk	*<node-hostname>*:Disk1	Ok	Catalyst Center Disk 2 is working as expected on *<node-hostname>*
			NotOk	Catalyst Center Disk 2 has failed on *<node-hostname>*
RAID Controller	RAIDController	*<node-hostname>*:Controller-1	Ok	Catalyst Center RAID VD-2 is working as expected on *<node-hostname>*
			NotOk	Catalyst Center RAID VD-2 has degraded on *<node-hostname>*
			Disabled	Catalyst Center RAID VD-2 is offline on *<node-hostname>*
Network Interfaces	NIC	*<node-hostname>*:nic-1	Ok	Catalyst Center network interfaces are working as expected
			NotOk	Catalyst Center: *<x>* network interfaces are missing for *<node-hostname>*: nic-1

Subdomain	Tag	Instance	State	Message
PSU_FAN	PSU	*<node-hostname>*:psu-1	Ok	Catalyst Center power supply (PSU-1) is powered on and thermal condition is normal for *<node-hostname>*
			NotOk	Catalyst Center power supply (PSU-2) is powered off and thermal condition is critical for *<node-hostname>*
Disaster Recovery	DisasterRecovery	*<disaster-recovery-hostname>*	Ok	• Disaster recovery cluster is up • Disaster recovery failover succeeded to *<site-name>*
			Degraded	• Disaster recovery failover triggered from *<site-name>* to *site-name* • Disaster recovery failed while failing over to *<site-name>* • Disaster recovery standby cluster on *<site-name>* is down; cannot failover • Disaster recovery witness is down; cannot failover • Disaster recovery replication halted; recovery point objective will be impacted • Disaster recovery pause failed • Disaster recovery route advertisement failed • Disaster recovery IPSec communication failed
			NotOk	• Disaster recovery configuration failed • Disaster recovery failed to rejoin the standby system
Platform Services	ManagedServices	<hostname>:<name>	OK	Managed Service *<service-name>* is Running
			NOTOK	Managed Service *<service-name>* is Interrupted

Subdomain	Tag	Instance	State	Message
Scale Limits	wired_concurrent_clients	<hostname>:<name>	OK	OK
			NOTOK	The number of concurrent wired clients exceeded 26250 (105% of limit)
			DEGRADED	The number of concurrent wired clients exceeded 21250 (85% of limit)
			CAUTION	The number of concurrent wired clients exceeded 18750 (75% of limit)
	wireless_concurrent_clients	<hostname>:<name>	OK	OK
			NOTOK	The number of concurrent wireless clients exceeded 18750 (75% of limit)
			DEGRADED	The number of concurrent wireless clients exceeded 21250 (85% of limit)
			CAUTION	The number of concurrent wireless clients exceeded 18750 (75% of limit)
	wired_devices	<hostname>:<name>	OK	OK
			NOTOK	The number of wired devices exceeded 1050 (105% of limit)
			DEGRADED	The number of wired devices exceeded 850 (85% of limit)
			CAUTION	The number of wired Devices exceeded 750 (75% of limit)
	wireless_devices	<hostname>:<name>	OK	OK
			NOTOK	The number of wireless devices exceeded 3800 (105% of limit)
			DEGRADED	The number of wireless devices exceeded 3400 (85% of limit)
			CAUTION	The number of wireless devices exceeded 3000 (75% of limit)
	interfaces	<hostname>:<name>	OK	OK
			NOTOK	The number of interfaces exceeded 1140000000 (95% of limit)
			DEGRADED	The number of interfaces exceeded 1020000000 (85% of limit)
			CAUTION	The number of interfaces exceeded 900000000 (75% of limit)
	ippools	<hostname>:<name>	OK	OK
			NOTOK	The number of IP pools exceeded 47500 (95% of limit)

Subdomain	Tag	Instance	State	Message
			DEGRADED	The number of IP pools exceeded 42500 (85% of limit)
			CAUTION	The number of IP pools exceeded 37500 (75% of limit)
	netflows	<hostname>:<name>	OK	OK
			NOTOK	The number of Netflows exceeded 37500 (75% of limit)
			DEGRADED	The number of Netflows exceeded xxx (x% of limit)
			CAUTION	The number of Netflows exceeded yyy (y% of limit)
	physical_ports	<hostname>:<name>	OK	OK
			NOTOK	The number of physical ports exceeded 50400 (95% of limit)
			DEGRADED	The number of physical ports exceeded 40800 (85% of limit)
			CAUTION	The number of physical ports exceeded 36000 (75% of limit)
	policy	<hostname>:<name>	OK	OK
			NOTOK	The number of policies exceeded 23750 (95% of limit)
			DEGRADED	The number of policies exceeded 21250 (85% of limit)
			CAUTION	The number of policies exceeded 18750 (75% of limit)
	security_group	<hostname>:<name>	OK	OK
			NOTOK	The number of security groups exceeded 3800 (95% of limit)
			DEGRADED	The number of security groups exceeded 3400 (85% of limit)
			CAUTION	The number of security groups exceeded 3000 (75% of limit)
	sites	<hostname>:<name>	OK	OK
			NOTOK	The number of sites exceeded 475 (95% of limit)
			DEGRADED	The number of sites exceeded 425 (85% of limit)
			CAUTION	

Subdomain	Tag	Instance	State	Message
				The number of sites exceeded 375 (75% of limit)
	transient_clients	<hostname>:<name>	OK	OK
			NOTOK	The number of transient clients exceeded 71250 (95% of limit)
			DEGRADED	The number of transient clients exceeded 63750 (85% of limit)
			CAUTION	The number of transient clients exceeded 56250 (75% of limit)
	MongoDB	<hostname>:<name>	CRITICAL	The disk usage exceeded 16.58 GB (80% of limit)
	Postgres	<hostname>:<name>	CRITICAL	The disk usage exceeded 65.53 GB (80% of limit)
Software Upgrade	Upgrade	<hostname>:<name>	OK	Successfully finished downloading package *<package-name>* with version *<package-version>*
			NOTOK	Catalog package download failed for *<package-name>*
Backup	Backup	<hostname>:<name>	OK	Successfully completed backup
			NOTOK	Failed to backup
Restore	Restore	<hostname>:<name>	OK	Successfully restored
			NOTOK	Failed to restore configuration
Domain: Connectivity				
ISE	ISE_ERS	*<Cisco-ISE-hostname>*	Success	ISE AAA trust establishment succeeded for ISE server *<ISE-server-details>*
			Failed	ISE AAA trust establishment failed for ISE server *<ISE-server-details>*
Domain: Integrations				
IPAM	IPAM	*<IPAM-hostname>*	Ok	IPAM connection to Catalyst Center established. IPAM *<IPAM-IP-address>*.
			Critical	IPAM connection to Catalyst Center offline. IPAM *<IPAM-IP-address>*.

Subdomain	Tag	Instance	State	Message
ISE	ISE_AAA	*<Cisco-ISE-hostname>*	Up	ISE AAA trust establishment succeeded for ISE server. ISE *<ISE-IP-address>*
			Down	ISE AAA trust establishment failed for ISE server. ISE *<ISE-IP-address>*
CMX	CMX	*<CMX-hostname>*	serviceAvailable	CMX connection to Catalyst Center offline. CMX *<CMX-IP-address>*.
			serviceNotAvailable	CMX connection to Catalyst Center offline. CMX *<CMX-IP-address>*.
ITSM	ITSM	*<ITSM-hostname>*	Up	ITSM connection to Catalyst Center offline. ITSM *<ITSM-IP-address>*.
			Down	ITSM connection to Catalyst Center offline. ITSM *<ITSM-IP-address>*.

System health scale numbers

System Health monitors Catalyst Center appliances and generates a notification whenever a network component listed in the following table exceeds a particular threshold. The priority of the notification that is generated depends on the percentage of a threshold that has been measured:

- When 75% of a threshold has been exceeded, an information (P3) notification is generated.
- When 85% of a threshold has been exceeded, a warning (P2) notification is generated.
- When 95% of a threshold has been exceeded, a critical (P1) notification is generated.

Note

- See the "Supported Hardware Appliances" topic in the *Release Notes for Cisco Catalyst Center, Release 2.3.7.x* for a listing of the Catalyst Center appliances that are available.
- 1,000,000 notifications are maintained in the audit log for every appliance (regardless of type) and are stored for one year.
- To view the current appliance scale numbers, see the *Cisco Catalyst Center Data Sheet*.
- System Health isn't supported on Catalyst Center clusters consisting of three 44-core appliances.

View the system topology

From the **System Health** window's topology, you can view a graphical representation of your Catalyst Center appliances and the external systems that are connected to your network, such as Cisco Connected Mobile Experiences (Cisco CMX) and Cisco Identity Services Engine (Cisco ISE). Here, you can quickly identify any network components that are experiencing an issue and require further attention. In order to populate this page with appliance and external system data, you must first complete the tasks described in thse topics:

- Establish Cisco IMC connectivity, on page 8

- Subscribe to system event notifications, on page 10

To view this page, click the menu icon and choose **System** > **System 360**, then click the **System Health** tab. Topology data is polled every 30 seconds. If any new data is received, the topology automatically updates to reflect this data.

Note

- Catalyst Center supports IPv6. When viewing a cluster on which IPv6 is enabled, the topology also displays the following information for that cluster's Enterprise virtual IP address:
  - **Pre** field: 16-bit prefix
  - **GID** field: 32-bit global ID
  - **Subnet** field: 16-bit subnet value

  The remainder of the cluster's Enterprise virtual IP address is used to label its topology icon.
- An IPv6-enabled cluster can only connect to and retrieve data from external systems that also support IPv6.
- Whenever a connected appliance or external system has a certificate installed that's set to expire, the topology does this:
  - If a certificate is set to expire within 90 days, the topology displays a warning.
  - If a certificate is set to expire within 30 days, the topology displays an error to bring your attention to the issue.
- System Health runs a hardware compliance check regularly and indicates whenever a connected appliance or external system does not meet the minimum configuration requirements. For example, System Health updates the topology to indicate when the **Write Through** cache write policy is not set for a connected virtual drive.
- If disaster recovery is operational in your production environment, System Health now provides hardware information for the appliances at both the main and recovery site. Previously, hardware information was provided only for main site appliances.

Troubleshoot appliance and external system issues

When viewing the System Health topology, the minor issue icon (⚠) and major issue icon (✖) indicate network components that require attention. To begin troubleshooting the issue that a component is experiencing, place your cursor over its topology icon to open a pop-up window that displays this information:

- A timestamp that indicates when the issue was detected.
- If you are viewing the pop-up window for a Catalyst Center appliance, the Cisco IMC firmware version that is installed on the appliance.
- A brief summary of the issue.
- The current state or severity of the issue.
- The domain, subdomain, and IP address or location associated with the issue.

If you open the pop-up window for a connected external system that has three or more associated servers or a Catalyst Center appliance that has three or more hardware components that are experiencing an issue, the **More Details** link is displayed. Click the link to open a slide-in pane that lists the relevant servers or components. You can then view information for a specific item by clicking **>** to maximize its entry.

Troubleshoot external system connectivity issues

If Catalyst Center is currently unable to communicate with an external system, to ping that system and troubleshoot why it cannot be reached, do this procedure:

Before you begin

Do the following before you complete this procedure:

- Install the Machine Reasoning package. See Download and install applications, on page 115.
- Create a role that has write permission to the Machine Reasoning function and assign that role to the user that completes this procedure. To access this parameter in the **Create a User Role** wizard, expand the **System** row in the **Define the Access** page. For more information, see Configure role-based access control, on page 124.

Procedure

Step 1 From the top-right portion of the **System Health** window, choose **Tools** > **Network Ping** to open the **Ping Device** window.

The window lists all the devices that Catalyst Center currently manages.

Step 2 Click the radio button for any device whose reachability status is **Reachable** and then click the **Troubleshoot** link.

The **Reasoner Inputs** window opens.

Step 3 In the **Target IP Address** field, enter the IP address of the external system that cannot be reached.

Step 4 Click **Run Machine Reasoning**.

A dialog box is displayed after Catalyst Center has pinged the external system.

Step 5 Click **View Details** to see whether the ping was successful.

Step 6 If the ping failed, click the **View Relevant Activities** link to open the **Activity Details** slide-in pane and then click the **View Details** icon.

The **Device Command Output** window opens, listing possible causes for the inability to reach the external system.

Use the Validation tool

The **Validation Tool** tests both the Catalyst Center appliance hardware and connected external systems. The tool identifies any issues that need to be addressed before they seriously impact your network. The validation process makes numerous checks, such as:

- The ability to connect to ciscoconnectdna.com (to download system and package updates).

- The presence of expiring certificates.
- The current health of appliance hardware and back-end services.
- The network components that have exceeded a scale number threshold.

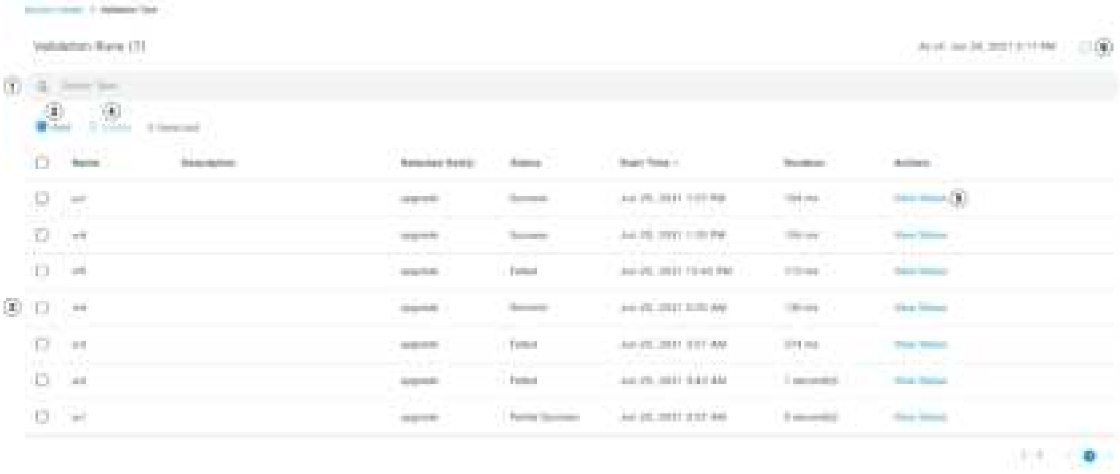
To access the tool:

1. From the main menu, choose **System** > **System 360**, and then click the **System Health** tab.
2. From the **Tools** drop-down menu, choose **Validation Tool**.

Navigate the Validation Tool window

The contents of the **Validation Tool** window depend on whether Catalyst Center has information for any validation runs that completed previously. If it doesn't, the window looks like this:

If Catalyst Center has validation run information, the window looks like this:



This table describes the components that make up the **Validation Tool** window and their function when validation run information is available.

Callout	Description
1	**Search Table** field: Enter a search string to filter the validation runs that are listed on this window.

Callout	Description
2	**Add** button: Click to open the **New Validation Run** slide-in pane and enter the required settings for a new run. For more information, see Start a validation run, on page 23.
3	**Validation Runs** table: Lists the validation runs that completed previously. For each run, the table provides information such as its name, applicable validation set, and completion status. **Note** • By default, the runs are ordered by start time, with the most recent run listed first. • A duration of zero is listed for any run that's currently in progress.
4	**Delete** button: With the check box for a validation run checked, click to delete the run. Then click **Ok** in the **Warning** dialog box to confirm deletion. **Note** You cannot delete a run that is in progress.
5	**View Status** link: Click to view the details for a particular run. For more information, see View Validation Run Details, on page 24.
6	**Refresh** button: Click to refresh the information that is displayed on this window.

Start a validation run

To start a validation run, complete these steps.

Note Only one validation run can take place at a time. If a validation run is already in progress, you need to wait until it completes before you can initiate another run.

Procedure

Step 1 Do one of these tasks in the **Validation Tool** window, depending on whether the **Validation Runs** table is displayed:

- If the table is not displayed, it means that either previous validation runs have been deleted or a validation run hasn’t been completed yet. Click **New Validation Run**.
- If the **Validation Runs** table is displayed, click **Add**.

The **New Validation Run** slide-in pane opens.

Step 2 In the **Name** field, enter a name for the validation run.

Ensure that the name that you enter is unique and contains only alphanumeric characters. Special characters aren’t allowed.

Step 3 (Optional) In the **Description** field, enter a brief description for the validation run you’re about to start.

You can enter a description that contains a maximum of 250 characters.

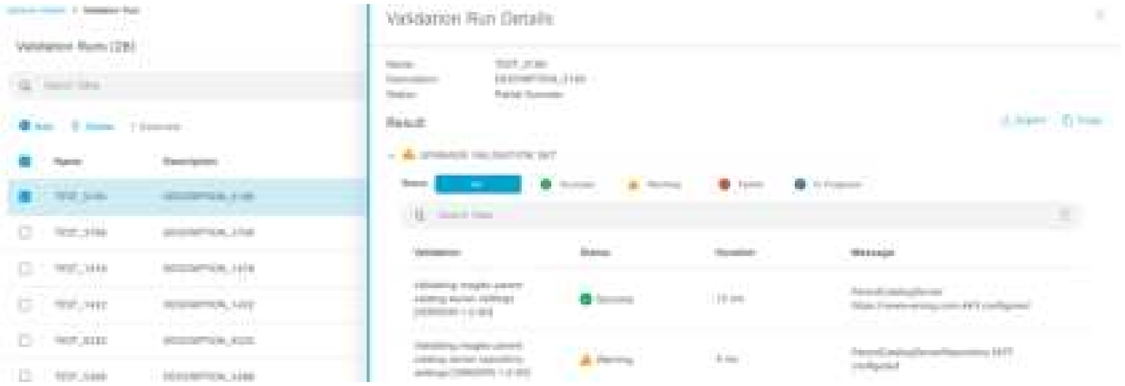
Step 4 In the **Validation Set(s) Selection** area, check the check box for the validation sets you want to run.

You can maximize a validation set to view the checks it makes.

Step 5 Click **Run**.

View Validation Run Details

From the **Validation Run Details** slide-in pane, you can view the checks that were made during the selected run, completion status, duration, and any other relevant information.



From here, you can also do these tasks:

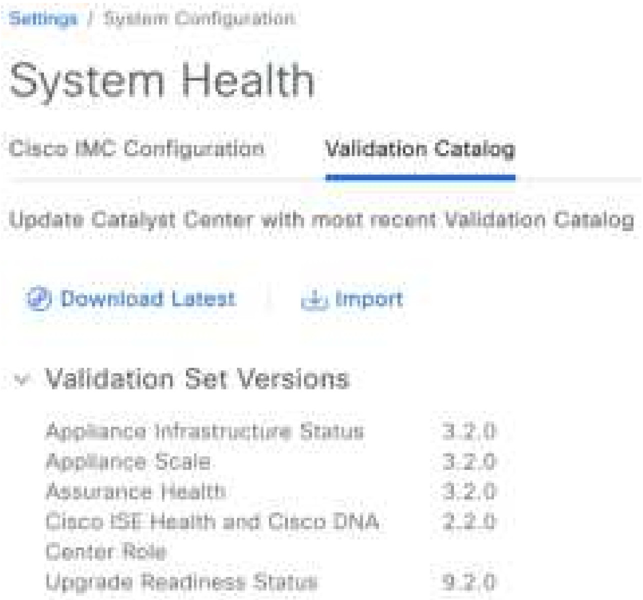
- To filter the information that's provided, in the **Search Table** field, enter a search string.
- To download the contents of this pane as a JSON file, click **Export**.
- To copy the contents of this pane, click **Copy**.

Update the validation set

Validation sets should be updated whenever you upgrade Catalyst Center. In case you need to update validation sets manually, do this procedure:

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration** > **System Health**.



Settings / System Configuration

System Health

Update Catalyst Center with most recent Validation Catalog

Validation Set Versions

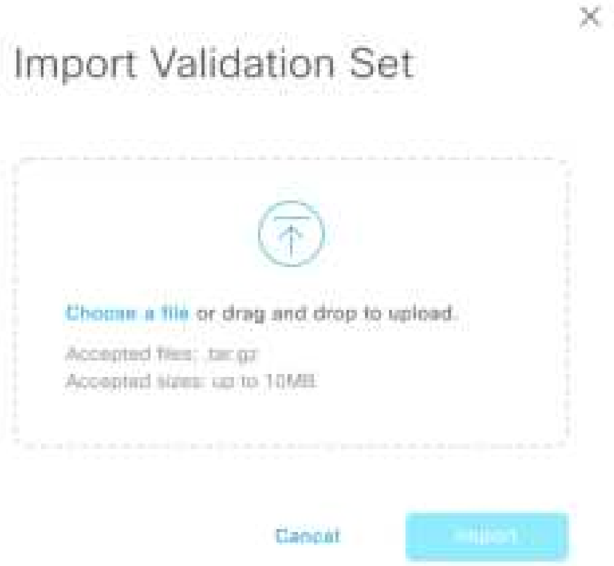
Appliance Infrastructure Status	3.2.0
Appliance Scale	3.2.0
Assurance Health	3.2.0
Cisco ISE Health and Cisco DNA Center Role	2.2.0
Upgrade Readiness Status	9.2.0

Step 2 Click the **Validation Catalog** tab.

Step 3 Click **Download Latest** to download a local copy of the latest available validation sets.

Step 4 Import the validation set to Catalyst Center:

a) Click **Import** to open the **Import Validation Set** dialog box.



Import Validation Set

Choose a file or drag and drop to upload.

Accepted files: .tar.gz
Accepted sizes: up to 10MB

b) Do one of these tasks:

- Click the **Choose a file** link and navigate to the .tar file that you want to import.
- Drag and drop the appropriate .tar file from your desktop into the highlighted area.

c) Click **Import**.

Use the System Analyzer tool

If you encounter an issue that requires troubleshooting, you can retrieve log files using the System Analyzer tool. In addition to system-level log files, you can retrieve log files that are specific to Cisco SD-Access and software image management (SWIM).

To access the **System Analyzer** tool:

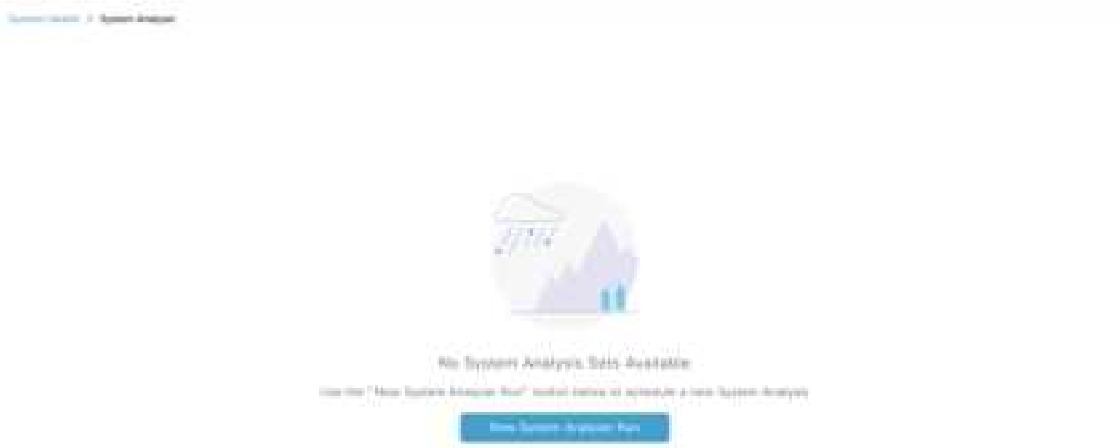
1. From the main menu, choose **System** > **System 360**, then click the **System Health** tab.
2. From the **Tools** drop-down list, choose **System Analyzer**.

Note Before you use this tool:

- Only admin users can start system analysis runs, download the resulting log files, and delete completed runs. All users can open and view the **System Analysis Details** slide-in pane for a selected run.
- The System Analyzer tool requires 5 GB of disk space on Catalyst Center's GlusterFS filesystem.
- Catalyst Center stores either 5 GB or the system analysis runs for the last three months, whichever is smaller.
- When either of the storage limits are reached, Catalyst Center deletes older runs once daily. It also deletes older runs before every new run is started.
- Since log file information is only useful for troubleshooting, data for system analysis runs is not backed up.
- In a deployment where HA is enabled, if the System Health service goes down while a run is in progress, you need to restart the run after System Health is up again.
- In a deployment where disaster recovery is enabled, run data is not replicated across the disaster recovery system's sites. The system's active and standby sites maintain their own run history.

Navigate the System Analyzer window

The contents of the **System Analyzer** window depend on whether Catalyst Center has information for any runs that completed previously. If it doesn't, the window looks like this:

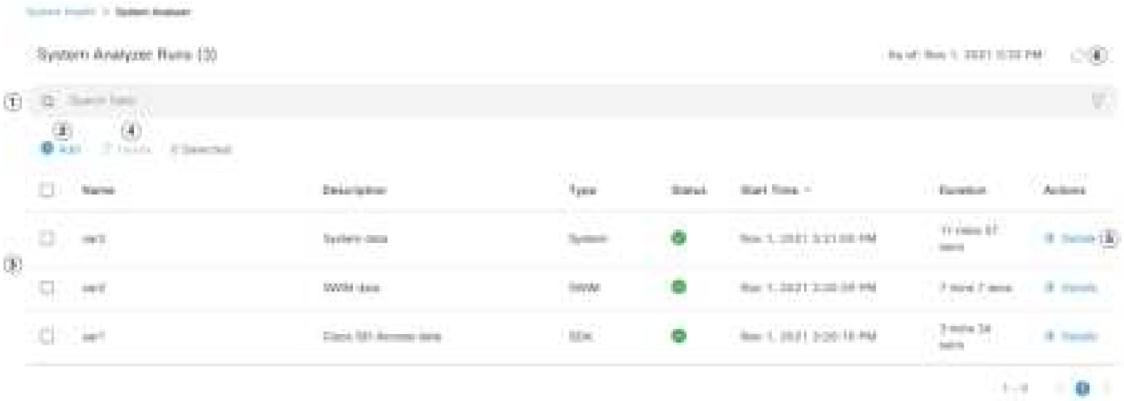


System Health > System Analyzer

No System Analysis Sets Available

Use the "New System Analyzer Run" button below to schedule a new System Analysis

If Catalyst Center has run information, the window looks like this:



System Health > System Analyzer

System Analyzer Runs (3)

As of: Nov 1, 2021 3:33 PM

□	Name	Description	Type	Status	Start Time	Duration	Actions
□	run3	System data	System	●	Nov 1, 2021 3:21:00 PM	11 mins 57 secs	Details
□	run2	SWIM data	SWIM	●	Nov 1, 2021 3:20:59 PM	7 mins 7 secs	Details
□	run1	Cisco SD-Access data	SDA	●	Nov 1, 2021 3:20:15 PM	3 mins 34 secs	Details

This table describes the components that make up the **System Analyzer** window and the functions when run information is available.

Callout	Description
1	**Search Table** field: Enter a search string to filter the runs that are listed on this page.
2	**Add** button: Click to open the **New System Analyzer Run** slide-in pane and enter the required settings for a run. See Start a System Analyzer run, on page 28 for more information.
3	**System Analyzer Runs** table: Lists the runs that are currently in progress or have completed previously. For each run, the table provides information such as its name, the relevant Catalyst Center component, and the amount of time it took to complete the run. **Note** • By default, the runs are ordered by start time, with the most recent run listed first. • A duration of zero is listed for any run that's currently in-progress.
4	**Delete** button: With the check box for a run checked, click **Delete** to remove it. **Note** You cannot delete a run that is in progress.

Callout	Description
5	**Details** link: Click to view the details for a particular run. For more information, see View System Analyzer run details, on page 28.
6	**Refresh** button: Click to refresh the information that displays on this window.

Start a System Analyzer run

Complete this procedure to start a System Analyzer run.

Procedure

Step 1 Do one of these tasks in the **System Analyzer** window, depending on whether the **System Analyzer Runs** table displays:

- If the table is not displayed, it indicates that either previous runs have been deleted or a run hasn't been completed yet. Click **New System Analyzer Run**.
- If the **System Analyzer Runs** table displays, click **Add**.

The **New System Analyzer Run** slide-in pane opens.

Step 2 In the **Name** field, enter a name for the run.

Ensure that the name that you enter is unique and only contains alphanumeric characters. Special characters are not allowed.

Step 3 (Optional) In the **Description** field, enter a brief description of the run you are about to start.

You can enter a description that contains a maximum of 250 characters.

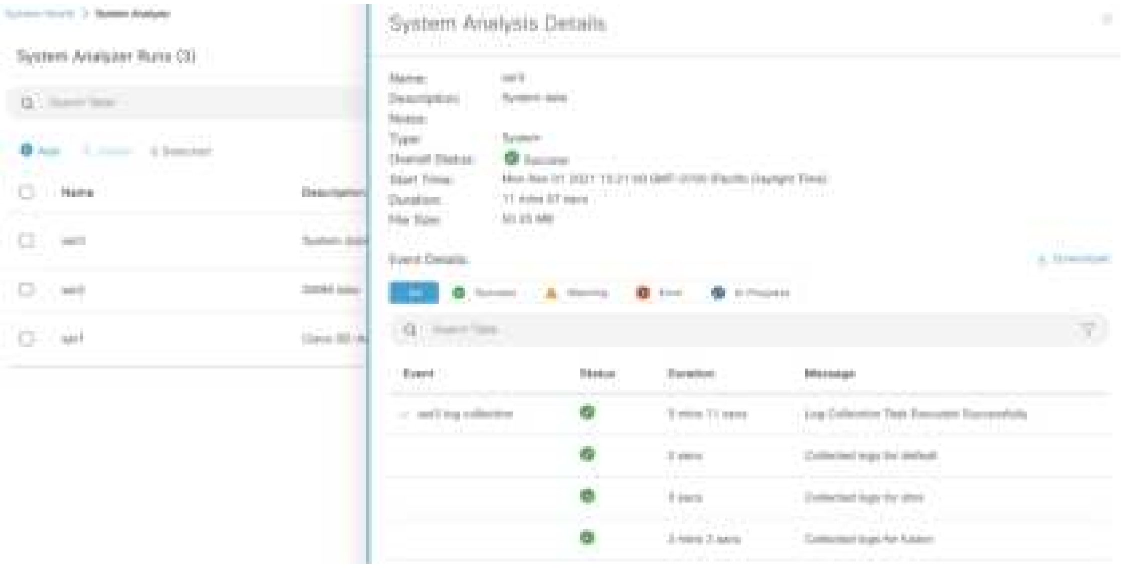
Step 4 (Optional) In the **Notes** field, enter any additional information (up to a maximum of 250 characters) you want to provide for the run.

Step 5 In the **Select a System Analyzer to run** area, click the radio button for the Catalyst Center component that you want to retrieve log files for.

Step 6 Click **Run**.

View System Analyzer run details

From the **System Analysis Details** slide-in pane, you can view additional information for the selected run, such as the total file size of the log files that were retrieved and the relevant Catalyst Center components. You can also identify any log files that encountered an issue during the run.



System Analysis Details

System Analyzer Runs (3)

Name:

Description:

Notes:

Type:

Overall Status:

Start Time:

Duration:

File Size:

Event Details

Event	Status	Duration	Message

From here, you can also do these tasks:

- In the **Search Table** field, enter a search string to filter the information that's displayed.
- Click **Download** to download the log files that were retrieved as a .tar.gz file.

To open the **System Analysis Details** slide-in pane for a particular run, click its **Details** link in the **Actions** column.

System topology notifications

These tables list the various notifications that are displayed in the system topology of the **System Health** page for your Catalyst Center appliances and any connected external systems. Notifications are grouped by their corresponding severity:

- Severity 1 (Error): Indicates a critical error, such as a disabled RAID controller or faulty power supply.
- Severity 2 (Warning): Indicates an issue such as the inability to establish trust with a Cisco ISE server.
- Severity 3: (Success): Indicates that a server or hardware component is operating as expected.

Note If all the hardware components on an appliance are operating without any issues, an individual notification is not provided for each component. An OK notification displays instead.

Table 3: Catalyst Center appliance notifications

Component	Severity 1 notification	Severity 2 notification	Severity 3 notification
CPU	Processor CPU1 (SerialNumber - *xxxxxx*) State is Disabled	Processor CPU1 (SerialNumber - *xxxxxx*) Health is NotOk and State is Enabled	Processor CPU1 (SerialNumber - *xxxxxx*) Health is Ok and State is Enabled

Component	Severity 1 notification	Severity 2 notification	Severity 3 notification
Disk	Driver - PD1 State is Disabled	Driver - PD1 Health is Critical and State is Enabled	Driver - PD1 Health is Ok and State is Enabled
MemoryV1	Memory Summary (TOTALSYSTEMMEMORYGIB - 256) Health is NotOk	—	Memory Summary (TOTALSYSTEMMEMORYGIB - 256) Health is Ok
MemoryV2	Storage DIMM1 (SerialNumber - *xxxxx*) Status is NotOperable	—	Storage DIMM1 (SerialNumber - *xxxxx*) Status is Operable
NIC	NIC Adapter Card MLOM State is Disabled	NIC Adapter Card MLOM State is Enabled and port0 is Down	NIC Adapter Card MLOM State is Enabled and port0 is Up
Power supply	PowerSupply PSU1 (SerialNumber - *xxxx*) State is Disabled	—	PowerSupply PSU1 (SerialNumber - *xxxx*) State is Enabled
RAID	Cisco 12G SAS Modular Raid Controller (SerialNumber - *xxxxx*) State is Disabled	Cisco 12G SAS Modular Raid Controller (SerialNumber - *xxxxx*) Health is NotOK and State is Enabled	Cisco 12G SAS Modular Raid Controller (SerialNumber - *xxxxx*) Health is OK and State is Enabled

Table 4: Connected external system notifications

Component	Severity 1 notification	Severity 2 notification	Severity 3 notification
Cisco Connected Mobile Experiences (CMX) server	—	There is a critical issue with the integrated CMX server.	CMX server is integrated and servicing.
IP address management (IPAM) server	There is a critical issue with the connected third-party IPAM provider	—	• A third-party IPAM provider is connected. • There is no third-party IPAM provider connected. • The third-party IPAM provider is currently synchronizing.
Cisco ISE—External RESTful Services (ERS)	—	ISE PAN ERS connection: ISE ERS API call unauthorized	ISE PAN ERS connection: ERS reachability with ISE - Success
Cisco ISE—Trust	—	ISE AAA Trust Establishment: Trust Establishment Error	ISE AAA Trust Establishment: Successfully established trust and discovered PSNs from PAN

Component	Severity 1 notification	Severity 2 notification	Severity 3 notification
IT service management (ITSM) server	Servicenow connection health status is NOT up and running	—	Servicenow connection health status is up and running

Disk use event notifications

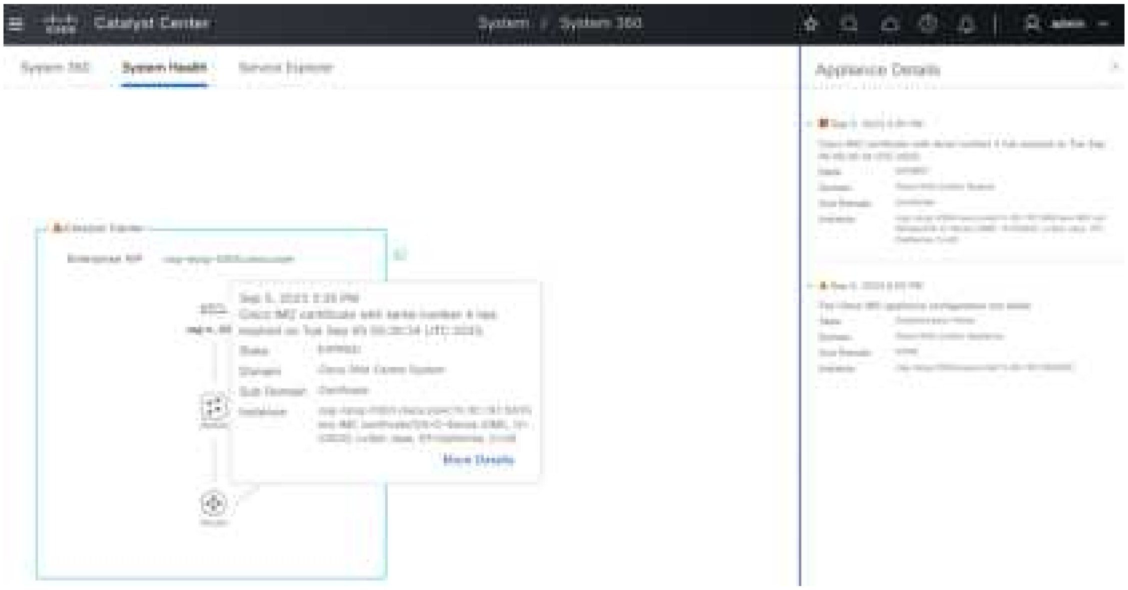
System Health monitors disk use by the nodes in your system and sends a notification whenever use on any of these nodes reaches a level that can impact network operations. When use exceeds 75%, System Health sends a warning notification. And when use exceeds 85%, System Health sends a critical notification. To configure and subscribe to these notifications, complete the steps described in the "Work with Event Notifications" topic of the *Catalyst Center Platform User Guide*. When completing this procedure, select and subscribe to the **System Performance: Filesystem Utilization** event.

Note

- After you restore a backup file or upgrade Catalyst Center, System Health restarts the monitoring of disk use and collects hourly updates.
- In a three-node HA deployment, every configured partition on the three cluster nodes is monitored. Any generated notifications are specific to the relevant partition.
- In a deployment where disaster recovery is enabled, System Health monitors disk use by the nodes at both the active and standby site.

Check for revoked and expired certificates

Catalyst Center checks daily for certificates that have been revoked, expired, or will expire in the near future. If you want to receive notifications whenever one of these events takes place, subscribe to the SYSTEM-CERTIFICATE-v2 and CISCO-IMC-CERTIFICATE-v2 events (see Subscribe to system event notifications, on page 10). In addition to the notifications you receive in the format of your choosing, Catalyst Center also updates the **System Health** window's topology to indicate certificate events. To view these notifications, place your cursor over an appliance. If available, you can also click the **More Details** link to view notifications in the **Appliance Details** slide-in pane.



Catalyst Center supports the storage and update of the Cisco trusted certificate bundle (**ios.p7b**) from the Cisco PKI web site. This bundle, which comes preinstalled with Catalyst Center, enables supported Cisco networking devices to authenticate the controller and its applications (such as Network Plug and Play) upon the presentation of a valid third-party vendor device certificate. Catalyst Center checks the status of the certificate bundle's third-party certificates individually. And for Cisco-signed certificates, it checks if a newer version of the bundle is available to download. To receive notifications when a third-party certificate or the trusted certificate bundle requires an update, subscribe to the CISCO-TRUSTED-CERTIFICATE-BUNDLE-v2 event.

Check required URLs access

Catalyst Center confirms whether these URLs are reachable:

- http://validation.identrust.com/crl/hydrantidcao1.crl
- http://commercial.ocsp.identrust.com
- https://www.ciscoconnectdna.com
- https://cdn.ciscoconnectdna.com
- https://registry.ciscoconnectdna.com
- https://registry-cdn.ciscoconnectdna.com

When any of these URLs are unreachable (especially the first two listed, as they're used to check the revocation status of system certificates), it could impact network operations. Subscribe to the INTERNET-URL-ACCESS-v2 event to receive a notification when this happens.

Suggested actions

This table lists the issues that you’ll most likely encounter while monitoring the health of your system and suggests actions you can take to remedy those issues.

Component	Subcomponent	Issue	Suggested actions
Cisco ISE	External RESTful Services (ERS)—Reachability	Timeout elapsed (possibly because the Cisco ISE ERS API load threshold has been exceeded).	• Check your proxy configuration for a proxy server between Catalyst Center and Cisco ISE. • Check whether you can reach Cisco ISE from Catalyst Center.
		Unable to establish a connection with Cisco ISE.	• Check whether a firewall is configured. • Check your proxy configuration for a proxy server between Catalyst Center and Cisco ISE. • Check whether you can reach Cisco ISE from Catalyst Center.
	ERS—Availability	No response to ERS API call.	• Check which version of Cisco ISE is installed. • Check if ERS is enabled on Cisco ISE. See the "Enable External RESTful Services APIs" topic in the *Cisco Identity Services Engine Administrator Guide* for more information.
	ERS—Authentication	Cisco ISE ERS API call is unauthorized.	Check whether the AAA settings credentials and the Cisco ISE credentials are the same.
	ERS—Configuration	Cisco ISE certificate has been changed.	From the Catalyst Center GUI, reestablish trust. For more information, see the "Enable PKI in Cisco ISE" topic in the *Cisco Identity Services Engine Administrator Guide*.
	ERS—Unclassified/Generic Error	An undefined diagnostic error occurred.	1. Delete the AAA settings that are currently configured in Catalyst Center. 2. Reenter the appropriate AAA settings. For more information, see the "Integrate Cisco ISE with Catalyst Center" topic in the *Cisco Catalyst Center Second Generation Appliance Installation Guide*. 3. Reestablish trust. For more information, see the "Enable PKI in Cisco ISE" topic in the *Cisco Identity Services Engine Administrator Guide*.
	Trust—Reachability	Unable to establish an HTTPS connection.	Check whether the AAA settings credentials and the Cisco ISE credentials are the same.

Component	Subcomponent	Issue	Suggested actions
		The Catalyst Center endpoint URL configured for Cisco ISE certificate chain uploads is unreachable.	• Check your proxy configuration for a proxy server between Catalyst Center and Cisco ISE. • Check whether you can reach Cisco ISE from Catalyst Center.
	Trust—Configuration	Invalid Cisco ISE certificate chain.	• If necessary, regenerate the Cisco ISE internal root CA chain. For more information, see the "ISE CA Chain Regeneration" topic in the *Cisco Identity Services Engine Administrator Guide*. • Ensure that the internal CA certificate chain has not been removed from Cisco ISE.
		The Catalyst Center endpoint URL configured for Cisco ISE certificate chain uploads is forbidden.	• Launch the URL and check whether you can access the /aaa/Cisco ISE/certificate directory on the endpoint. • Check whether the **Use CSRF Check for Enhanced Security** option is enabled in Cisco ISE. For more information, see the "Enable External RESTful Services APIs" topic in the *Cisco Identity Services Engine Administrator Guide*.
	Trust—Authentication	The Cisco ISE password has expired.	• Regenerate the Cisco ISE admin password. For more information, see the "Administrative Access to Cisco ISE" topic in the *Cisco Identity Services Engine Administrator Guide*. • Ensure that you can log in to the Cisco ISE GUI.
	Trust—Unclassified/Generic Error	An undefined diagnostic error occurred.	**1.** Delete the AAA settings that are currently configured in Catalyst Center. **2.** Reenter the appropriate AAA settings. For more information, see the "Integrate Cisco ISE with Catalyst Center" in the *Cisco Catalyst Center Second Generation Appliance Installation Guide*. **3.** Reestablish trust. For more information, see the "Enable PKI in Cisco ISE" topic in the *Cisco Identity Services Engine Administrator Guide*.

Component	Subcomponent	Issue	Suggested actions
Cisco Connected Mobile Experiences (CMX) server IP address management (IPAM) server IT service management (ITSM) server	Reachability	Unable to establish connectivity with the server.	Check whether the server in question is currently down.
	Authentication	Unable to log in to the server.	Confirm that the correct login credentials are configured in Catalyst Center.
Hardware	Disk	The specified hardware component is experiencing an issue.	Replace the faulty component.
	Fan		
	Power supply		
	Memory module		
	CPU		
	Networking card		
	RAID controller		
	Networking	Interfaces are missing.	**1.** Connect to Cisco IMC. **2.** If the PID is UCSC-C220-M4 or UCSC-C220-M4S, complete the following steps: **a.** From the main menu, choose **Compute** > **BIOS** > **Configure BIOS**. **b.** Click the **Advanced** tab. **c.** Expand **LOM and PCIe Slots Configuration**. **d.** Enable the disabled mLOMs and reboot the host. **3.** For all other PIDs, replace the faulty component.

Component	Subcomponent	Issue	Suggested actions
System configuration	Hardware configuration	You cannot specify write-back as the write cache policy for the Catalyst Center *<IP_address>* virtual drive. The write policy must be write-through.	1. Connect to Cisco IMC. 2. From the main menu, choose **Storage** > **Raid Controller**. 3. Click the **Virtual Drive** tab. 4. Select a virtual drive and click **Edit**. If the write policy is not write-through, update the virtual drives. The write policy must be write-through.
System resources	Storage	The specified mount directory is full.	• Clear up storage space in the current directory by removing unnecessary data. • Specify a new mount directory that has more storage space.

Typical node operations

Hardware Peripherals RMA

We recommend that you perform a graceful shutdown of Catalyst Center when replacing hardware peripherals such as DIMMs, CPUs, or a single solid-state drive (SSD) during a return materials authorization (RMA) procedure.

Switch Under Maintenance Without HA

If a directly linked switch in the Layer 2 network is undergoing maintenance without a fallback (HA) mechanism to uphold network service, we recommend that you perform a graceful shutdown. To achieve Layer 2 network redundancy, see "NIC Bonding Overview" in the *Cisco Catalyst Center Appliance Installation Guide*.

Catalyst Center and Cisco ISE integration

Cisco ISE has three use cases with Catalyst Center:

1. Cisco ISE can be used as a AAA (pronounced "triple A") server for user, device, and client authentication. If you are not using access control policies, or are not using Cisco ISE as a AAA server for device authentication, you do not have to install and configure Cisco ISE.
2. Access control policies use Cisco ISE to enforce access control. Before you create and use access control policies, integrate Catalyst Center and Cisco ISE. The process involves installing and configuring Cisco ISE with specific services, and configuring Cisco ISE settings in Catalyst Center. For more information about installing and configuring Cisco ISE with Catalyst Center, see the *Cisco Catalyst Center Installation Guide*.

3. If your network uses Cisco ISE for user authentication, configure Assurance for Cisco ISE integration. This integration lets you see more information about wired clients, such as the username and operating system, in Assurance. For more information, see "About Cisco ISE Configuration for Catalyst Center" in the *Cisco Catalyst Assurance User Guide*.

After Cisco ISE is successfully registered and its trust established with Catalyst Center, Catalyst Center shares information with Cisco ISE. Catalyst Center devices that are assigned to a site that is configured with Cisco ISE as its AAA server have their inventory data propagated to Cisco ISE. Additionally, any updates to the following settings on these devices in Catalyst Center also updates Cisco ISE with the changes:

- Device hostname
- AAA server configurations under **Design** > **Network Settings** > **Servers**.
- Device credentials
- Device Loopback0 IP address
- Device management IP address
- Network Device Group (NDG) tag associated with the device

If a Catalyst Center device associated to a site with Cisco ISE as its AAA server is not propagated to Cisco ISE as expected, Catalyst Center automatically retries after waiting for a specific time interval. This subsequent attempt occurs when the initial Catalyst Center device push to Cisco ISE fails due to any networking issue, Cisco ISE downtime, or any other auto correctable errors. Catalyst Center attempts to establish eventual consistency with Cisco ISE by retrying to add the device or update its data to Cisco ISE. However, a retry is not attempted if the failure to propagate the device or device data to Cisco ISE is due to a rejection from Cisco ISE itself, as an input validation error.

If you change the RADIUS shared secret for Cisco ISE, Cisco ISE does not update Catalyst Center with the changes. To update the shared secret in Catalyst Center to match Cisco ISE, edit the AAA server with the new password. Catalyst Center downloads the new certificate from Cisco ISE, and updates Catalyst Center.

Cisco ISE does not share existing device information with Catalyst Center. The only way for Catalyst Center to know about the devices in Cisco ISE is if the devices have the same name in Catalyst Center; Catalyst Center and Cisco ISE uniquely identify devices for this integration through the device's hostname variable.

Note The process that propagates Catalyst Center inventory devices to Cisco ISE and updates the changes to it are all captured in the Catalyst Center audit logs. If there are any issues in the Catalyst Center-to-Cisco ISE workflow, view the audit logs in the Catalyst Center GUI for information.

Catalyst Center integrates with the primary Administration ISE node. When you access Cisco ISE from Catalyst Center, you connect with this node.

Catalyst Center polls Cisco ISE every 15 minutes. If the Cisco ISE server is down, Catalyst Center shows the Cisco ISE server as red (unreachable).

When the Cisco ISE server is unreachable, Catalyst Center increases polling to 15 seconds, and then doubles the polling time to 30 seconds, 1 minute, 2 minutes, 4 minutes, and so on, until it reaches the maximum polling time of 15 minutes. Catalyst Center continues to poll every 15 minutes for 3 days. If Catalyst Center does not regain connectivity, it stops polling and updates the Cisco ISE server status to **Untrusted**. If this happens, you must reestablish trust between Catalyst Center and the Cisco ISE server.

Network Device Group (NDG) tags, which are prefixed with `NDG:`, are reflected in Cisco ISE.

When you delete devices integrated with Cisco ISE, those deleted devices are moved to the new NDG group in Cisco ISE.

Review the following additional requirements and recommendations to verify Catalyst Center and Cisco ISE integration:

- Catalyst Center and Cisco ISE integration is not supported over a proxy server. If you have Cisco ISE configured with a proxy server in your network, configure Catalyst Center such that it does not use the proxy server; it can do this by bypassing the proxy server's IP address.
- Catalyst Center and Cisco ISE integration is not supported through a Catalyst Center virtual IP address (VIP). If you are using an enterprise CA-issued certificate for Catalyst Center, make sure the Catalyst Center certificate includes the IP addresses of all interfaces on Catalyst Center in the Subject Alternative Name (SAN) extension. If Catalyst Center is a three-node cluster, the IP addresses of all interfaces from all three nodes must be included in the SAN extension of the Catalyst Center certificate.
- You must have Admin-level access in Cisco ISE.
- Disable password expiry for the Admin user in Cisco ISE. Alternatively, make sure that you update the password before it expires. For more information, see the *Cisco Identity Services Engine Administrator Guide*.
- When the Cisco ISE certificate changes, Catalyst Center must be updated. To do that, edit the AAA server (Cisco ISE), reenter the password, and save. This forces Catalyst Center to download the certificate chain for the new admin certificate from Cisco ISE, and update Catalyst Center. If you are using Cisco ISE in HA mode, and the admin certificate changes on either the primary or secondary administrative node, you must update Catalyst Center.
- Catalyst Center configures certificates for itself and for Cisco ISE to connect over pxGrid. You can use other certificates with pxGrid for connections to other pxGrid clients, such as Firepower. These other connections do not interfere with the Catalyst Center and Cisco ISE pxGrid connection.
- You can change the RADIUS secret password. You provided the secret password when you configured Cisco ISE as a AAA server under **System** > **Settings** > **External Services** > **Authentication and Policy Servers**. To change the secret password, choose **Design** > **Network Settings** > **Network** and click the **Change Shared Secret** link. This causes Cisco ISE to use the new secret password when connecting to network devices managed by Catalyst Center.
- In distributed Cisco ISE clusters, each node performs only certain functions, such as PAN (Admin), MnT (Monitoring and Troubleshooting), or PSN (Policy Service). It is possible to have only Admin certificate usage on PAN nodes, and only EAP Authentication certificate usage on PSN nodes. However, this configuration prevents Catalyst Center and Cisco ISE integration for pxGrid. Therefore, we recommend that you enable EAP Authentication certificate usage on the Cisco ISE primary PAN node.
- To ensure that Catalyst Center recognizes a PSN after it's been upgraded, you must do the following:
  1. Readd the PAN that's associated with the PSN. In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure a Primary Policy Administration Node" topic.
  2. Reintegrate Cisco ISE with Catalyst Center. In the *Cisco Catalyst Center Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.
- Catalyst Center supports certificate revocation checks via CRL Distribution Point (CDP) and Online Certificate Status Protocol (OCSP). During integration, Catalyst Center receives the Cisco ISE admin certificate over port 9060 and verifies its validity based on the CDP and OCSP URLs inside that Cisco

ISE admin certificate. If both CDP (which contains a list of CRLs) and OCSP are configured, Catalyst Center uses OCSP to verify the revocation status of the certificate and falls back to CDP if the OCSP URL is not accessible. If there are multiple CRLs present in CDP, Catalyst Center contacts the next CRL if the first CRL is not reachable. However, due to a JDK PKI Oracle bug, the system does not check for all CRL entries.

Proxy is not supported for certificate verification. Catalyst Center contacts the CRL and OCSP servers without proxy.

- OCSP and CRL entries are optional in the certificate.
- LDAP is not supported as a protocol for certificate validation. Do not include LDAP URLs in CDP or AIA extensions.
- All URLs in CDP and OCSP must be reachable from Catalyst Center. Unreachable URLs can cause a poor integration experience, including a failed integration.

- The Cisco ISE certificates' subject name and issuer must adhere to ASN.1 PrintableString characters, where only spaces and the following characters are allowed: A – Z, a – z, 0 – 9, ‘ ( ) + , - . / : = ?

Anonymize data

Catalyst Center allows you to anonymize wired and wireless endpoints data. You can scramble personally identifiable data, such as the user ID, and device hostname of wired and wireless endpoints.

Ensure that you enable anonymization before you run Discovery. If you anonymize the data after you run Discovery, the new data coming into the system is anonymized, but the existing data isn’t anonymized.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Trust & Privacy** > **Anonymize Data**.

Step 2 In the **Anonymize Data** window, check the **Enable Anonymization** check box.

Step 3 Click **Save**.
After you enable anonymization, you can only search for the device using nonanonymized information such as the MAC address, IP address, and so on.

Configure authentication and policy servers

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

Before you begin

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

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

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

Before you configure Cisco ISE, confirm that:

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

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

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

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

  The PSNs that you configure in Cisco ISE to handle TrustSec or SD Access content and Protected Access Credentials (PACs) must also be defined in **Work Centers** > **Trustsec** > **Trustsec Servers** > **Trustsec AAA Servers**. For more information, see the *Cisco Identity Services Engine Administrator Guide*.
- You must enable communication between Catalyst Center and Cisco ISE on these ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Catalyst Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or the fully qualified domain name (FQDN) in either the certificate subject name or the Subject Alternative Name (SAN).
- The Catalyst Center system certificate must list both the Catalyst Center appliance IP address and FQDN in the SAN field.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**.

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

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

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

Note
Make sure that you do not configure a PSN that is part of an existing Cisco ISE cluster as a primary AAA server.

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

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

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

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

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

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

  hostname.domainname.com

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

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

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

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

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

  When you enable this option, ensure that:

  - The Catalyst Center certificate is generated by the same CA as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).

  - The Certificate Extended Key Use (EKU) field includes "Client Authentication."

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

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

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

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

- **Port**: TCP port used to communicate with the TACACS server. The default TCP port used for TACACS is 49.

- **Retries**: Number of times that Catalyst Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.

- **Timeout**: The time period for which the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

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

Cisco ISE server registration phase:

- **Authentication and Policy Servers** window: "In Progress"

- **System 360** window: "Primary Available"

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** window: "Active"

- **System 360** window: "Primary Available" and "pxGrid Available"

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

Step 6 Click **Add**.

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

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

a. From the main menu, choose **Provision** > **Inventory**.

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

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

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

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

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

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

Configure Cisco AI Network Analytics

Use this procedure to enable the Cisco AI Analytics features to export network event data from network devices and inventory, site hierarchy, and topology data to the Cisco AI Cloud.

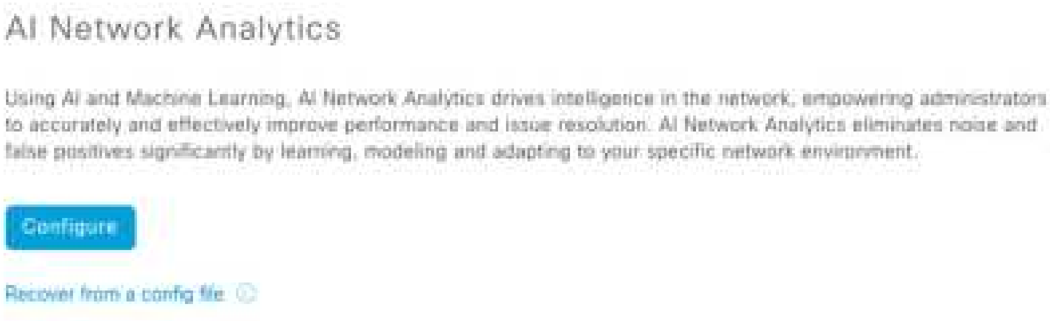
Before you begin

- Make sure that you have the Advantage software license for Catalyst Center. The **AI Network Analytics** application is part of the Advantage software license.
- Make sure that the latest version of the AI Network Analytics application is installed. See Download and install applications, on page 115.
- Make sure that your network or HTTP proxy is configured to allow outbound HTTPS (TCP 443) access to these cloud hosts:
  - **api.use1.prd.kairos.ciscolabs.com** (US East Region)
  - **api.euc1.prd.kairos.ciscolabs.com** (EU Central Region)

Procedure

Step 1 From the main menu, choose **System** > **Settings**.

Step 2 Scroll down to **External Services** and select **Cisco AI Analytics**.
The **AI Network Analytics** window opens.



AI Network Analytics

Using AI and Machine Learning, AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

Step 3 Do one of these tasks:

- If you have an earlier version of Cisco AI Network Analytics installed in your appliance, do these steps:
  a. Click **Recover from a config file**.

     The Restore AI Network Analytics window opens.

  b. Drag-and-drop the configuration files in the area provided or select the files from your file system.

c. Click **Restore**.

   Cisco AI Network Analytics might take a few minutes to restore, and then the **Success** dialog box opens.

- For the first-time configuration of Cisco AI Network Analytics, do these steps:

  a. Click **Configure**.

  b. In the **Where should we securely store your data?** area, select the location to store your data. Options are: **Europe (Germany)** or **US East (North Virginia)**.

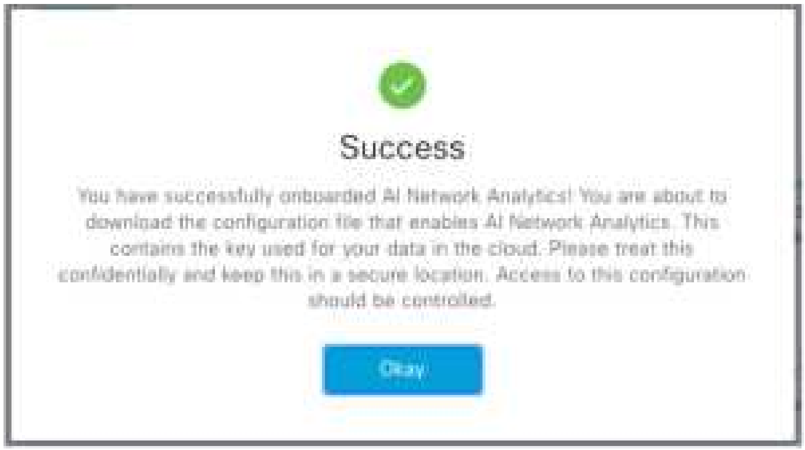
     The system starts testing cloud connectivity as indicated by the **Testing cloud connectivity...** tab. After cloud connectivity testing completes, the **Testing cloud connectivity...** tab changes to **Cloud connection verified**.

  c. Click **Next**.

     The terms and conditions window opens.

  d. Click the **Accept Cisco Universal Cloud Agreement** check box to agree to the terms and conditions, and then click **Enable**.

     Cisco AI Network Analytics might take a few minutes to enable, and then the **Success** dialog box opens.



Success

You have successfully onboarded AI Network Analytics! You are about to download the configuration file that enables AI Network Analytics. This contains the key used for your data in the cloud. Please treat this confidentially and keep this in a secure location. Access to this configuration should be controlled.

Step 4 In the **Success** dialog box, click **Okay**.
The **AI Network Analytics** window opens, and the **Enable AI Network Analytics** toggle button displays ☑.

Step 5 (Recommended) In the **AI Network Analytics** window, click **Download Configuration file**.

Client certificate renewal

AI agents use X.509 client certificates to authenticate to the AI Cloud. Certificates are created and signed by the AI Cloud CA upon tenant onboarding to the AI Cloud and remain valid for three years (reduced to one year in August 2021). Before their expiration, client certificates must be renewed to avoid losing cloud connectivity. An automatic certificate renewal mechanism is in place. This mechanism requires that you manually back up the certificate after renewal. The backup is required in case you restore or migrate to a new Catalyst Center.

After renewal, a notification is shown on every AI Analytics window (Peer Comparison, Heatmap, Network Comparison, Trends and Insights) to tell you to back up the new AI Network Analytics configuration.

Disable Cisco AI Network Analytics

To disable Cisco AI Network Analytics data collection, you must disable the AI Network Analytics feature:

Procedure

Step 1 From the main menu, choose **System** > **Settings**.

Step 2 Scroll down to **External Services** and choose **Cisco AI Analytics**.

For each feature, a check mark (☑) indicates that the feature is enabled. If the check box is unchecked (☒), the feature is disabled.

Step 3 In the **AI Network Analytics** area, click the **Enable AI Network Analytics** toggle button so that it's unchecked (☒).

Step 4 Click **Update**.

Step 5 To delete your network data from the Cisco AI Network Analytics cloud, contact the Cisco Technical Response Center (TAC) and open a support request.

Step 6 If you have misplaced your previous configuration, click **Download configuration file**.

Update the Machine Reasoning Knowledge Base

Machine Reasoning knowledge packs are step-by-step workflows that are used by the Machine Reasoning Engine (MRE) to identify security issues and improve automated root cause analysis. These knowledge packs are continuously updated as more information is received. The Machine Reasoning Knowledge Base is a repository of these knowledge packs (workflows). To have access to the latest knowledge packs, you can either configure Catalyst Center to automatically update the Machine Reasoning Knowledge Base daily, or you can do a manual update.

Procedure

Step 1 From the main menu, choose **System** > **Settings**.

Step 2 Scroll down to **External Services** and select **Machine Reasoning Knowledge Base**.
The **Machine Reasoning Knowledge Base** window shows this information:

- **INSTALLED**: Shows the installed version and installation date of the Machine Reasoning Knowledge Base package.

When there's a new update to the Machine Reasoning Knowledge Base, the **AVAILABLE UPDATE** area is displayed in the **Machine Reasoning Knowledge Base** window, which provides the **Version** and **Details** about the update.

- **AUTO UPDATE**: Automatically updates the Machine Reasoning Knowledge Base in Catalyst Center daily.

- **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER, SECURITY ADVISORY, FIELD NOTICES AND EOX**: Integrates Catalyst Center with CX Cloud that allows you to perform an automated config. This integration provides enhanced vulnerability detection on devices directly from the security advisories tool on Catalyst Center.

Step 3 (Recommended) Check the **AUTO UPDATE** check box to automatically update the Machine Reasoning Knowledge Base.
The **Next Attempt** area shows the date and time of the next update.

You can perform an automatic update only if Catalyst Center is successfully connected to the Machine Reasoning Engine in the cloud.

Step 4 To manually update the Machine Reasoning Knowledge Base in Catalyst Center, do one of these tasks:

- Under **AVAILABLE UPDATES**, click **Update**. A **Success** pop-up window appears with the status of the update.
- Manually download the Machine Reason Knowledge Base to your local machine and import it to Catalyst Center. Do these steps:

  a. Click **Download**.

  The **Opening mre_workflow_signed** dialog box appears.

  b. Open or save the downloaded file to the desired location in your local machine, and then click **OK**.

  c. Click **Import** to import the downloaded Machine Reasoning Knowledge Base from your local machine to Catalyst Center.

Step 5 Check the **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY** check box to enable Cisco CX Cloud connection with network bug identifier and security advisory.

Step 6 In the **Security Advisories Settings** area click the **RECURRING SCAN** toggle button to enable or disable the weekly recurring scan.

Step 7 Click the **CISCO CX CLOUD** toggle button to enable or disable the Cisco CX cloud.

Configure Cisco credentials

Complete this procedure to configure the credentials Catalyst Center uses for software image and update downloads. These credentials are the username and password that you use to log in to the Cisco website

Important

- Cisco has implemented a new authentication infrastructure. As a result, if you back up data from Catalyst Center Release 2.3.7.7, where a Cisco.com user was configured, and restore the data in Catalyst Center Release 3.1.3, you must reauthenticate that user.
- Catalyst Center no longer stores the Cisco.com user's credentials locally, for security purposes.

Before you begin

Only users with SUPER-ADMIN-ROLE permissions or CUSTOM-ROLE with "Write" permission to System Settings can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **Cisco.com Credentials**.

Step 2 Configure the Cisco.com user:

a) Open an Incognito/private window in your browser (to avoid using previously cached credentials).
b) Open another Catalyst Center GUI instance and log in.
c) Open another instance of the **Cisco.com Credentials** window.
d) In the **Cisco.com ID** field, click the **Add** link.
e) In the **Information** pop-up window, check the **I am in private or incognito mode** check box and then click **Proceed**.
f) In the **Activate your device** pop-up window, confirm that an activation code is displayed and then click **Next**.
g) In the **Log in** pop-up window, enter the cisco.com user's email address and then click **Next**.
h) In the **Verify with your password** pop-up window, enter the cisco.com user's password and then click **Verify**.

The **Device activated** pop-up window appears.

Step 3 Confirm that the user was configured successfully.

a) Close the **Device Activated** pop-up window.
b) Refresh the **Cisco.com Credentials** page.
c) In the **Cisco.com ID** field, confirm that the email address you entered for the user is displayed. Also confirm that you see both the **Change** and **Delete** links.

Clear Cisco credentials

To delete the cisco.com credentials that are currently configured for Catalyst Center, complete this procedure.

Note

- When you perform any tasks that involve software downloads or device provisioning and cisco.com credentials are not configured, you'll be prompted to enter them before you can proceed. In the resulting dialog box, check the **Save For Later** check box in order to save these credentials for use throughout Catalyst Center. Otherwise, you'll need to enter credentials each time you perform these tasks.
- Completing this procedure will undo your acceptance of the end-user license agreement (EULA). See Accept the license agreement, on page 56 for a description of how to reenter EULA acceptance.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions or CUSTOM-ROLE with "Write" permission to System Settings can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **Cisco.com Credentials**.

Step 2 Click the **Delete** link.

Step 3 In the resulting dialog box, click **Delete** to confirm the operation.

Configure connection mode

Connection mode manages the connections between smart-enabled devices in your network that interact with Catalyst Center and the Cisco Smart Software Manager (SSM). Ensure that you have SUPER-ADMIN access permission to configure the different connection modes.

The SSL certificate for the SSM must include the associated IP address within the SAN field.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **SSM Connection Mode**.

Connection modes include:

- **Direct**
- **On-Prem CSSM**
- **Smart proxy**

Step 2 Choose **Direct** to enable a direct connection to the Cisco SSM cloud.

Step 3 If your organization is security sensitive, choose **On-Prem CSSM**. The on-prem option lets you access a subset of Cisco SSM functionality without using a direct internet connection to manage your licenses with the Cisco SSM cloud.

a) Before you enable **On-Prem CSSM**, confirm that the satellite is deployed, up, and running in your network site.

If the satellite is configured with FQDN, the call-home configuration of satellite FQDN is pushed instead of the IP address.

b) Enter the details for the **On-Prem CSSM Host**, **Smart Account name**, **Client ID**, and **Client Secret**.

In the Smart Account field, enter the name of one SSM on-prem account only. Do not use a space or an underscore in the name.

For information about how to retrieve the client ID and client secret, see the *Cisco Smart Software Manager On-Prem User Guide*.

c) Click **Test Connection** to validate the Cisco SSM connection.

d) Click **Save** and then **Confirm**.

e) If there are devices that need to be registered again with the changed SSM, the **Need to Re-Register Devices** dialog box appears. Click **OK** in the dialog box.

f) In the **Tools** > **License Manager** > **Devices** window, choose the devices that you want to register again and click **Sync Connection Mode**.

Note
Such devices display the **Connection Mode out of sync** tag or message.

g) In the **Resync Devices** dialog box:

- Enter the **Smart Account**.
- Enter the **Virtual Account**.
- Click **Now** to start the resync immediately or click **Later** to schedule the resync at a specific time.
- Click **Resync**.

The **Recent Tasks** window shows the resync status of the devices.

Step 4 Choose **Smart proxy** to register your smart-enabled devices with the Cisco SSM cloud through Catalyst Center. With this mode, devices do not need a direct connection to the Cisco SSM cloud. Catalyst Center proxies the requests from the device to the Cisco SSM cloud through itself.

While provisioning the call-home configuration to the device, if the satellite is configured with FQDN, the FQDN of the satellite is pushed instead of the IP address.

Register Plug and Play

You can register Catalyst Center as a controller for Cisco Plug and Play (PnP) Connect, in a Cisco Smart Account for redirection services. This lets you synchronize the device inventory from the Cisco PnP Connect cloud portal to PnP in Catalyst Center.

Before you begin

Only a user with **SUPER-ADMIN-ROLE** or **CUSTOM-ROLE** with system management permissions can perform this procedure.

In the Smart account, users are assigned roles that specify the functions and authorized to perform:

- Smart Account Admin user can access all the Virtual Accounts.
- Users can access assigned Virtual Accounts only.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **PnP Connect**.

A table of PnP connected profiles is displayed.

Step 2 If you have already configured the Cisco.com user, skip ahead to Step 3. If you haven't, complete these steps:

a) Open an Incognito/private window in your browser (to avoid using previously cached credentials).
b) Open another Catalyst Center GUI instance and log in.
c) Open another instance of the **PnP Connect** window.
d) In the **Cisco.com ID** field, click the **Add** link.
e) In the **Information** pop-up window, check one or both of these check boxes and then click **Authenticate**:

- Mandatory: **I am in private or incognito mode**
- Optional: **Save credentials**

f) In the **Activate your device** pop-up window, confirm that an activation code is displayed and then click **Next**.
g) In the **Log in** pop-up window, enter the cisco.com user's email address and then click **Next**.
h) In the **Verify with your password** pop-up window, enter the cisco.com user's password and then click **Verify**.

   The **Device activated** pop-up window appears.

i) Close the **Device Activated** pop-up window.
j) Refresh the **PnP Connect** window.
k) In the **Cisco.com ID** field, confirm that the email address you entered for the user is displayed. Also confirm that you see the **Change** link.

Step 3 Click **Register** to register a virtual account.

Step 4 In the **Register Virtual Account** window, the Smart Account you configured is displayed in the **Select Smart Account** drop-down list. You can select an account from the **Select Virtual Account** drop-down list.

Step 5 Click the required **IP** or **FQDN** radio button.

Step 6 Enter the IP address or FQDN (Fully Qualified Domain Name) of the controller.

Step 7 Enter the profile name. A profile is created for the selected virtual account with the configuration that you provided.

Step 8 Check the **Use as Default Controller Profile** check box to register this Catalyst Center controller as the default controller in the Cisco PnP Connect cloud portal.

Step 9 Click **Register**.

Create PnP event notifications

You receive a notification whenever a Plug and Play (PnP) event takes place in Catalyst Center by creating event notifications. See the "Work with Event Notifications" topic in the *Cisco Catalyst Center Platform User Guide* to configure the supported channels and create event notifications.

Ensure that you create event notifications for these PnP events:

Event name	Event ID	Description
Add device failed	NETWORK-TASK_FAILURE-3-008	Device(s) are not added through single or bulk import. An error occurs when adding devices through single or bulk import.
Add device successful	NETWORK-TASK_COMPLETE-4-007	Device(s) are added through single or bulk import successfully.
Device in error state	NETWORK-ERROR_1-002	Device goes to **Error** state.
Device in provisioned state	NETWORK-INFO_4-003	Device goes to **Provisioned** state.
Device stuck in onboarding state	NETWORK-TASK_PROGRESS-2-006	Device is stuck in onboarding state for more than 15 minutes.
Device waiting to be claimed	NETWORK-INFO_2-001	Device reaches **Unclaimed** state and is ready to be provisioned.
Smart Account sync failed	NETWORK-TASK_FAILURE-1-005	Smart Account sync is failed for some devices.

Event name	Event ID	Description
Smart Account sync successful	NETWORK-TASK_COMPLETE-4-004	Smart Account sync is successful for some devices.

Configure Smart Account

Cisco Smart Account credentials are used for connecting to your Smart Licensing account. The License Manager tool uses the details of license information from this Smart Account for entitlement and license management.

Important Cisco has implemented a new authentication infrastructure. As a result, if you back up data from Catalyst Center Release 2.3.7.7, where Smart Account credentials were configured, and restore the data in Catalyst Center Release 3.1.3, you must reauthenticate the associated Smart Accounts.

Before you begin

Ensure that you have SUPER-ADMIN-ROLE permissions or CUSTOM-ROLE with "Write" permission to System Settings.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **Smart Account**.

Step 2 Link the appropriate Smart Account user and Smart Account name to your Smart Licensing account:

a) Open an Incognito/private window in your browser (to avoid using previously cached credentials).
b) Open another Catalyst Center GUI instance and log in.
c) Open another instance of the **Smart Account** window.
d) Click the **Add** link.
e) In the **Information** pop-up window, check the **I am in private or incognito mode** check box and then click **Proceed**.
f) In the **Activate your device** pop-up window, confirm that an activation code is displayed and then click **Next**.
g) In the **Log in** pop-up window, enter the cisco.com user's email address and then click **Next**.
h) In the **Verify with your password** pop-up window, enter the cisco.com user's password and then click **Verify**.

The **Device activated** pop-up window appears.

i) Confirm whether the Smart Account user you just added is listed in both the **Smart Account Credentials** and **Expired Smart Accounts** sections:

If the Smart Account user...	Then...
is listed in both sections,	delete the user from the **Expired Smart Accounts** section by clicking their trash icon in the **Actions** column.
is *not* listed in both sections,	proceed to Step 3.

Step 3 If you want to change the selected Smart Account Name, click **Change**. You will be prompted to select the Smart Account that will be used for connecting to your Smart Licensing Account on Cisco SSM cloud.

a) Choose the **Smart Account** from the drop-down list.

b) Click **Save**.

Step 4 Click **View all virtual accounts** to view all the virtual accounts associated with the Smart Account.

Note
Cisco Accounts supports multiple smart and virtual accounts.

Step 5 (Optional) If you want to register smart license-enabled devices automatically to a virtual account, check the **Auto register smart license enabled devices** check box. A list of virtual accounts associated with the smart account is displayed.

Step 6 Select the required virtual account. Whenever a smart license-enabled device is added in the inventory, it's automatically registered to the selected virtual account.

Step 7 If you want to remove the licensed smart account users and their associated historical data, click **Delete historical information**.

The **Delete Historical Data** slide-in pane displays the licensed smart account users. It also displays the existing smart accounts that aren't currently present in Catalyst Center, but their historical data is still available.

Step 8 In the **Smart Account list** area check the check box next to the smart account that you want to delete.

Step 9 Click **Delete**.

Step 10 Click **Delete** in the subsequent confirmation window.

Step 11 Check the **Delete the associated license historical information** check box to delete the historical information of the associated license.

Smart Licensing

Cisco Smart licensing allows you to register Catalyst Center on to the Cisco SSM.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco licensing, go to cisco.com/go/licensingguide.

Note Smart license registration for a Catalyst Center instance is supported using these connection modes:

- Direct
- On-Prem Cisco SSM, and
- Smart proxy.

Before you begin

- To enable Smart Licensing, you must configure Cisco Credentials (see Configure Cisco credentials, on page 46) and upload Catalyst Center license conventions in Cisco SSM.

- To enable Smart Licensing, you must add a Smart Account in **System** > **Settings** > **Cisco Accounts** > **Smart Account**. For more information, see Configure Smart Account, on page 51.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **Smart Licensing**.

By default, **Smart Account** details are displayed.

Step 2 Choose a virtual account from the **Search Virtual Account** drop-down list to register.

Step 3 Click **Register**.

Step 4 After successful registration, click the **View Available Licenses** link to view the available Catalyst Center licenses.

Device controllability

Device controllability is a system-level process on Catalyst Center that enforces state synchronization for some device-layer features. Its purpose is to aid in the deployment of network settings that Catalyst Center needs to manage devices. Changes are made on network devices when running discovery, when adding a device to inventory, or when assigning a device to a site.

To view the configuration that is pushed to the device, go to **Provision** > **Inventory** and from the **Focus** drop-down list, choose **Provision**. In the **Provision Status** column, click **See Details**.

Note When Catalyst Center configures or updates devices, the transactions are captured in the audit logs, which you can use to track changes and troubleshoot issues.

Device settings enabled as part of device controllability include:

- **Device Discovery**
  - SNMP Credentials
  - NETCONF Credentials
- **Adding Devices to Inventory**

  Cisco TrustSec (CTS) Credentials

  Note Cisco TrustSec (CTS) Credentials are pushed during inventory only if the **Global** site is configured with Cisco ISE as AAA. Otherwise, CTS is pushed to devices during "Assign to Site" when the site is configured with Cisco ISE as AAA.

- **Assigning Devices to a Site**
  - Controller Certificates

Note For Cisco IOS devices, we recommend that you configure the time zone from the device UI console to prevent any issues in the processing of PKCS certificate expiry time.

- SNMP Trap Server Definitions
- Syslog Server Definitions
- NetFlow Server Definitions
- Wireless Service Assurance (WSA)
- IPDT Enablement

Device controllability is enabled by default. If you do not want device controllability enabled, disable it manually. For more information, see Configure device controllability, on page 55.

When device controllability is disabled, Catalyst Center does not configure any of the preceding credentials or features on devices while running discovery or when the devices are assigned to a site.

Circumstances that dictate whether or not device controllability configures network settings on devices include:

- **Device Discovery**: If SNMP and NETCONF credentials are not already present on a device, these settings are configured during the discovery process.

- **Device in Inventory**: After a successful initial inventory collection, IPDT is configured on the devices.

  In earlier releases, the following IPDT commands were configured:

  ```
  ip device tracking
  ip device tracking probe delay 60
  ip device tracking probe use-svi
  ```

  For each interface:

  ```
  interface $physicalInterface
  ip device tracking maximum 65535
  ```

  In the current release, the following IPDT commands are configured for any newly discovered device:

  ```
  device-tracking tracking
  device-tracking policy IPDT_POLICY
  tracking enable
  ```

  For each interface:

  ```
  interface $physicalInterface
  device-tracking attach-policy IPDT_POLICY
  ```

- **Device in Global Site**: When you successfully add, import, or discover a device, Catalyst Center places the device in the **Managed** state and assigns it to the **Global** site by default. Even if you have defined SNMP server, Syslog server, and NetFlow collector settings for the **Global** site, Catalyst Center *does not* change these settings on the device.

- **Device Moved to Site**: If you move a device from the **Global** site to a new site that has SNMP server, Syslog server, and NetFlow collector settings configured, Catalyst Center changes these settings on the device to the settings configured for the new site.

- **Device Removed from Site**: If you remove a device from a site, Catalyst Center does not remove the SNMP server, Syslog server, and NetFlow collector settings from the device.
- **Device Deleted from Catalyst Center**: If you delete a device from Catalyst Center and check the **Configuration Clean-up** check box, the SNMP server, Syslog server, and NetFlow collector settings are removed from the device.
- **Device Moved from Site to Site**: If you move a device—for example, from Site A to Site B—Catalyst Center replaces the SNMP server, Syslog server, and NetFlow collector settings on the device with the settings assigned to Site B.
- **Update Site Telemetry Changes**: The changes made to any settings that are under the scope of device controllability are applied to the network devices during device provisioning or when the **Update Telemetry Settings** action is performed.

When device controllability is enabled, if Catalyst Center can't connect to the device through the user-provided SNMP credentials and collect device information, Catalyst Center pushes the user-provided SNMP credentials to the device. For SNMPv3, the user is created under the *default* group.

Note For Cisco AireOS devices, the user-provided SNMPv3 passphrase must contain from 12 to 31 characters.

Configure device controllability

Device controllability deploys the required network settings that Catalyst Center needs to manage devices. Device controllability is enabled by default.

To manually disable device controllability, use this procedure.

Note If you disable device controllability, Catalyst Center doesn't automatically configure discovered devices with essential settings, including SNMP credentials, trap servers, IP Device Tracking (IPDT), NetFlow, Syslog, and NETCONF.

If you assign a device to a site after disabling device controllability, Catalyst Center doesn't support out-of-band configuration change notifications and management of APs, because Catalyst Center is no longer registered as a trap receiver on the device.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **Device Controllability**.

Step 2 Uncheck the **Enable Device Controllability** check box.

Step 3 To prevent Catalyst Center from automatically correcting any issues identified in device telemetry configuration, leave the **Enable autocorrect telemetry config** check box unchecked.

By default, this check box is disabled. You can only enable it when device controllability is enabled.

Step 4 Click **Save**.

Accept the license agreement

You must accept the end-user license agreement (EULA) before you download software or provision a device.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **Device EULA Acceptance**.

Step 2 If you have already configured the Cisco.com user, skip ahead to Step 3. If you haven't, complete these steps:

a) Open an Incognito/private window in your browser (to avoid using previously cached credentials).
b) Open another Catalyst Center GUI instance and log in.
c) Open another instance of the **Device EULA Acceptance** window. From the main menu, choose **System** > **Settings** > **Device Settings** > **Device EULA Acceptance**.
d) In the **Cisco.com ID** field, click the **Add** link.
e) In the **Information** pop-up window, check the **I am in private or incognito mode** check box and then click **Proceed**.
f) In the **Activate your device** pop-up window, confirm that an activation code is displayed and then click **Next**.
g) In the **Log in** pop-up window, enter the cisco.com user's email address and then click **Next**.
h) In the **Verify with your password** pop-up window, enter the cisco.com user's password and then click **Verify**.

   The **Device activated** pop-up window appears.

i) Close the **Device Activated** pop-up window.
j) Refresh the **Device EULA Acceptance** window.
k) In the **Cisco.com ID** field, confirm that the email address you entered for the user is displayed. Also confirm that you see the **Change** link.

Step 3 Open the **Cisco End User License Agreement Supplemental Product Terms** link in a new browser tab.

Step 4 Open and read the Catalyst Center EULA.

Step 5 Check the **I have read and accept the Device EULA** check box.

Step 6 Click **Save**.

Configure SNMP properties

You can configure retry and timeout values for SNMP.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **SNMP**.

Step 2 Configure these fields:

- **Retries**: Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.
- **Timeout**: Number of seconds Catalyst Center waits when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds in intervals of 5 seconds. The default is 5 seconds.

Step 3 Click **Save**.

Step 4 (Optional) To return to the default settings, click **Reset** and **Save**.

Enable ICMP ping

When Internet Control Message Protocol (ICMP) ping is enabled and there are unreachable access points in FlexConnect mode, Catalyst Center uses ICMP to ping these access points every 5 minutes to enhance reachability.

To enable an ICMP ping:

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **ICMP Ping**.

Step 2 Check the **Enable ICMP ping for unreachable access points in FlexConnect mode** check box.

Step 3 Click **Save**.

Configure AP location for PnP onboarding

Catalyst Center allows you to use the site assigned during the PnP claim as the AP location for PnP onboarding. If you check the **Configure AP Location** check box, Catalyst Center configures the assigned site as the AP location for PnP onboarding. If you uncheck this check box, use the **Configure Access Points** workflow to configure the AP location for PnP onboarding. For more information, see "AP Configuration in Catalyst Center" in the *Catalyst Center User Guide*.

Note These settings aren't applicable during the day-*n* operations. To configure the AP location for day-*n* operations, you can use the **Configure Access Points** workflow.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **PnP AP Location**.

Step 2 Check the **Configure AP Location** check box.

Step 3 Click **Save**.

Configure an image distribution server

An image distribution server helps in the storage and distribution of software images. You can configure up to three external image distribution servers to distribute software images. You can also set up one or more protocols for the newly added image distribution servers.

For information about the supported servers, see the "Server Requirements for Automation Data Backup" section in Backup server requirements, on page 173.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **Image Distribution Servers**.

Step 2 In the **Image Distribution Servers** window, click **Servers**.

The table displays details about the host, username, SFTP, SCP, and connectivity of image distribution servers.

Step 3 Click **Add** to add a new image distribution server.

The **Add a New Image Distribution Server** slide-in pane is displayed.

Step 4 Configure these image distribution server settings:

- **Host**: Enter the hostname or IP address of the image distribution server.
- **Root Location**: Enter the working root directory for file transfers.

  Note
  For Cisco AireOS Wireless Controllers, image distribution fails if the configured path is longer than 16 characters.
- **Username**: Enter a username to log in to the image distribution server. The username must have read/write privileges in the working root directory of the server.
- **Password**: Enter a password to log in to the image distribution server.
- **Port Number**: Enter the port number on which the image distribution server is running.

Step 5 Click **Save**.

Step 6 Because some legacy wireless controller software versions support only weak ciphers (such as SHA1-based ciphers) for SFTP, Catalyst Center should enable SFTP compatibility mode for SFTP connections from wireless controllers for software image management and wireless assurance. You can temporarily enable support for weak ciphers on the Catalyst Center SFTP server for up to 90 days. To allow weak ciphers:

a) Hover over the **i** icon next to the IP address of the SFTP server and click **Click here**.
b) In the **Compatibility Mode** slide-in pane, check the **Compatibility Mode** check box and enter a duration (from 1 minute to 90 days).
c) Click **Save**.

Step 7 (Optional) To edit the settings, click the **Edit** icon next to the corresponding image distribution server, make the required changes, and click **Save**.

Step 8 (Optional) To delete an image distribution server, click the **Delete** icon next to the corresponding image distribution server and click **Delete**.

Enable PnP device authorization

To enable authorization on a device:

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings**.

Step 2 From the **Device Settings** drop-down list, choose **PnP Device Authorization**.

Note
By default, devices are automatically authorized.

Step 3 Check the **Device Authorization** check box to enable authorization on the device.

Step 4 Click **Save**.

Configure device prompts

Catalyst Center allows you to create custom prompts for the username and password. You can configure the devices in your network to use custom prompts and collect information about the devices.

Create custom prompts

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **Device Prompts**.

The **Device Prompts** window opens.

Step 2 Click **Create Custom Prompt**.

The **Create Custom Prompt** slide-in pane opens.

Step 3 To create custom prompts for the username:

a. From the **Prompt Type** drop-down list, choose **username**.

b. In the **Prompt Text** field, enter the text in Regular Expression (Regex).

c. Click **Save**.

Step 4 To create custom prompts for the password,:

a. From the **Prompt Type** drop-down list, choose **password**.

b. In the **Prompt Text** field, enter the text in Regular Expression (Regex).

c. Click **Save**.

Note
The custom prompts are displayed in the **Device Prompts** window. You can create up to eight custom prompts for the username and password.

Step 5 Drag and drop the custom prompts in the order that you want.

Note
Catalyst Center maintains the order of the custom prompts and passes the prompts to the devices as comma-separated values. The custom prompt in the top order gets higher priority.

Step 6 Click the edit icon to edit a custom prompt.

Step 7 Click the delete icon to delete a custom prompt.

Note
Username prompts and password prompts must have unique Regex. Creating the same or similar Regex causes authentication issues with the devices.

Configure device configuration backup settings

Catalyst Center performs periodic backup of your device running configuration. You can choose the day and time for the backup and the total number of config drifts that can be saved per device.

Note

- Daily Backup: Catalyst Center performs an automated configuration backup that is scheduled to run every day at 11:00 p.m. (UTC time zone). During this process, Catalyst Center compares the timestamp of the last device configuration collection with the timestamp of the device configuration archived. If the difference is more than 30 minutes, the device configuration archive will be performed.

  Daily backup is not performed on the day when weekly backup is scheduled.

- Weekly Backup: Catalyst Center performs an automated configuration backup, that is scheduled to run every Sunday at 11:30 p.m. (UTC time zone).

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Configuration Archive**.

Step 2 In the **Configuration Archive** window, click the **Internal** tab.

Step 3 Click the **Number of config drift per device** drop-down list and choose the number of config drifts to save per device.

You can save 7–50 config drifts per device. The total config drifts to save include all the labeled configs for the device.

Note
By default, the number of config drifts to save per device is 15.

Step 4 Choose the backup day and time.

The selected backup date and time is based on the time zone of the Catalyst Center cluster deployed for your network.

Step 5 Click **Save**.

After the backup is scheduled, you can view it in the activity center.

Step 6 Click the **External** tab to configure an external server for archiving the device configuration. For more information, see Configure an external server for archiving device configuration, on page 61.

Configure an external server for archiving device configuration

You can configure an external SFTP server for archiving the running configuration of devices.

For information about the supported servers, see the "Server Requirements for Automation Data Backup" section in Backup server requirements, on page 173.

Before you begin

Confirm that SSH, SFTP, and SCP are enabled on the external server.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Configuration Archive**.

Step 2 In the **Configuration Archive** window, click the **External** tab.

Step 3 Click **Add** to add an **External Repository**.

Note
Only one SFTP server can be added.

Step 4 In the **Add New External Repository** slide-in pane, complete the following details:

a) **Host**: Enter the host IP address.

b) **Root Location**: Enter the location of the root folder.

Note

- Ensure the root location path is absolute and not relative.
- The external server root location must be empty.

c) **Server Protocol**: Enter the username, password, and port number of the SFTP server.

d) Choose the **Backup Format**:

- **RAW**: A full running configuration will be disclosed. All sensitive/private configurations are unmasked in the backup data. Enter a password to lock the backup file.

  Note
  File passwords are not saved on Catalyst Center. You must remember the password to access the files on the SFTP server.

- **Sanitized (Masked)**: The sensitive/private configuration details in the running configuration will be masked.

  The password is applicable only when the raw backup format is selected.

e) Schedule the backup cycle.

Enter the backup date, time, time zone, and recurrence interval.

Step 5 Click **Save**.

Step 6 To edit the SFTP server details, click the edit button under the **Action** column.

Step 7 To remove the SFTP server, click the delete button under the **Action** column.

Cloud access keys

You can register cloud access keys after installing the Cloud Device Provisioning Application package in Catalyst Center. The system supports multiple cloud access keys. Each key is used as a separate cloud profile that contains all the AWS infrastructure constructs or resources that are discovered by using that cloud access key. After a cloud access key is added, an AWS VPC inventory collection is triggered automatically for it. The AWS infrastructure constructs resources that get discovered by VPC inventory collection for that cloud access key that can then be viewed and used for cloud provisioning of CSRs and wireless controllers.

Before you begin

- Obtain the access key ID and secret key from the Amazon Web Services (AWS) console.
- Subscribe to CSR or wireless controller products in the AWS marketplace and verify the image ID for the target region.
- Identify the key pair that CSRs will use during HA failover on AWS. The key pair's name is selected from a list in Catalyst Center when provisioning CSRs in that region.
- Identify the IAM role that CSRs will use during HA failover on AWS. The IAM role is selected from a list in Catalyst Center when provisioning CSRs.
- Configure the proxy for Catalyst Center to communicate with AWS via HTTPS REST APIs. See Configure the proxy, on page 84.

- The Cloud Connect extension to the eNFV app is enabled by deploying a separate Cloud Device Provisioning Application package. The package is not included by default in the standard Catalyst Center installation. You must download and install the package from a catalog server. For more information, see Download and install applications, on page 115.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Cloud Access Keys**.

Step 2 Click **Add**.

Step 3 Enter the **Access Key Name** and choose the **Cloud Platform** from the drop-down list. Enter the **Access Key ID** and **Secret Key** obtained from the AWS console.

Step 4 Click **Save and Discover**.

What to do next

- After a cloud access key is added, an AWS VPC inventory collection is triggered automatically for it. It takes several minutes to synchronize with the cloud platform. Inventory collection is scheduled to occur at the default interval.
- After successful cloud inventory collection, the **Cloud** tab in the **Provision** section provides a view of the collected AWS VPC inventory.

Integrity Verification

Integrity Verification (IV) monitors key device data for unexpected changes or invalid values that indicate possible compromise, if any of the devices are at risk. It does this by comparing each device's software, hardware, platform, and configuration settings against an authoritative set of Known Good Values (KGV) for these settings for all supported Cisco devices. The objective is to minimize the impact of a compromise by substantially reducing the time to detect unauthorized changes to a Cisco device.

Note IV runs integrity verification checks on software images that are uploaded into Catalyst Center. To run these checks, the IV service needs the Known Good Value (KGV) file to be uploaded.

Upload the KGV file

To provide security integrity, Cisco devices must be verified as running authentic and valid software. Currently, Cisco devices have no point of reference to determine whether they are running authentic Cisco software. IV uses a system to compare the collected image integrity data with the KGV for Cisco software.

Cisco produces and publishes a KGV data file that contains KGVs for many of its products. This KGV file is in standard JSON format, is signed by Cisco, and is bundled with other files into a single KGV file that can be retrieved from the Cisco website. The KGV file is posted at:

https://tools.cisco.com/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar

The KGV file is imported into IV and used to verify integrity measurements obtained from the network devices.

Note Device integrity measurements are made available to and used entirely within the IV. Connectivity between IV and cisco.com is not required. The KGV file can be air-gap transferred into a protected environment and loaded into the IV.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Integrity Verification**.

Step 2 Review the current KGV file information:

- **File Name**: Name of the KGV tar file.
- **Imported By**: Catalyst Center user who imported the KGV file. If it is automatically downloaded, the value is **System**.
- **Imported Time**: Time at which the KGV file is imported.
- **Imported Mode**: Local or remote import mode.
- **Records**: Records processed.
- **File Hash**: File hash for the KGV file.
- **Published**: Publication date of the KGV file.

Step 3 To import the KGV file, do one of these steps:

- Click **Import New from Local** to import a KGV file locally.
- Click **Import Latest from Cisco** to import a KGV file from cisco.com.

Note
The **Import Latest from Cisco** option does not require a firewall setup. However, if a firewall is already set up, only the connections to https://tools.cisco.com must be open.

Step 4 If you clicked **Import Latest from Cisco**, a connection is made to cisco.com and the latest KGV file is automatically imported to Catalyst Center.

Note
A secure connection to https://tools.cisco.com is made using the certificates added to Catalyst Center and its proxy (if one was configured during the first-time setup).

Step 5 If you clicked **Import New from Local**, the **Import KGV** window appears.

Step 6 Do one of these procedures to import locally:

- Drag and drop a local KGV file into the **Import KGV** field.
- Click **Click here to select a KGV file from your computer** to select a KGV file from a folder on your computer.
- Click the **Latest KGV file** link and download the latest KGV file before dragging and dropping it into the **Import KGV** field.

Step 7 Click **Import**.

The KGV file is imported into Catalyst Center.

Step 8 After the import is finished, verify the current KGV file information in the GUI to ensure that it has been updated.

IV automatically downloads the latest KGV file from cisco.com to your system 7 days after Catalyst Center is deployed. The auto downloads continue every 7 days. You can also download the KGV file manually to your local system and then import it to Catalyst Center. For example, if a new KGV file is available on a Friday and the auto download is every 7 days (on a Monday), you can download it manually.

The KGV auto download information that displays includes:

- **Frequency**: The frequency of the auto download.
- **Last Attempt**: The last time the KGV scheduler was triggered.
- **Status**: The status of the KGV scheduler's last attempt.
- **Message**: A status message.

Note
When you import the latest KGV file, if there is any error, an error message displays. These error messages are now translated into multiple languages.

What to do next

After importing the latest KGV file, choose **Design** > **Image Repository** to view the integrity of the imported images.

Note The effect of importing a KGV file can be seen in the **Image Repository** window, if the images that are already imported have an **Unable to verify** status (physical or virtual). Additionally, future image imports, if any, will also refer to the newly uploaded KGV for verification.

Update the KGV bundle

Catalyst Center allows you to cancel or clear all stale or stuck IV workflows and initiate a new workflow. This feature is asynchronous in nature because it takes some time for the functionality to come into effect.

With the IV KGV file download workflow, you trigger the latest KGV download directly from cisco.com, or you manually upload a new KGV. In addition, a scheduler runs daily to download or update the latest KGV bundle from cisco.com.

If a scheduler IV workflow or a user-triggered IV workflow gets stuck during the KGV file download or during another phase, you cannot submit a new request. Only one IV KGV workflow is allowed at a time.

There is no option for you to submit a new request, other than raising a service request and doing a service restart. To overcome this issue, Catalyst Center has introduced a new API that allows you to cancel any stale or stuck IV workflow, clear the task entry associated with the canceled IV workflow, and reset the locking mechanism, which prevents a simultaneous request to submit a new IV workflow request.

Note This cancellation function:

- Applies only if you choose **Import Latest From Cisco** while importing the KGV file.
- Works only for stale workflows, not for other scenarios.

Cisco SD-Access Compatibility Matrix

Catalyst Center periodically compares the operational SD-Access fabric nodes hardware and software attributes against information in the *Cisco SD-Access Compatibility Matrix*.

Any compatibility issues that are detected will be aggregated and displayed in the SD-Access Compliance state of each fabric site. The fabric site's aggregate Compliance state can be reviewed from the **Provision** > **SD-Access** > **Fabric Sites** window.

To import or download the latest SD-Access compatibility matrix information:

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **SD-Access Compatibility Matrix**.

The **SD-Access Compatibility Matrix** window displays the information of the compatibility matrix that was last imported.

Note
Catalyst Center runs an autodownload for SD-Access compatibility matrix information that is scheduled to run once everyday.

The date and time of the autodownload is also displayed in the **SD-Access Compatibility Matrix** window.

Step 2 To manually import the SD-Access compatibility matrix file, click the **Import Latest From Cisco** hyperlink.

Note
A banner is displayed at the top of the **SD-Access Compatibility Matrix** window if the latest version of the file already exists.

Step 3 For air-gapped deployments, the ability to import the SD-Access compatibility matrix file from Cisco is not possible, so Catalyst Center provides the following upload process:

a. Download the SD-Access compatibility matrix file from *Cisco SD-Access Compatibility Matrix* for your device role and Catalyst Center package version.

Note
You should not make any changes to the downloaded JSON file.

b. Click the **Import New From Local** hyperlink and do one of the following:

- Click **Choose a file** to import the file.
- Drag and drop the JSON file to the drag and drop area.

Note
The file size cannot exceed 10 MB.

Disable SD-Access image compatibility checks

Catalyst Center 2.3.7.5 and later releases give you the option to disable SD-Access image compatibility checks.

Note Always enable SD-Access image compatibility checks to ensure proper network operations.

To disable the SD-Access image compatibility checks:

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **SD-Access Compatibility Matrix**.

Step 2 On the **SD-Access Compatibility Matrix** window, click the **SD-Access Image Compatibility Checks** toggle button so that it is unchecked.

Configure an IP address manager

You can configure Catalyst Center to communicate with an external IP address manager (IPAM). When you use Catalyst Center to create, reserve, or delete any IP address pool, Catalyst Center conveys this information to your external IPAM.

Before you begin

Requirements for external IPAM integration:

- Create a role that has write permission to the IPAM function and assign it to the user account used for integration with Catalyst Center.
- To enable IP pool creation by LAN automation for point-to-point addressing, the role must include:
  - For Infoblox: Write permission for **Network Views**.
  - For Bluecat: Full access permission for **Configurations**.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **IP Address Manager**.

Step 2 In the **Server Name** field, enter the name of the IPAM server.

Step 3 In the **Server URL** field, enter the URL or IP address of the IPAM server.

A warning icon and message appear, indicating that the certificate is not trusted for this server. To import the trust certificate directly from the IPAM:

a) Click the warning icon.

A **Certificate Warning** dialog box appears.

b) Verify the issuer, serial number, and validity dates for the certificate.

c) If the information is correct, check the check box to allow Catalyst Center to access the IP address and add the untrusted certificate to the trusted certificates.

d) Click **Allow**.

Step 4 In the **Username** and **Password** fields, enter the IPAM credentials.

Step 5 From the **Provider** drop-down list, choose a provider.

Note

If you choose **BlueCat** as your provider, ensure that your user has been granted API access in the BlueCat Address Manager. See your BlueCat documentation for information about configuring API access for your user or users.

To integrate Catalyst Center with BlueCat in Federal Information Processing Standards (FIPS) mode, use BlueCat 9.3.0.

Step 6 From the **View** drop-down list, choose a default IPAM network view. If you only have one view configured, only **default** appears in the drop-down list. The network view is created in the IPAM and is used as a container for IP address pools.

Step 7 If you want to synchronize the IP address pools on Catalyst Center with the IPAM, check the **Sync global pools from IP Address Pools to the selected view from IPAM server** check box. If you don't want to synchronize the IP pools, leave the check box unchecked.

Note

You should only skip the synchronization if you know that the view of the IPAM is already synchronized with the IP address pool on Catalyst Center. For example, this can occur when:

- The IPAM has been upgraded through backup and restore to a new server instance
- The IPAM was accidentally deleted and you want to readd it

If you skip synchronization when adding or updating the IPAM when the view is out of sync with IP address pools on Catalyst Center, pool operations might fail in the future.

Step 8 Click **Save**.

What to do next

Go to **System** > **Settings** > **Trust & Privacy** > **Trusted Certificates** to verify that the certificate has been successfully added.

Note In trusted certificates, the certificate is referenced as a third-party trusted certificate.

Go to **System** > **System 360** and verify the information to ensure that your external IP address manager configuration succeeded.

Configure Webex integration

Catalyst Center provides Webex meeting session information for Client 360.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Webex Integration**.

Step 2 Click **Authenticate to Webex**.

Step 3 In the **Cisco Webex** pop-up window, enter the email address and click **Sign In**.

Step 4 Enter the password and click **Sign In**.

Webex authentication is completed successfully.

Step 5 Under **Default Email Domain for Webex Meetings Sign-In**, enter the Webex user email domain and click **Save**.

The Webex domain is organization-wide, and all users who use the domain can host or attend meetings.

Step 6 (Optional) Under **Authentication Token**, click **Delete** to delete Webex authentication.

Configure an AppX MS-Teams integration

When activated, Catalyst Center provides call quality metrics information for Application 360 and Client 360 dashboards.

Before you begin

You must have a Microsoft Teams account with admin privileges.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Cisco Catalyst - Cloud**.

Step 2 From the **Region** drop-down list, select the DNA Cloud US region. For the integration to work, Microsoft Teams must be enabled in the same region (DNA Cloud US).

Step 3 Click the 🔍 icon, search by name, and locate **AppX MS-Teams**.

Step 4 Click **Activate**.

You are redirected to the **Cisco Catalyst - Cloud** window.

Step 5 In the **Cisco Catalyst - Cloud** window:

a) Log in to Cisco Catalyst - Cloud with your cisco.com credentials.

If you do not have cisco.com credentials, you can create them.

b) In the **Activate application on your product** window, click the consent flow link and do these tasks:

- In the **Sign in to your account** window, enter the Microsoft admin username and password, and click **Sign In**.
- Click **Accept**.

c) In the **Activate application on your product** window, select Catalyst Center and click **Next**.

To register a new Catalyst Center, click the **here** link and:

- In the **Host Name/IP** field, enter the Catalyst Center IP address.
- In the **Product Name** field, enter the Catalyst Center name.
- In the **Type** field, enter the Catalyst Center type.
- Click **Register**.

d) **Cisco Catalyst - Cloud** synchronizes with Catalyst Center automatically; you are redirected to the **Choose the Scope for your Cisco Catalyst Center** window. Click **Next**.

e) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

f) Click **Activate**.
You are redirected back to Catalyst Center.

Note
If you want to deactivate the product or disconnect from AppX MS-Teams application, see Configure an AppX MS-Teams integration through Cisco Cloud Services, on page 70.

Configure an AppX MS-Teams integration through Cisco Cloud Services

Use this procedure to activate, deactivate, or check the status of MS-Teams integration on the devices through Cisco Cloud Services.

Before you begin

You must have a Microsoft Teams account with admin privileges.

Procedure

Step 1 Log in to Cisco Cloud Services with your cisco.com credentials.

If you do not have cisco.com credentials, you can create them.

Step 2 From the main menu, choose **Applications and Products**.

Step 3 From the **Region** drop-down list, select the DNA Cloud US region. For the integration to work, Microsoft Teams must be enabled in the same region (DNA Cloud US).

Step 4 Click the 🔍 icon, search by name, and locate **AppX MS-Teams**.

Step 5 In the **AppX MS-Teams** tile, click **Activate**. For details, see Configure an AppX MS-Teams integration, on page 69.

Step 6 After the product is activated, click **Exit**.

Step 7 You are redirected to the **Applications** window.

Step 8 Click the **AppX MS-Team** tile to view the details in the **App 360** window.

Step 9 (Optional) To activate products from the **App 360** window:

a) In the **Product Activations** table, click **Add**.

b) Choose the product that you want to activate and click **Next**.

Note
You cannot select more than one product at a time.

c) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**. Otherwise, click **Activate**.

Step 10 (Optional) To deactivate the product:

a) Click the **AppX MS-Teams** tile.

b) In the **Product Activations** table, check the check box next to the product that you want to deactivate.

c) From the **More Action** drop-down list, choose **Deactivate**.

d) In the confirmation window, click **Deactivate**.

Step 11 (Optional) To disconnect the product from AppX MS-Teams application:

a) Click the **AppX MS-Teams** tile to view the details in the **App 360** window.

b) In the top menu bar, click **View all details**.
The **Details** slide-in pane is displayed.

c) Click **Disconnect now**.

Configure ThousandEyes integration

You can configure Catalyst Center to communicate with an external ThousandEyes API agent to enable ThousandEyes integration using an authentication token. After integration, Catalyst Center provides ThousandEyes agent test data in the Application Health dashboard.

Before you begin

Ensure that you have deployed the ThousandEyes agent through application hosting, which supports Cisco Catalyst 9300 and 9400 Series switches.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **ThousandEyes Integration**.

Step 2 To connect ThousandEyes account to Catalyst Center:

a. Click **Start set up**. The device authentication code is displayed.

b. Click **Login** and enter the device authentication code in the **Cisco ThousandEyes authentication** pop-up window and click **Verify**.

c. In the **ThousandEyes login** window, enter the ThousandEyes credentials and click **Login**.

Step 3 To disconnect the ThousandEyes, click **Disconnect**.

Configure debugging logs

To assist in troubleshooting service issues, you can change the logging level for the Catalyst Center services.

A logging level determines the amount of data that is captured in the log files. Each logging level is cumulative; that is, each level contains all the data generated by the specified level and higher levels, if any. For example, setting the logging level to **Info** also captures **Warn** and **Error** logs. We recommend that you adjust the logging level to assist in troubleshooting issues by capturing more data. For example, by adjusting the logging level, you can capture more data to review in a root cause analysis or RCA support file.

The default logging level for services is informational (**Info**). You can change the logging level from informational to a different logging level (**Debug** or **Trace**) to capture more information.

Caution Due to the type of information that might be disclosed, logs collected at the **Debug** level or higher should have restricted access.

Note Log files are created and stored in a centralized location on your Catalyst Center host for display in the GUI. From this location, Catalyst Center can query and display logs in the GUI (**System** > **System 360** > **Log Explorer**). Logs are available to query for only the last 2 days. Logs that are older than 2 days are purged automatically from this location.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration** > **Debugging Logs**.

The **Debugging Logs** window is displayed.

Step 2 From the **Service** drop-down list, choose a service to adjust its logging level.

The **Service** drop-down list displays the services that are currently configured and running on Catalyst Center.

Step 3 Enter the **Logger Name**.

This is an advanced feature that has been added to control which software components emit messages into the logging framework. Use this feature with care. Misuse of this feature can result in loss of information needed for technical support purposes. Log messages will be written only for the loggers (packages) specified here. By default, the Logger Name includes packages that start with *com.cisco*. You can enter additional package names as comma-separated values. Do not remove the default values unless you are explicitly directed to do so. Use * to log all packages.

Step 4 From the **Logging Level** drop-down list, choose the new logging level for the service.

Catalyst Center supports logging levels in descending order of detail, including:

- **Trace**: Trace messages
- **Debug**: Debugging messages
- **Info**: Normal, but significant condition messages
- **Warn**: Warning condition messages
- **Error**: Error condition messages

Step 5 From the **Time Out** field, choose the time period for the logging level.

Configure logging-level time periods in increments of 15 minutes up to an unlimited time period. If you specify an unlimited time period, the default level of logging should be reset each time a troubleshooting activity is completed.

Step 6 Review your selection and click **Save**.

Configure the network resync interval

You can update the polling interval at the global level for all devices by choosing **System** > **Settings** > **Network Resync Interval**. Or, you can update the polling interval at the device level for a specific device by choosing **Device Inventory**. When you set the polling interval using the **Network Resync Interval**, that value takes precedence over the **Device Inventory** polling interval value.

Before you begin

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **Network Resync Interval**.

Step 2 In the **Resync Interval** field, enter a new time value (in minutes).

Step 3 (Optional) Check the **Override for all devices** check box to override the existing configured polling interval for all devices.

Step 4 Click **Save**.

View audit logs

Audit logs capture information about the various applications running on Catalyst Center. Audit logs also capture information about device public key infrastructure (PKI) notifications. The information in these audit logs can be used to help in troubleshooting issues, if any, involving the applications or the device CA certificates.

Audit logs also record system events that occurred, when and where they occurred, and which users initiated them. With audit logging, configuration changes to the system get logged in separate log files for auditing.

Procedure

Step 1 From the main menu, choose **Activities** > **Audit Logs**.

The **Audit Logs** window opens, where you can view logs about the current policies in your network. These policies are applied to network devices by the applications installed on Catalyst Center.

Step 2 Click the timeline slider to specify the time range of data you want displayed on the window:

a. In the **Time Range** area, select a time range—**Last 2 Weeks**, **Last 7 Days**, **Last 24 Hours**, or **Last 3 Hours**.

b. To specify a custom range, click **By Date** and specify the start and end date and time.

c. Click **Apply**.

Step 3 Click the arrow next to an audit log to view the corresponding child audit logs.

Each audit log can be a parent to several child audit logs. By clicking the arrow, you can view a series of additional child audit logs.

Note
An audit log captures data about a task done by Catalyst Center. Child audit logs are subtasks to a task done by Catalyst Center.

Step 4 (Optional) From the list of audit logs in the left pane, click a specific audit log message. In the right pane, click **Event ID** > **Copy Event ID to Clipboard**. With the copied ID, you can use the API to retrieve the audit log message based on the event ID.

The audit log displays the **Description**, **User**, **Interface**, and **Destination** of each policy in the right pane.

Note
The audit log displays northbound operation details such as POST, DELETE, and PUT with payload information, and southbound operation details such as the configuration pushed to a device. For detailed information about the APIs on Cisco DevNet, see Catalyst Center Platform Intent APIs.

Step 5 (Optional) Click **Filter** to filter the log by **User ID**, **Log ID**, or **Description**.

Step 6 Click the pencil icon to subscribe to the audit log events.

A list of syslog servers is displayed.

Step 7 Check the syslog server check box that you want to connect to and click **Save**.

Note
Uncheck the syslog server check box to unsubscribe from the audit log events and click **Save**.

Step 8 In the right pane, use the **Search** field to search for specific text in the log message.

Step 9 From the main menu, choose **Activities** > **Tasks** to view the upcoming, in-progress, completed, and failed tasks (such as operating system updates or device replacements) and existing, pending-review, and failed work items.

Export audit logs to syslog servers

Security recommendation: For secure and easier log monitoring, we recommend that you export audit logs from Catalyst Center to a remote syslog server in your network.

You can export the audit logs from Catalyst Center to multiple syslog servers by connecting to them.

Before you begin

Configure the syslog servers in the **System** > **Settings** > **External Services** > **Destinations** > **Syslog** area.

Procedure

Step 1 From the main menu, choose **Activities** > **Audit Logs**.

Step 2 At the top of the window, click the pencil icon.

Step 3 Select the syslog servers that you want to connect to and click **Save**.

Step 4 (Optional) To disconnect from a syslog server, deselect it and click **Save**.

Enable visibility and control of configurations

The Visibility and Control of Configurations feature provides a solution to further secure your planned network configurations before deploying them on to your devices. With enhanced visibility, you can enforce the previewing of device configurations (CLI and NETCONF commands) before deploying them. Visibility is enabled by default. When visibility is enabled, you cannot deploy your device configurations until you review them. With enhanced control, you can send the planned network configurations to IT Service Management

(ITSM) for approval. When control is enabled, you cannot deploy the configurations until an IT administrator approves them.

Note If a provisioning workflow supports **Visibility and Control of Configurations**, this banner message displays when you schedule the deployment of your task:

This workflow supports enforcing network administrators and other users to preview configurations before deploying them on the network devices. To configure this setting, go to **System** > **Settings** > **Visibility and Control of Configurations**.

Before you begin

Make sure that ITSM is enabled and configured in Catalyst Center so that you can enable **ITSM Approval**. For information about how to enable and configure ITSM, see “Configure the Catalyst Center Automation Events for ITSM (ServiceNow) Bundle” in the *Catalyst Center ITSM Integration Guide*.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration** > **Visibility and Control of Configurations**.

Step 2 Click the **Configuration Preview** toggle button to enable or disable visibility.

Enabling visibility means you must preview the device configurations before deploying them.

Disabling visibility means you are not enforcing the previewing of device configurations before deploying them. When visibility is disabled, you can schedule and deploy the configurations with or without previewing them.

Step 3 (Optional) Click the **ITSM Approval** toggle button to enable or disable control.

Enabling control means you must submit the planned network configurations to an ITSM administrator for approval before deploying them.

Disabling control means you are not requiring ITSM approval before the deployment of planned network configurations. When control is disabled, you can deploy the configurations without ITSM approval.

View, search, and filter for task and work item details

You can view, search, and filter for task and work item details on the **Tasks** window.

Procedure

Step 1 From the main menu, choose **Activities** > **Tasks**.

By default, the **Tasks** window displays all the upcoming, in-progress, failed, and successful tasks and existing, pending-review, and failed work items. All failed tasks have a trace ID that provides a hint to analyze the error log quickly.

The left **SUMMARY** pane displays filtering options for you to refine the list of displayed tasks and work items. You can expand and collapse the **SUMMARY** pane by clicking the arrow icon.

Step 2 Use this table to view, search, and filter for task and work item details on the **Tasks** window.

Action	Steps
Filter for specific task and work item details.	**a.** In the **SUMMARY** pane, under **Type**, click **Task** to filter for only tasks or **Work Item** to filter for only work items. **b.** Filter for task and work item details using the filter options available under **Status**, **Review Status**, **Last Updated**, **Categories**, and **Recurring**. The **Tasks** window displays the results of applied filters. **Tip** Under **Categories**, you can search for a specific category by clicking **Show all** and using the **Search** field.
Remove an applied filter.	**a.** In the **SUMMARY** pane, under **FILTERED BY**, click **x** next to the applied filter. The **Tasks** window displays the results of removing the filter. **b.** You can also remove the **Status**, **Review Status**, and **Categories** filters by unchecking the check boxes.
Search for a task and work item by title or username.	By default, the **Search** field, searches tasks and work items by description. If any filters are applied when you search for a task or work item, the system searches within the applied filters. For example, if you applied the **In Progress** filter and search for all tasks and work items with “provision” in the name, the system searches only in-progress tasks and work items for this keyword. **a.** In the **Search by description** field, enter a description of the task or work item. The **Tasks** window displays the filtered list of tasks and work items based on the entered description. **b.** To search by username, in the **Search** field, do the following: **1.** Click the filter icon. **2.** Click **username**. **3.** Enter a username in the **Search by username** field. **4.** Click **Apply**.

Action	Steps
Sort the list of tasks and work items.	By default, the tasks and work items are listed by when they were last updated. You can sort tasks and work items by their start time or update time. **a.** To the right of the **Search** field, hover your cursor over the sort drop-down list and choose a sorting option. The **Tasks** window displays the sorted list of tasks and work items based on the chosen sorting option.

View, edit, stop, and delete tasks

You can view information about all the upcoming, in-progress, failed, and successful tasks running on Catalyst Center.

A task is an operation that you or the system scheduled, which can reoccur. If you have a task, this means that you have no corresponding work items to complete for it to deploy as scheduled.

The information available in a task depends on its category, and there are a variety of categories. Common task categories include provision, config archive, inventory, and security advisories. However, all tasks display the following details: who initiated the task, its category, its completion status, its success status, and its start date, last updated date, and end date.

Procedure

Step 1 From the main menu, choose **Activities** > **Tasks**.

By default, the **Tasks** window displays all the upcoming, in-progress, failed, and successful tasks and existing, pending-review, and failed work items.

Note
If you enabled Site Settings for multiple devices in different time zones in a task, the **Starts** field displays the start time of the device in the earliest time zone based on your local time zone. For example, let's say that you are in the Pacific Time Zone, and you have two devices scheduled to deploy on May 8, 2024, at 12 PM. One device is in San Jose, CA, and the other device is in Bengaluru, India. The **Starts** field displays May 8, 2024, at 12:00 PM, because your local time zone aligns with the device in the earliest time zone. If you are in Bengaluru, India, this field displays May 9, 2024, at 12:30 AM, because your local time is 12 hours and 30 minutes ahead of the device in the earliest time zone.

Step 2 Use this table to view, edit, or delete a task on the **Tasks** window.

Action	Steps
View a task.	**a.** Click the task name to open a slide-in pane with more information. The task details depend on what type of task you're viewing. **b.** In the slide-in pane, depending on the details displayed, you can do the following: • View device and provisioning details by clicking **Device Details** or **Provision Details**. • View more information about in-progress, completed, and failed tasks by clicking **View Details** or **See Details**. • Search for a task using **Search Table**. • Filter for a task using the filter icon in the top-right corner of the table. • Download an error report of a failed task by clicking **Download Error Report**. A tar file is created and saved to your local machine. **Tip** While creating a support case, you can attach the downloaded error report in addition to other details you may want to include.
Edit the schedule of a recurring task.	**a.** Locate the task and click **Edit**. **b.** In the **Edit Schedule** slide-in pane, define the **Start Date** and **Start Time**. **c.** Using the **Recurrence** toggle button, click a recurrence interval. **d.** In the **Run at Interval** field, enter a value. **e.** (Optional) To schedule an end date and time for this task, do the following: **1.** Check the **Set Schedule End** check box. **2.** To end the task on a specific date, click **End Date** and choose the date. **3.** To end the task after a number of occurrences, click **End After** and in the **Occurrences** field, enter a numerical value. **f.** Click **Preview** to review the changes in the table. **g.** Ensure the table's listed **Site Time** (the device's time zone) and **Local Time** (your time zone) for each device reflect the intended scheduled time **h.** When you're ready, click **Save**.

Action	Steps
Stop a task.	**a.** Click the task name to open a slide-in pane with more information. **b.** Click **Stop**. **Note** **Stop** is disabled if the provisioning workflow doesn't support this capability. **c.** In the **Stop** dialog box, click **Yes** to confirm the stoppage of the task. A task can only be stopped when it is in progress. When the system starts configuring devices, the task can't be stopped. Only the devices pending provisioning are stopped.
Delete a task.	**a.** Locate the task and click **Delete**.

View and discard work items

If you enabled the Visibility and Control of Configurations feature, a work item is created when you choose **Generate configuration preview** during any workflow. When the configurations are reviewed and ready for deployment, the work item becomes a task.

To enable Visibility and Control of Configurations, see Enable visibility and control of configurations, on page 75.

Procedure

Step 1 From the main menu, choose **Activities** > **Tasks**.

By default, the **Tasks** window displays all the upcoming, in-progress, failed, and successful tasks and existing, pending-review, and failed work items.

Step 2 Use this table to view and discard a work item on the **Tasks** window.

Action	Steps
View a work item.	**a.** In the **SUMMARY** pane, under **Type**, click **Work Item**. The **Tasks** window filters for and displays only work items. **b.** Click the work item name to open a slide-in pane with more information. The first listed device's configuration preview is displayed. **c.** In the slide-in pane, you can do the following: • Preview a device's configurations by choosing a device in the left pane. • Filter the data in the configuration preview pane with the **View by Configuration Source** drop-down list. • View a side-by-side comparison view of the planned configuration and the running configuration or view only the planned configuration by clicking the view switcher (▫ ▣). **Note** Viewing YANG configurations in the side-by-side comparison view isn't supported. • Click one command in one configuration to highlight the corresponding command in the other configuration when you're in the side-by-side comparison view. **Note** Keep the following limitations in mind: • The system supports only side-by-side highlighting for first-level commands, not sublevel commands. • All commands must be a complete match for the system to display the side-by-side highlighting between configurations. • If you click any commands starting with `No` in one configuration, the system will ignore the `No` portion when checking for a match in the other configuration. • Search for a value in the displayed configuration with the **Search configuration** field. • Display the workflow progression view for the selected device by clicking **Back to workflow progress** in the top-right corner of the right pane. To return to the configuration preview pane, click **Go to generated config**. **Note** **Back to workflow progress** and **Go to generated config** are only available if the workflow supports the workflow progression view.

Action	Steps
Discard a work item.	**a.** Locate the work item and click **Discard**. You can also click the work item name to open a slide-in pane and then click **Discard**. **b.** In the **Discard** dialog box, do one of the following: • If you want to discard the work item and return to the current activity, click **Discard**. **Note** Discarding the work item means you can't recover it later. • If you want to retain any generated configurations and discard all other resources, check the **Retain generated configs (if any)** check box and click **Accept**. After retaining any generated configurations and discarding all other resources, the work item displays **Exit** instead of **Exit and Preview Later** because you've previewed all the configurations and chosen to discard the nongenerated ones. **Tip** Consider retaining any generated configurations and discarding all other resources if a configuration preview fails so that you or your IT administrator can further inspect the issue.

What to do next

To deploy the previewed device configurations or submit the planned network configurations for ITSM approval, see "Visibility and Control of Configurations Workflow," “Visibility and Control of Wireless Device Configurations,” or “Visibility and Control of Fabric Configurations” in the *Cisco Catalyst Center User Guide*.

Activate high availability

Complete this procedure to activate high availability (HA) on your Catalyst Center cluster:

Note The three-node HA is not supported for Catalyst Center running on ESXi.

Before you begin

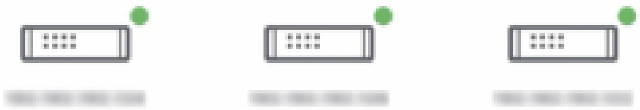
Review these topics in the *Cisco Catalyst Center High Availability Guide, Release 3.1.3* and confirm that your production environment meets the requirements they describe:

- "High availability requirements"
- "Supported appliances"

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration** > **High Availability**.

Step 2 Confirm that the page displays the three Catalyst Center appliances in your cluster.



Step 3 Click **Activate High Availability**.

Step 4 Confirm that HA has been enabled:

- The **Status** field displays `Active`.
- In the top-right corner of the **High Availability** page, click the **Activities** link. In the resulting table, verify that the status displayed for the HA activation event is `SUCCESS`.

Configure integration settings

In cases where firewalls or other rules exist between Catalyst Center and any third-party apps that need to reach the Catalyst Center platform, you must configure **Integration Settings**. These cases occur when the IP address of Catalyst Center is internally mapped to another IP address that connects to the internet or an external network.

Important After a backup and restore of Catalyst Center, you need to access the **Integration Settings** page and update (if necessary) the **Callback URL Host Name** or **IP Address** using this procedure.

Before you begin

You have installed the Catalyst Center platform.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Integration Settings**.

Step 2 Enter the **Callback URL Host Name** or **IP Address** that the third-party app needs to connect to when communicating with the Catalyst Center platform.

Note
The **Callback URL Host Name** or **IP Address** is the external facing hostname or IP address that is mapped internally to Catalyst Center. Configure the VIP address for a three-node cluster setup.

Step 3 Click **Apply**.

Set up a login message

You can set up a message that is displayed to all users after they log in to Catalyst Center.

Before you begin

Only a user with **SUPER-ADMIN-ROLE** or **CUSTOM-ROLE** with system management permissions can perform this procedure.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration** > **Login Message**.

Step 2 In the **Login Message** text box, enter the message.

Step 3 Click **Save**.

The message appears below the **Log In** button on the Catalyst Center login page.

Later, if you want to remove this message, do the following:

a. Return to the **Login Message** settings page.

b. Click **Clear** and then click **Save**.

Configure the proxy

If Catalyst Center has a proxy server configured as an intermediary between itself and the network devices that it manages, you must configure access to the proxy server.

Note Catalyst Center does not support a proxy server that uses Windows New Technology LAN Manager (NTLM) authentication.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration**.

Step 2 From the **System Configuration** drop-down list, choose **Proxy** > **Outgoing Proxy**.

Step 3 Enter the proxy server URL address.

Step 4 Enter the proxy server port number.

Note

- For HTTP, the port number is usually 80.
- The port number ranges from 0 through 65535.

Step 5 (Optional) If the proxy server requires authentication, click **Update** and enter the username and password for access to the proxy server.

Step 6 Check the **Validate Settings** check box to have Catalyst Center validate your proxy configuration settings when applying them.

Step 7 Review your selections and click **Save**.

To cancel your selection, click **Reset**. To delete an existing proxy configuration, click **Delete**.

After configuring the proxy, you can view the configuration in the **Proxy** window.

Important

It can take up to five minutes for Catalyst Center services to get updated with the proxy server configuration.

Configure geo map settings

You can configure geo map settings in Catalyst Center.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration** > **Geo Map Settings**.

Step 2 Choose any one of the available administrative boundaries that identify geographic features with characteristics defined differently by audiences belonging to various regional, cultural, or political groups.

- China (CN)
- India (IN)
- Japan (JP)
- United States (US) (default)

Step 3 Click **Save**.

Security recommendations

Catalyst Center provides many security features for itself, for the hosts and network devices that it monitors and manages. You must clearly understand and configure the security features correctly. Follow these security recommendations:

- Deploy Catalyst Center in a private internal network and behind a firewall that does not expose Catalyst Center to an untrusted network, such as the internet.
- If you have separate management and enterprise networks, connect Catalyst Center's management and enterprise interfaces to your management and enterprise networks, respectively. Doing so ensures network isolation between the services used to administer and manage Catalyst Center and the services used to communicate with and manage your network devices.
- If deploying Catalyst Center in a three-node cluster setup, verify that the cluster interfaces are connected in an isolated network.
- Upgrade Catalyst Center with critical upgrades, including security patches, as soon as possible after a patch announcement. For more information, see the Catalyst Center Upgrade Guide.
- Restrict the remote URLs accessed by Catalyst Center using an HTTPS proxy server. Catalyst Center is configured to access the internet to download software updates, licenses, and device software, as well as provide up-to-date map information, user feedback, and so on. Providing internet connections for these purposes is a mandatory requirement. However, provide connections securely through an HTTPS proxy server.
- Restrict the ingress and egress management and enterprise network connections to and from Catalyst Center using a firewall, by only allowing known IP addresses and ranges and blocking network connections to unused ports.
- Replace the self-signed server certificate from Catalyst Center with the certificate signed by your internal certificate authority (CA).
- If possible in your network environment, disable SFTP Compatibility Mode. This mode allows legacy network devices to connect to Catalyst Center using older cipher suites.
- Disable the browser-based appliance configuration wizard, which comes with a self-signed certificate.

Change the minimum TLS version and enable RC4-SHA (not secure)

Security recommendation: Upgrade the minimum TLS version to TLSv1.2 for incoming TLS connections to Catalyst Center.

Northbound REST API requests from an external network, include northbound REST API-based apps, browsers, and network devices connecting to Catalyst Center using HTTPS. The Transport Layer Security (TLS) protocol makes such requests secure.

By default, Catalyst Center supports TLSv1.1 and TLSv1.2, and does not support RC4 ciphers for SSL/TLS connections. Since RC4 ciphers have well-known weaknesses, we recommend that you upgrade the minimum TLS version to TLSv1.2 if your network devices support it.

Catalyst Center provides a configuration option to downgrade the minimum TLS version and enable RC4-SHA. You can use this option if your network devices under Catalyst Center control cannot support the existing minimum TLS version (TLSv1.1) or ciphers. For security reasons, however, we recommend that you do not downgrade Catalyst Center TLS version or enable RC4-SHA ciphers.

To change the TLS version or enable RC4-SHA for Catalyst Center, log in to the corresponding appliance and use the CLI.

Note CLI commands can change from one release to the next. The CLI example uses command syntax that might not apply to all Catalyst Center releases, especially Catalyst Center on ESXi releases.

Before you begin

You must have maglev SSH access privileges to do this procedure.

Note This security feature applies to port 443 on Catalyst Center. Doing this procedure may disable traffic on the port to the Catalyst Center infrastructure for a few seconds. For this reason, you must configure TLS infrequently and only during off-peak hours or during a maintenance period.

Procedure

Step 1 Using an SSH client, log in to the Catalyst Center appliance with the IP address that you specified using the configuration wizard.

The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your username and password for SSH access.

Step 3 Enter this command to check the TLS version currently enabled on the cluster.

Here is an example:

```
Input
$ magctl service tls_version --tls-min-version show
Output
TLS minimum version is 1.1
```

Step 4 If you want to change the TLS version on the cluster, enter these commands. For example, you can change the current TLS version to an earlier version if your network devices under Catalyst Center control cannot support the existing TLS version.

This example shows how to change from TLS Version 1.1 to 1.0:

```
Input
$ magctl service tls_version --tls-min-version 1.0
Output
Enabling TLSv1.0 is recommended only for legacy devices
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.0 for api-gateway
deployment.extensions/kong patched
```

This example shows how to change from TLS Version 1.1 to 1.2 (only allowed if you haven't enabled RC4-SHA):

```
Input
$ magctl service tls_version --tls-min-version 1.2
Output
Enabling TLSv1.2 will disable TLSv1.1 and below
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.2 for api-gateway
deployment.extensions/kong patched
```

Note
Setting TLS Version 1.2 as the minimum version is not supported when RC4-SHA ciphers are enabled.

Step 5 If you want to change the TLS version for streaming telemetry connections between Catalyst Center and Catalyst 9000 devices (via the TCP 25103 port), enter this command. For example, you can change the current TLS version if the network devices that Catalyst Center manages can support TLS version 1.2.

This example shows how to change from TLS Version 1.1 to 1.2:

```
Input
$ magctl service tls_version --tls-min-version 1.2 -a assurance-backend collector-iosxe-db
Output
Enabling TLSv1.2 will disable TLSv1.1 and below
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.2 for api-gateway
deployment.apps/collector-iosxe-db patched
```

Step 6 Enter this command to enable RC4-SHA on a cluster (not secure; proceed only if needed).

Enabling RC4-SHA ciphers is not supported when TLS Version 1.2 is the minimum version.

This example shows TLS version 1.2 is not enabled:

```
Input
$ magctl service ciphers --ciphers-rc4=enable kong
Output
Enabling RC4-SHA cipher will have security risk
Do you want to continue? [y/N]: y
WARNING: Enabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

Step 7 Enter the command at the prompt to confirm that TLS and RC4-SHA are configured.

Here is an example:

```
Input
$ magctl service display kong
Output
      containers:
      - env:
        - name: TLS_V1
          value: "1.1"
        - name: RC4_CIPHERS
          value: "true"
```

Note
If RC4 and TLS minimum versions are set, they are listed in the env: of the **magctl service display kong** command. If these values are not set, they do not appear in the env:.

Step 8 To disable the RC4-SHA ciphers that you enabled previously, enter this command on the cluster:

```
Input
$ magctl service ciphers --ciphers-rc4=disable kong
Output
```

```
WARNING: Disabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

Step 9 Log out of the Catalyst Center appliance.

Configure the proxy certificate

In some network configurations, proxy gateways might exist between Catalyst Center and the remote network it manages (containing various network devices). Common ports, such as 80 and 443, pass through the gateway proxy in the DMZ, and for this reason, SSL sessions from the network devices meant for Catalyst Center terminate at the proxy gateway. Therefore, the network devices located within these remote networks can only communicate with Catalyst Center through the proxy gateway. For the network devices to establish secure and trusted connections with Catalyst Center, or, if present, a proxy gateway, the network devices should have their PKI trust stores appropriately provisioned with the relevant CA root certificates or the server's own certificate under certain circumstances.

If such a proxy is in place during onboarding of devices through PnP Discovery/Services, the proxy and the Catalyst Center server certificate must be the same so that network devices can trust and authenticate Catalyst Center securely.

In network topologies where a proxy gateway is present between Catalyst Center and the remote network it manages, import a proxy gateway certificate in to Catalyst Center:

Before you begin

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.
- You must use the proxy gateway's IP address to reach Catalyst Center and its services.
- You should have the certificate file that is currently being used by the proxy gateway. The certificate file contents should consist of any of these:
  - The proxy gateway's certificate in PEM or DER format, with the certificate being self-signed.
  - The proxy gateway's certificate in PEM or DER format, with the certificate being issued by a valid, well-known CA.
  - The proxy gateway's certificate and its chain in PEM or DER format.

The certificate used by the devices and the proxy gateway must be imported in to Catalyst Center by following this procedure.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration**.

Step 2 From the **System Configuration** drop-down list, choose **Proxy** > **Incoming Proxy**.

Step 3 In the **Proxy Certificate** window, view the current proxy gateway certificate data (if it exists).

Note

The **Expiration Date and Time** is displayed as a Greenwich Mean Time (GMT) value. A system notification appears in the Catalyst Center GUI two months before the certificate expires.

Step 4 To add a proxy gateway certificate, drag and drop the self-signed or CA certificate into the **Drag and Drop Here** area.

Note
Only PEM or DER files (public-key cryptography standard file formats) can be imported into Catalyst Center using this area. Additionally, private keys are neither required nor uploaded into Catalyst Center for this procedure.

Step 5 Click **Save**.

Step 6 Refresh the **Proxy Certificate** window to view the updated proxy gateway certificate data.
The information displayed in the **Proxy Certificate** window should have changed to reflect the new certificate name, issuer, and certificate authority.

Step 7 Click the **Enable** button to enable the proxy gateway certificate functionality.

If you click the **Enable** button, the controller returns the imported proxy gateway certificate when requested by a proxy gateway. If you don't click the **Enable** button, the controller returns its own self-signed or imported CA certificate to the proxy gateway.

The **Enable** button is dimmed if the proxy gateway certificate functionality is used.

Upload an SSL intercept proxy certificate

If SSL decryption is enabled on the proxy server that is configured between Catalyst Center and the Cisco cloud from which it downloads software updates, ensure that the proxy is configured with a certificate that is issued from an official certificate authority. If you are using a *private* certificate, complete the following steps.

Note For added security, access to the root shell is disabled in Catalyst Center. With restricted shell, users can't access the underlying operating system and file system, which reduces operational risk. However, the commands in this section require that you contact the Cisco TAC to access the root shell temporarily.

Procedure

Step 1 Transfer your proxy server’s certificate (in PEM format) to a directory on the Catalyst Center server.

Step 2 As a maglev user, SSH to the Catalyst Center server and enter this command:

```
# /usr/local/bin/update_cacerts.sh -v -a example.pem
```

The command returns output that is similar to this example.

```
Reading CA cert from file example.pem
Adding certficate import_04:F7:6B:24:92:95:5A:20:3E:05:83:40:FA:19:8D:94:B2:B0:69:60.crt
Sending MKS Event..
(Attempt 1) Command to execute kubectl create -f /tmp/event_file.yaml
(Attempt 1) kubectl create -f /tmp/event_file.yaml completed successfully
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,
it does not contain exactly one certificate or CRL
```

```
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Attempting to restart containerd (Attempt 1)...
containerd restarted successfully.
[Attempt 1/10] Restarting Pod/Service that has a host mounted certificate dependency.
Please wait for the pods to come back up and resume normal working. This might take a while
Successfully triggered a restart for the containers needing the certificates.
Deleting tempfiles /tmp/tmp.CMu8bA83SC /tmp/tmp.6STo8fQRNB /tmp/tmp.cjBhl4gw5b
```

Step 3 Check the command output for the line "1 added" and confirm that the number added is not zero. The number can be one or greater, based on the certificates in the chain.

Step 4 In Catalyst Center, upload the same certificate and check the connectivity.

a) Log in to the Catalyst Center GUI.

b) Navigate to **System** > **Settings** > **Certificates** > **Trusted Certificates** and upload the same certificate.

For more information, see Configure trusted certificates, on page 106.

c) Check the cloud, Cisco Connected Mobile Experiences (CMX), and Cisco Spaces connectivity.

Renew internal certificates

Catalyst Center uses a number of certificates, such as the ones generated by Kubernetes and the ones used by Kong and Credential Manager Services. These certificates are valid for one year, which starts as soon as you install your cluster. Catalyst Center automatically renews these internal certificates for another year before they are set to expire.

- We recommend that you renew internal certificates before they expire, not after.
- You can only renew internal certificates that are set to expire up to 100 days from now. This procedure does not do anything to certificates that will expire later than that.
- The script refreshes only self-signed certificates, not third-party/certificate authority (CA)-signed certificates. For third-party/CA-signed certificates, the script updates the internal certificates used by Kubernetes and the Credential Manager.
- For self-signed certificates, the renewal process does not require you to push certificates back out to devices, because the root CA is unchanged.
- The term *cluster* applies to both single-node and three-node Catalyst Center setups.

Procedure

Step 1 Ensure that each cluster node is healthy and not experiencing any issues.

Step 2 To view a list of the certificates that are currently used by that node and their expiration date, enter this command:

```
sudo maglev-config certs info
```

Step 3 Renew the internal certificates that are set to expire soon by entering this command:

```
sudo maglev-config certs refresh
```

Step 4 Repeat the preceding steps for the other cluster nodes.

Step 5 For utility help, enter:

```
$ sudo maglev-config certs --help
Usage: maglev-config certs [OPTIONS] COMMAND [ARGS]...

Options:
  --help  Show this message and exit.

Commands:
  info
  refresh
```

Certificate and private key support

Catalyst Center supports the Certificate Authority Management feature, which is used to authenticate sessions (HTTPS). These sessions use commonly recognized trusted agents that are called CAs. Catalyst Center uses the Certificate Authority Management feature to import, store, and manage X.509 certificates from your internal CA. The imported certificate becomes an identity certificate for Catalyst Center, and Catalyst Center presents this certificate to its clients for authentication. The clients are the northbound API applications and network devices.

You can import these files (in either the PEM or PKCS file format) using the Catalyst Center GUI:

- X.509 certificate
- Private key

Note For the private key, Catalyst Center supports the import of RSA keys. Keep the private key secure in your own key management system. The private key must have a minimum modulus size of 2048 bits.

Prior to importing the files, you must obtain a valid X.509 certificate and private key that is issued by your internal CA, and the certificate must correspond to a private key in your possession. After importing the files, the security functionality that is based on the X.509 certificate and private key is automatically activated. Catalyst Center presents the certificate to any device or application that requests it. Northbound API applications and network devices can use these credentials to establish a trust relationship with Catalyst Center.

Note We recommend that you do not use and import a self-signed certificate to Catalyst Center. We recommend that you import a valid X.509 certificate from your internal CA. Additionally, you must replace the self-signed certificate (installed in Catalyst Center by default) with a certificate that is signed by your internal CA for the Plug and Play functionality to work correctly.

Catalyst Center supports only one imported X.509 certificate and private key at a time. When you import a second certificate and private key, the latter overwrites the first (existing) imported certificate and private key values.

Certificate chain support

Catalyst Center is able to import certificates and private keys through its GUI. If subordinate certificates are involved in a certificate chain leading to the certificate that is to be imported into Catalyst Center (signed certificate), both the subordinate certificates as well as the root certificate of these subordinate CAs must be appended together into a single file to be imported. When appending these certificates, you must append them in the same order as the actual chain of certification.

The following certificates should be pasted together into a single PEM file. Review the certificate subject name and issuer to ensure that the correct certificates are being imported and correct order is maintained. Ensure that all of the certificates in the chain are pasted together.

- **Signed Catalyst Center certificate**: Its Subject field includes CN=<*FQDN of Catalyst Center*>, and the issuer has the CN of the issuing authority.

Note If you install a certificate signed by your internal certificate authority (CA), ensure that the certificate specifies all of the DNS names (including the Catalyst Center FQDN) that are used to access Catalyst Center in the **alt_names** section. For more information, see "Generate a Certificate Request Using Open SSL" in the Catalyst Center Security Best Practices Guide.

- **Issuing (subordinate) CA certificate that issues the Catalyst Center certificate**: Its Subject field has CN of the (subordinate) CA that issues the Catalyst Center certificate, and the issuer is that of the root CA.
- **Next issuing (root/subordinate CA) certificate that issues the subordinate CA certificate**: Its Subject field is the root CA, and the issuer has the same value as the Subject field. If they are not the same, you must append the next issuer, and so on.

Update the Catalyst Center server certificate

Catalyst Center allows you to import and store an X.509 certificate from your certificate authority (CA) and private key that's generated by Catalyst Center. These can be used to create a secure and trusted environment between Catalyst Center, northbound API applications, and network devices. You can import a certificate and a private key on the **System Certificates** window.

To update the Catalyst Center server certificate:

1. Generate a Certificate Signing Request (CSR).
2. Submit the CSR to your CA to get a signed certificate.
3. Import the signed certificate and its chain into Catalyst Center.

This procedure uses Microsoft Active Directory Certificate Services as an example CA. If you use a different CA, adapt the steps accordingly.

Before you begin

You must obtain a valid X.509 certificate from your internal CA that corresponds to your private key.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **System Certificates**.

When you first view the **System Certificates** window, the current certificate data is displayed in the Catalyst Center self-signed certificate. The self-signed certificate expires one year after its creation date.

This window displays information about Catalyst Center server certificates and provides actions to manage those certificates. The **System Certificates** table displays this information for each certificate:

- **Issued To**: Indicates who the certificate was issued to.
- **Issued By**: Name of the entity that has signed and issued the certificate.
- **Used For**: Indicates whether the certificate is used for controller, disaster recovery, or both.
- **Certificate Serial Number**: Shows the last five characters of the certificate serial number.
- **Time Left**: Time left in the certificate life.
- **Status**: Shows the certificate status.
- **Valid From/Valid To**: Indicates when the certificate is valid.

  Note
  The certificate's valid dates and times display as a Greenwich Mean Time (GMT) value. A system notification displays in the notification center two months before the certificate expires. Click the notifications icon in the top-right corner of the window to view it.

- **Action**: Shows available actions to manage the certificate, such as replace or delete.

Step 2 Click **+ New Certificate Request (CSR)**.

This **+ New Certificate Request (CSR)** link is enabled when you generate the CSR for the first time.

If you don't want to use the existing CSR, delete the existing request.

a. In the table, locate the request that you want to delete.

b. Under **Action**, hover your cursor over the vertical ellipsis (⋮) and click **Delete** for that request.

c. In the **Delete CSR(s)** dialog box, check the **Controller** check box to indicate that you want to delete the CSR for the controller. Then, click **Delete**.

The **+ New Certificate Request (CSR)** link is enabled.

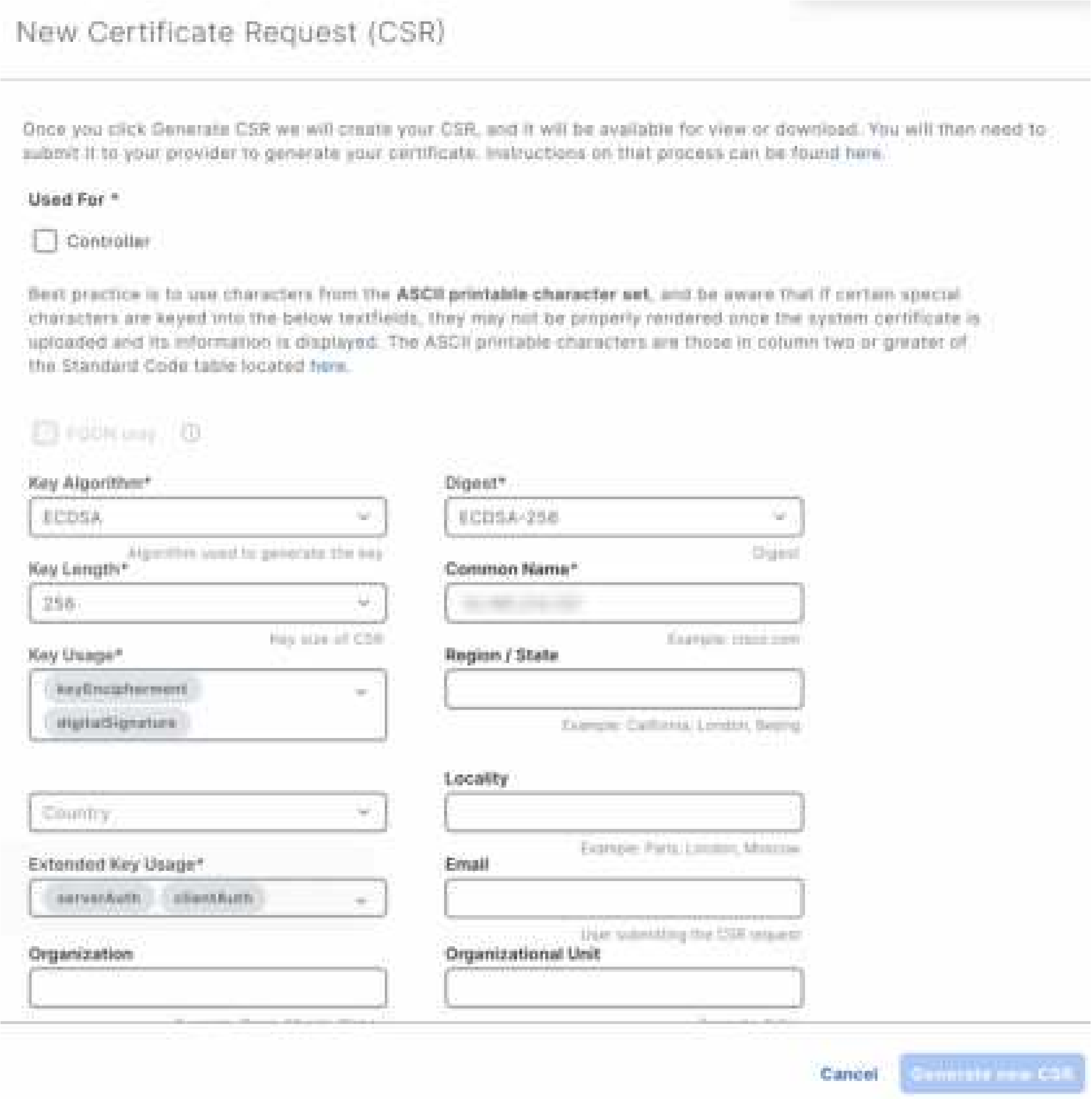
Step 3 In the **New Certificate Request (CSR)** slide-in pane, create the CSR.

a. Under **Used For**, check the **Controller** check box to use the CSR for the controller.

b. Enter the values for these required fields:

  - **Key Algorithm**: The algorithm used to generate the key.
  - **Digest**: The digest algorithm used to secure and verify the CSR.
  - **Key Length**: The certificate key's bit size.

- **Common Name**: The server's IP address, hostname, or FQDN.
- **Key Usage**: Purpose of the certificate's key. See RFC 5280, Section 4.2.1.3 for a description of the available values.
- **Extended Key Usage**: Additional purpose of the certificate's key. See RFC 5280, Section 4.2.1.12 for a description of the available values.



New Certificate Request (CSR)

Once you click Generate CSR we will create your CSR, and it will be available for view or download. You will then need to submit it to your provider to generate your certificate. Instructions on that process can be found here.

Used For *

□ Controller

Best practice is to use characters from the **ASCII printable character set**, and be aware that if certain special characters are keyed into the below textfields, they may not be properly rendered once the system certificate is uploaded and its information is displayed. The ASCII printable characters are those in column two or greater of the Standard Code table located here.

□ FQDN only

Key Algorithm*: ECDSA (Algorithm used to generate the key)

Digest*: ECDSA-256 (Digest)

Key Length*: 256 (Key size of CSR)

Common Name*: [redacted] (Example: cisco.com)

Key Usage*: keyEncipherment, digitalSignature

Region / State: (Example: California, London, Beijing)

Country

Locality: (Example: Paris, London, Moscow)

Extended Key Usage*: serverAuth, clientAuth

Email: (User submitting the CSR request)

Organization

Organizational Unit

c. Click **Generate new CSR**.

Step 4 Download a copy of the CSR.

a. Under **Issued To**, click the hyperlinked text for the CSR.

b. In the **Certificate Signing Request** slide-in pane, click **Download CSR**.

The CSR is downloaded locally as a Base64 file.

c. Click **Done** to close the slide-in pane.

Step 5 Submit a certificate request to the CA and download the issuer CA chain from the CA.

For example, you can submit a certificate request using Microsoft Active Directory Certificate Services by following these steps.

a. Copy the CSR that you just downloaded.

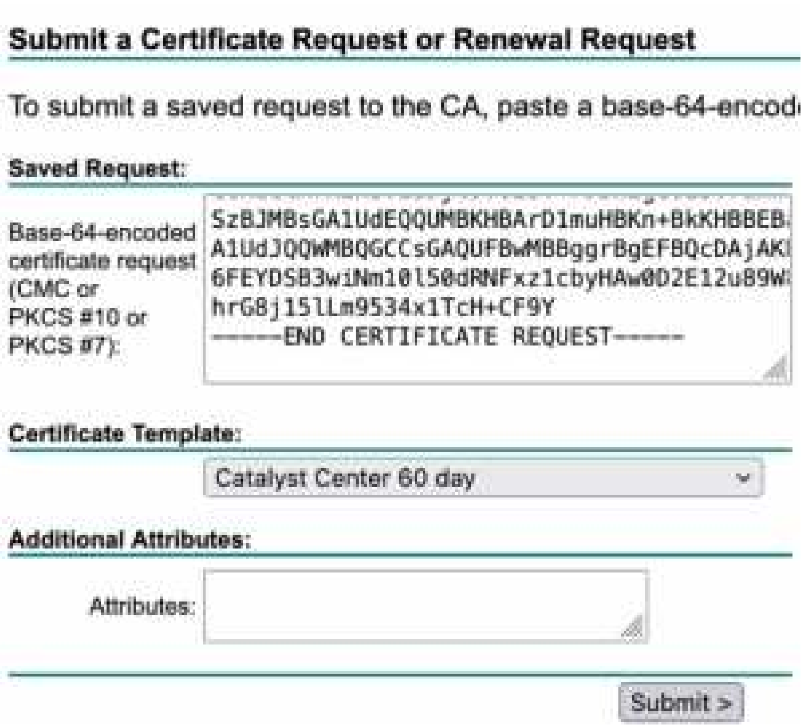
b. Open Active Directory Certificate Services in a new browser window.

c. On the **Welcome** page, click **Request a certificate**.

d. On the **Request a Certificate** page, click **advanced certificate request**.

e. On the **Submit a Certificate Request or Renewal Request** page, paste the request in the **Saved Request** field, select a certificate template, and click **Submit**.

Ensure that the selected certificate template is configured for both client and server authentication.



Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encod

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
SzBJMBsGA1UdEQQUMBKHBArD1muHBKn+BkKHBBEB
A1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAK
6FEYDSB3wiNm10l50dRNFxz1cbyHAw0D2E12u89W
hrG8j15lLm9534x1TcH+CF9Y
-----END CERTIFICATE REQUEST-----
```

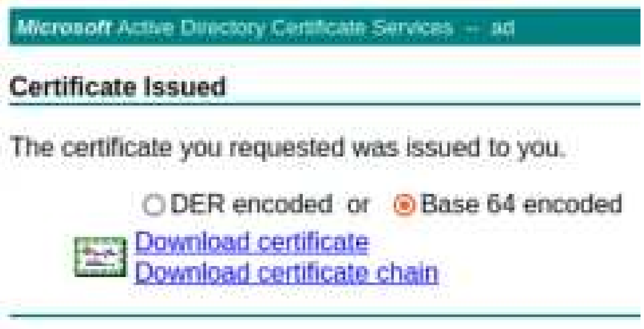
Certificate Template: Catalyst Center 60 day

Additional Attributes:

Attributes:

f. On the **Certificate Issued** page, select how you want the certificate encoded and click **Download certificate chain**.

The certificate chain is downloaded from the CA.



Microsoft Active Directory Certificate Services -- ad

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

Step 6 Confirm that the certificate issuer provided the certificate full chain (server and CA) in p7b. When in doubt, complete these steps to examine and assemble the chain:

a) Download the p7b bundle in DER format and save it as server-cert-chain.p7b.

b) Enter this command:

```
openssl pkcs7 -in server-cert-chain.p7b -inform DER -out server-cert-chain.pem -print_certs
```

Step 7 On the Catalyst Center GUI, in the **+ System Certificates** window, click **Import** under **Action** for the CSR.

Step 8 In the **Import Certificate** slide-in pane, import the signed certificate with its certificate signed authority chain concatenated into Catalyst Center.

a. Under **Used For**, check the **Controller** check box to use this certificate for the controller.

b. Under **Type**, select the file format type for the certificate using this table.

Type	Description	Action
PEM Chain	Privacy-enhanced mail file format.	Click **PEM Chain**. If the certificate issuer provides the certificate and its issuer CA chain in loose files, complete these steps. **1.** Gather the PEM (base64) files or use OpenSSL to convert DER files to the PEM format. **2.** Concatenate the certificate and its issuer CA, starting with the certificate, followed by subordinate CA, all the way to the root CA, and output it to the server-cert-chain.pem file. cat certificate.pem subCA.pem rootCA.pem > server-cert-chain.pem
PKCS	Public-Key Cryptography Standard file format.	Click **PKCS**. **Note** **PKCS** file type is disabled if you chose the **+ New Certificate Request (CSR)** option to request a certificate.

c. Depending on the type of file chosen, upload the file.

If you upload a...	Then...
PEM file and, if applicable, the private key,	1. Drag and drop the PEM and private key files. **Note** • A PEM file must have a valid PEM format extension (.pem, .cer, or .crt). The maximum file size for the certificate is 1 MB. • Private keys must have a valid private key format extension (.key). The maximum file size for the private key is 1 MB. • If you used **+ New Certificate Request (CSR)** to create a CSR, there is no private key to import. The private key is stored within Catalyst Center. 2. For the private key, under **Encrypted**, indicate if you want it encrypted. If you indicate **Yes**, enter the password for the private key in the **Password** field.
PKCS file	1. In the **Bundle Password** field, enter the password for the certificate. 2. Drag and drop the PKCS file. **Note** A PKCS file must have a valid PKCS format extension (.pfx or .p12). The maximum file size for the certificate is 1 MB. After the upload succeeds, the system certificate is validated.

d. Click **Submit**.

Note
After the Catalyst Center server SSL certificate is replaced, you are automatically logged out. Because importing the certificate can take about two minutes, wait at least two minutes before logging back in.

Step 9 After logging back in to Catalyst Center, go to the **System Certificates** window to view the updated certificate data.

For the updated certificate, under **Action**, hover your cursor over the vertical ellipsis (⋮) and click **View** to view a slide-in pane with information about the certificate, such as the valid dates.

Manage device certificates

You can view and manage certificates that are issued by Catalyst Center for managed devices to authenticate and identify the devices.

As a best practice, when a device is no longer managed by Catalyst Center (for example, because the device is lost or no longer active), revoke or delete the device certificate.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **Device Certificates**.

The **Device Certificate** window shows the status of issued certificates in separate status tabs:

- **Expired**: Shows the list of expired certificates.
- **Expiring**: Shows the list of certificates that are nearing the expiry date in ascending order.
- **All**: Shows the list of valid, expired, and expiring certificates.
- **Revoked**: Shows the list of revoked certificates.

Step 2 To revoke a valid certificate:

a) Click **All**.
b) In the **Actions** column, click the **Revoke** icon that corresponds to the certificate that you want to revoke.
c) In the confirmation window, click **OK**.

Step 3 To delete an expired certificate:

a) Click the **All**.
b) In the **Actions** column, click the **Delete** icon that corresponds to the certificate that you want to delete.
c) In the confirmation window, click **OK**.

Step 4 If you want to export the certificate details, click **Export**.

The certificate details are exported in CSV format.

Configure the device certificate lifetime

Catalyst Center lets you change the certificate lifetime of network devices that the private (internal) Catalyst Center CA manages and monitors. The Catalyst Center default value for the certificate lifetime is 365 days. After the certificate lifetime value is changed using the Catalyst Center GUI, network devices that subsequently request a certificate from Catalyst Center are assigned this lifetime value.

Note The device certificate lifetime value cannot exceed the CA certificate lifetime value. Also, if the remaining lifetime of the CA certificate is less than the configured device's certificate lifetime, the device gets a certificate lifetime value that is equal to the remaining CA certificate lifetime.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **Device Certificates**.

Step 2 Review the device certificate and the current device certificate lifetime.

Step 3 In the **Device Certificates** window, click **Modify**.

Step 4 In the **Device Certificates Lifetime** dialog box, enter a new value, in days.

Step 5 Click **Save**.

Certificate authority

A certificate authority (CA) is an entity that manages the certificates and keys that are used to establish and secure server-client connections. Catalyst Center provides a private (internal) Catalyst Center CA, which acts as the device CA. This Catalyst Center CA can either operate as a root CA or be configured as a subordinate CA, which cannot be reversed.

Change the role of the certificate authority from root to subordinate

The device CA, a private CA that is provided by Catalyst Center, manages the certificates and keys that are used to establish and secure server-client connections. To change the role of the device CA from a root CA to a subordinate CA, complete this procedure.

You can change the role of the private (internal) Catalyst Center CA from a root CA to a subordinate CA using the **Certificate Authority** window in the GUI. When making this change:

- If you intend to have Catalyst Center act as a subordinate CA, it is assumed that you already have a root CA, for example, Microsoft CA, and you are willing to accept Catalyst Center as a subordinate CA.
- As long as the subordinate CA is not fully configured, Catalyst Center continues to operate as an internal root CA.
- You must generate a Certificate Signing Request file for Catalyst Center (as described in this procedure) and have it manually signed by your external root CA.

Note Catalyst Center continues to run as an internal root CA during this time period.

- After the Certificate Signing Request is signed by the external root CA, this signed file must be imported back into Catalyst Center using the GUI (as described in this procedure).

  After the import, Catalyst Center initializes itself as the subordinate CA and provides all the existing functionalities of a subordinate CA.
- When switching a CA's role from root to subordinate, the old CA is retired and the new subordinate CA's PKI chain takes over. The revocation list is published by a CA, and after the CA is retired, revocation is moot since trust cannot be established. If your organization's policy mandates that unused certificates are revoked first, you can revoke the certificate from the GUI's **Device Certificates** window before switching the CA's role from root to subordinate.

  Device controllability (enabled by default) will automatically update the device with a new certificate chain, sourced from the subordinate CA. New telemetry connections would only authenticate with this new certificate chain, which aligns with the trusted subordinate CA on the authenticator side.
- The subordinate CA certificate lifetime, as displayed in the GUI, is just read from the certificate; it is not computed against the system time. Therefore, if you install a certificate with a lifespan of 1 year

today and look at it in the GUI the same time next year, the GUI will still show that the certificate has a 1-year lifetime.

- The subordinate CA certificate must be in PEM or DER format only.
- The subordinate CA does not interact with the higher CAs; therefore, it is not aware of revocation, if any, of the certificates at a higher level. Because of this, any information about certificate revocation is also not communicated from the subordinate CA to the network devices. Because the subordinate CA does not have this information, all the network devices use only the subordinate CA as the Cisco Discovery Protocol (CDP) source.
- Consider that if you use EAP-Transport Level Security (EAP-TLS) authentication for AP profiles in Plug and Play (PnP), you cannot use a subordinate CA. You can only use a root CA.

Before you begin

You must have a copy of the root CA certificate.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificate Authority**.

Step 2 Click the **CA Management** tab.

Step 3 Review the existing root or subordinate CA certificate configuration information from the GUI:

- **Root CA Certificate**: Displays the current root CA certificate (either external or internal).
- **Root CA Certificate Lifetime**: Displays the current lifetime value of the current root CA certificate, in days.
- **Current CA Mode**: Displays the current CA mode (root CA or subordinate CA).
- **SubCA Mode**: Enables a change from a root CA to a subordinate CA.

Step 4 In the **CA Management** tab, click **Enable SubCA Mode** button.

Step 5 Review the warnings that display:

For example,

- Changing from root CA to subordinate CA is a process that cannot be reversed.
- You must ensure that no network devices have been enrolled or issued a certificate in root CA mode. Network devices that have been accidentally enrolled in root CA mode must be revoked before changing from root CA to subordinate CA.
- Network devices must come online only after the subordinate CA configuration process finishes.

Step 6 Click **OK** to proceed.

Step 7 Drag and drop your root CA certificate into the **Import External Root CA Certificate Chain** field and click **Upload**.

The root CA certificate is uploaded into Catalyst Center and used to generate a Certificate Signing Request.

After the upload process finishes, a `Certificate Uploaded Successfully` message is displayed.

Step 8 Click **Next**.

Catalyst Center generates and displays the Certificate Signing Request.

Step 9 View the Catalyst Center-generated Certificate Signing Request in the GUI and do one of these actions:

- Click the **Download** link to download a local copy of the Certificate Signing Request file.

  You can then attach this Certificate Signing Request file to an email to send to your root CA.

- Click the **Copy to the Clipboard** link to copy the Certificate Signing Request file's content.

  You can then paste this Certificate Signing Request content to an email or include it as an attachment to an email and send it to your root CA.

Step 10 Send the Certificate Signing Request file to your root CA.

Your root CA will then return a subordinate CA file, which you must import back into Catalyst Center.

Step 11 After receiving the subordinate CA file from your root CA, access the Catalyst Center GUI again and return to the **Certificate Authority** window.

Step 12 Click the **CA Management** tab.

Step 13 Click **Yes** for the **Change CA mode** button.

After clicking **Yes**, the GUI view with the Certificate Signing Request display.

Step 14 Click **Next**.

The **Certificate Authority** window displays the **Import SubCA Certificate** field.

Step 15 Drag and drop your subordinate CA certificate into the **Import SubCA Certificate** field and click **Apply**.

The subordinate CA certificate is uploaded into Catalyst Center.

After the upload finishes, the GUI displays the subordinate CA mode under the **CA Management** tab.

Step 16 Review the fields under the **CA Management** tab:

- **Sub CA Certificate**: Displays the current subordinate CA certificate.
- **External Root CA Certificate**: Displays the root CA certificate.
- **Sub CA Certificate Lifetime**: Displays the lifetime value of the subordinate CA certificate, in days.
- **Current CA Mode**: Displays SubCA mode.

Provision a rollover subordinate CA certificate

Catalyst Center lets you apply a subordinate certificate as a rollover subordinate CA when 70 percent of the existing subordinate CA lifetime has elapsed.

Before you begin

- To initiate subordinate CA rollover provisioning, you must have changed the certificate authority role to subordinate CA mode. See Change the role of the certificate authority from root to subordinate, on page 100.

- 70 percent or more of the lifetime of the current subordinate CA certificate must have expired. When this occurs, Catalyst Center displays a **Renew** button under the **CA Management** tab.
- You must have a signed copy of the rollover subordinate CA certificate.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **Certificate Authority**.

Step 2 In the **CA Management** tab, review the CA certificate configuration information:

- **Subordinate CA Certificate**: Displays the current subordinate CA certificate.
- **External Root CA Certificate**: Displays the root CA certificate.
- **Subordinate CA Certificate Lifetime**: Displays the lifetime value of the current subordinate CA certificate, in days.
- **Current CA Mode**: Displays SubCA mode.

Step 3 Click **Renew**.

Catalyst Center uses the existing subordinate CA to generate and display the rollover subordinate CA Certificate Signing Request.

Step 4 View the generated Certificate Signing Request in the GUI and do one of these actions:

- Click the **Download** link to download a local copy of the Certificate Signing Request file.

  You can then attach this Certificate Signing Request file to an email to send it to your root CA.

- Click the **Copy to the Clipboard** link to copy the content of the Certificate Signing Request file.

  You can then paste this Certificate Signing Request content to an email or include it as an attachment to an email and send it to your root CA.

Step 5 Send the Certificate Signing Request file to your root CA.

Your root CA will then return a rollover subordinate CA file that you must import back into Catalyst Center.

The Certificate Signing Request for the subordinate CA rollover must be signed by the same root CA who signed the subordinate CA you imported when you switched from RootCA mode to SubCA mode.

Step 6 After receiving the rollover subordinate CA file from your root CA, return to the **Certificate Authority** window.

Step 7 Click the **CA Management** tab.

Step 8 Click **Next** in the GUI in which the Certificate Signing Request displays.

The **Certificate Authority** window displays the **Import Sub CA Certificate** field.

Step 9 Drag and drop your subordinate rollover CA certificate into the **Import Sub CA Certificate** field and click **Apply**.

The rollover subordinate CA certificate is uploaded into Catalyst Center.

After the upload finishes, the GUI changes to disable the **Renew** button under the **CA Management** tab.

Use an external SCEP broker

Catalyst Center uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and the provisioning of certificates to network devices. You can use your own SCEP broker and certificate service, or you can use an external SCEP broker. To set up an external SCEP broker, complete this procedure:

Note For more information regarding SCEP, see Simple Certificate Enrollment Protocol Overview.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **Certificate Authority**.

Step 2 In the **Certificate Authority** window, click the **Use external SCEP broker** radio button.

Step 3 Use one of these options to upload an external certificate:

- Choose a file
- Drag and drop to upload

Note
Only file types such as .pem, .crt, and .cer are accepted. The file size cannot exceed 1 MB.

Step 4 Click **Upload**.

Step 5 By default, **Manages Device Trustpoint** is enabled, meaning Catalyst Center configures the sdn-network-infra-iwan trustpoint on the device. You must complete these steps:

a) Enter the enrollment URL where the device requests the certificate via SCEP.

b) (Optional) Enter any optional subject fields used by the certificate, such as country, locality, state, organization, and organization unit. The common name (CN) is automatically configured by Catalyst Center with the device platform ID and device serial number.

c) In the **Revocation Check** field, click the drop-down list and choose the appropriate revocation check option.

d) (Optional) Check the **Auto Renew** check box and enter an auto enrollment percentage.

If **Manages Device Trustpoint** is disabled, for devices to send wired and wireless Assurance telemetry to Catalyst Center, you must manually configure the sdn-network-infra-iwan trustpoint on the device and then import a certificate. See Configure the Device Certificate Trustpoint.

Step 6 Click **Save**.

The external CA certificate is uploaded.

If you want to replace the uploaded external certificate, click **Replace Certificate** and enter the required details.

Switch back to an internal certificate authority

After uploading an external certificate, to switch back to the internal certificate:

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **Certificate Authority**.

Step 2 In the **Certificate Authority** window, click the **Use Catalyst Center** radio button.

Step 3 In the **Switching back to Internal Certificate Authority** alert, click **Apply**.

The **Settings have been updated** message appears. For more information, see Change the role of the certificate authority from root to subordinate, on page 100.

Export the Catalyst Center certificate authority

Catalyst Center allows you to download the device certificates that are required to set up an external entity such as an AAA server or a Cisco ISE server to authenticate the devices.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **Certificate Authority**.

Step 2 Click **Download** to export the device CA and add it as the trusted CA on the external entities.

Configure the device certificate trustpoint

If **Manages Device Trustpoint** is disabled in Catalyst Center, for devices to send wired and wireless Assurance telemetry to Catalyst Center, you must manually configure the sdn-network-infra-iwan trustpoint on the device and then import a certificate.

This manual configuration procedure is required to enroll from an external CA via SCEP.

Procedure

Step 1 Enter the following commands:

```
crypto pki trustpoint sdn-network-infra-iwan
  enrollment url http://<SCEP_enrollment_URL_to_external_CA>
  fqdn <device_FQDN>
  subject-name CN=<device_platform_ID>_<device_serial_number>_sdn-network-infra-iwan
  revocation-check <crl, crl none, or none>  # to perform revocation check with CRL, CRL fallback to
 no check, or no check
  rsakeypair sdn-network-infra-iwan
  fingerprint <CA_fingerprint> # to verify that the CA at the url connection matches the fingerprint
 given
```

Step 2 (Optional, but recommended) Automatically renew the certificate and avoid certificate expiry:

```
auto-enroll 80 regenerate
```

Step 3 (Optional) Specify the interface that is reachable to the enrollment URL. Otherwise, the default is the source interface of the http service.

```
source interface <interface>
```

Configure trusted certificates

Catalyst Center contains a preinstalled Cisco trusted certificate bundle (Cisco Trusted External Root Bundle). Catalyst Center also supports the import and storage of an updated trusted certificate bundle from Cisco. The trusted certificate bundle is used by supported Cisco networking devices to establish a trust relationship with Catalyst Center and its applications.

Note The Cisco trusted certificate bundle is a file called ios.p7b that only supported Cisco devices can unbundle and use. This ios.p7b file contains root certificates of valid certificate authorities, including Cisco. This Cisco trusted certificate bundle is available on the Cisco cloud (Cisco InfoSec). The bundle is located at https://www.cisco.com/security/pki/.

The trusted certificate bundle provides you with a safe and convenient way to use the same CA to manage all your network device certificates, as well as your Catalyst Center certificate. Catalyst Center uses the trusted certificate bundle to validate its own certificate and any proxy gateway certificate and to determine whether the certificates are valid CA-signed certificates. Additionally, the trusted certificate bundle is available for upload to Network PnP-enabled devices at the beginning of their PnP workflow so that they can trust Catalyst Center for subsequent HTTPS-based connections.

You import the Cisco trusted bundle using the **Trusted Certificates** window in the GUI.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **Trusted Certificates**.

Step 2 In the **Trusted Certificates** window, click the **Update trusted certificates now** hyperlink to initiate a new download and install of the trusted certificate bundle.

The hyperlink is displayed on the window only when an updated version of the ios.p7b file is available and internet access is available.

After the new trusted certificate bundle is downloaded and installed on Catalyst Center, Catalyst Center makes this trusted certificate bundle available to supported Cisco devices for download.

Step 3 If you want to import a new certificate file, click **Import**, choose a valid certificate file from your local system, and click **Import** in the **Import Certificate** window.

Step 4 Click **Export** to export the certificate details in CSV format.

About restricted shell

For added security, access to the root shell is disabled. With restricted shell, users can't access the underlying operating system and file system, which reduces operational risk.

Restricted shell is enabled for security purposes. However, if you want to access the root shell temporarily, you must contact the Cisco TAC for assistance.

If necessary, you can use the following restricted list of commands:

Table 5: Restricted Shell Commands

Command	Description
cat	Concatenate and print files in restricted mode.
clear	Clear the terminal screen.
date	Display the current time in the given format or set the system date.
debug	Enable console debug logs.
df	File system information.
dmesg	Print or control the kernel ring buffer.
du	Summarize disk usage of the set of files recursively for directories.
free	Quick summary of memory usage.
history	Enable shell commands history.
htop	Interactive process viewer.
ip	Print routing, network devices, interfaces and tunnels.
kubectl	Interact with Kubernetes Cluster in a restricted manner.
last	Show a listing of last logged in users.
ls	Restricted file system view chrooted to maglev Home.
lscpu	Print information about the CPU architecture.
magctl	Tool to manage a Maglev deployment.
maglev-config	Tool to configure a Maglev deployment.
manufacture_check	Tool to perform manufacturing checks.
netstat	Print networking information.
nslookup	Query internet name servers interactively.
ntpq	Standard NTP query program.
ping	Send ICMP ECHO_REQUEST to network hosts.

Command	Description
ps	Check status of active processes in the system.
rca	Root cause analysis collection utilities.
reboot	Reboot the machine.
rm	Delete files in restricted mode.
route	Print the IP routing table.
runonce	Execute runonce scripts.
scp	Restricted secure copy.
sftp	Secure file transfer.
shutdown	Shut down the machine.
ssh	OpenSSH SSH client.
tail	Print the last 10 lines of each file to standard output.
top	Display a sorted list of system processes.
traceroute	Print the route packets trace to network host.
uname	Print system information.
uptime	Tell how long the system has been running.
vi	Text editor.
w	Show who is logged on and what they are doing.

About product telemetry

Product telemetry data is collected by default in Catalyst Center, but you can opt out of some data collection. The data collection is designed to help the development of product features and address any operational issues, providing greater value and return on investment (ROI). Cisco collects the following categories of data: Cisco.com ID, System, Feature Usage, Network Device Inventory, and License Entitlement. See the *Cisco Catalyst Center Data Sheet* for a more expansive list of data that we collect. To opt out of some of data collection, contact your Cisco account representative and the Cisco Technical Assistance Center (TAC).

From the main menu, choose **System** > **Settings** > **Terms and Conditions** > **Product Telemetry**. You can review the license agreement, the privacy statement, and the privacy data sheet from the **Product Telemetry** window.

Account lockout

You can configure the account lockout policy to manage user login attempts, account lockout period, and number of login retries.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Trust & Privacy** > **Account Lockout**.

Step 2 Click the **Enforce Account Lockout** toggle button so that you see a check mark.

Step 3 Enter values for these **Enforce Account Lockout** parameters:

- Maximum Login Retries
- Lockout Effective Periods (minutes)
- Reset Login Retries after (minutes)

Note
Hover your cursor over **Info** to view details for each parameter.

Step 4 Select the **Idle Session Timeout** value (the duration after which the session expires and users are redirected to the login page). The default is 1 hour.

Step 5 Click **Save**.

If you leave the session idle, a **Session Timeout** dialog box appears five minutes before the session timeout.

To continue, do one of these tasks:

- If you want to continue the session, click **Stay signed in**.
- To end the session immediately, click **Sign out**.

Password expiry

You can configure the password expiration policy to manage:

- Password expiration frequency
- Number of days that users are notified before their password expires
- Grace period

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Trust & Privacy** > **Password Expiry**.

Step 2 Click the **Enforce Password Expiry** toggle button so that you see a check mark.

Step 3 Enter values for the following **Enforce Password Expiry** parameters:

- Password Expiry Period (days)
- Password Expiration Warning (days)
- Grace Period (days)

Note
Hover your cursor over **Info** to view details for each parameter.

Step 4 Click **Save** to set the password expiry settings.

IP access control

IP access control allows you to control the access to Catalyst Center based on the IP address of the host or network. This feature controls access to the Catalyst Center GUI only; this feature doesn't control enterprise-wide network access.

Catalyst Center provides options for IP access control, including:

- Allow all IP addresses to access Catalyst Center (the default).
- Allow only selected IP addresses to access Catalyst Center.

Configure IP access control

To configure IP access control and allow only selected IP addresses to access Catalyst Center:

1. Enable IP access control, on page 110
2. Add an IP address to the IP access list, on page 111
3. (Optional) Delete an IP address from the IP access list, on page 112

Enable IP access control

Before you begin

- Ensure that you have SUPER-ADMIN-ROLE permissions.
- Add the Catalyst Center services subnet, cluster service subnet, and cluster interface subnet to the list of allowed subnets.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 Click the **Allow only listed IP addresses to connect** radio button.

Step 3 Click **Add IP List**.

Step 4 In the **IP Address** field of the **Add IP** slide-in pane, enter your IPv4 address.

Note
If you don’t add your IP address to the IP access list, you may lose access to Catalyst Center.

Step 5 In the **Subnet Mask** field, enter the subnet mask.

The valid range for subnet mask is from 0 through 32.

Step 6 Click **Save**.

Add an IP address to the IP access list

To add more IP addresses to the IP access list:

Before you begin

Ensure that you enable IP access control. For more information, see Enable IP access control, on page 110.

Procedure

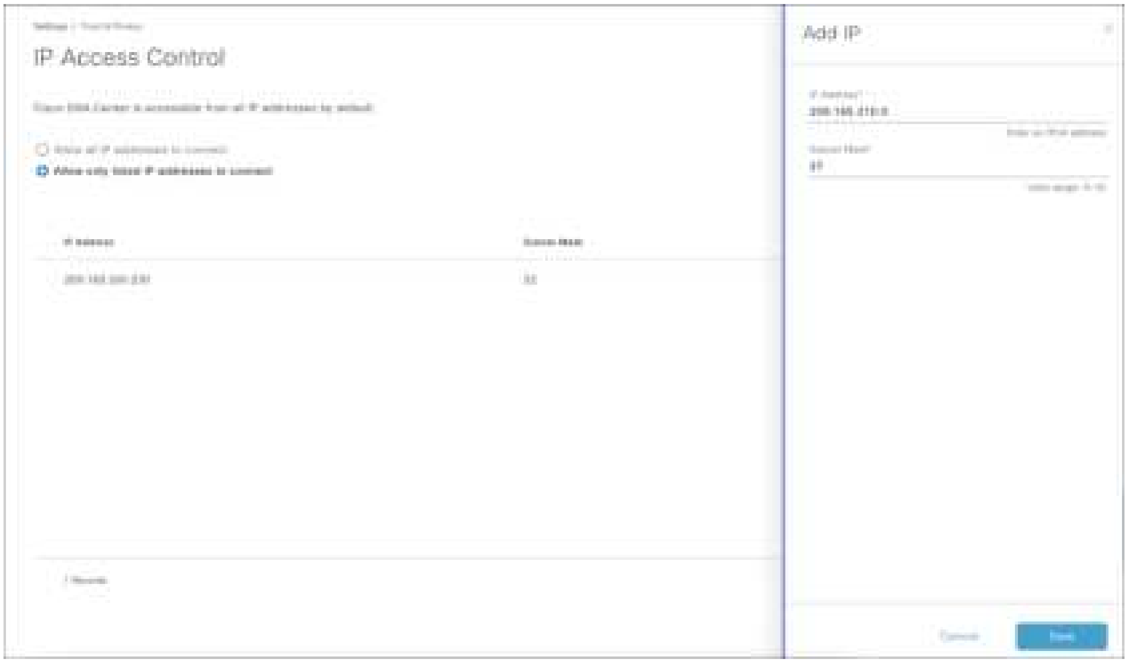
Step 1 From the main menu, choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 Click **Add**.

Step 3 In the **IP Address** field of the **Add IP** slide-in pane, enter the IPv4 address of the host or network.

Step 4 In the **Subnet Mask** field, enter the subnet mask.

The valid range for subnet mask is from 0 through 32.



Step 5 Click **Save**.

Delete an IP address from the IP access list

To delete an IP address from the IP access list and disable its access to Catalyst Center:

Before you begin

Ensure that you have enabled IP access control and added IP addresses to the IP access list. For more information, see Enable IP access control, on page 110 and Add an IP address to the IP access list, on page 111.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 In the **Action** column, click the **Delete** icon for the corresponding IP address.

Step 3 Click **Delete**.

Disable IP access control

To disable IP access control and allow all IP addresses to access Catalyst Center:

Before you begin

Ensure that you have SUPER-ADMIN-ROLE permissions.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 Click the **Allow all IP addresses to connect** radio button.

CHAPTER 3

Manage Applications

Application management

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

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

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

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

Note

- We recommend against using any CLI command for package management activities. If you encounter issues with package install or upgrade tasks in Catalyst Center, contact Cisco TAC for assistance.
- From the **Software Maintenance** window, you can also upgrade to the latest available Catalyst Center release. For upgrade instructions, see the *Cisco Catalyst Center Upgrade Guide*.

Download and install applications

Catalyst Center treats individual applications as separate from the core infrastructure. Specifically, individual packages for applications can be installed to run on Catalyst Center.

Packages for applications may take time to install and deploy. Therefore, install the packages during a maintenance period for your network.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Software Management**.

Important
At this point, Catalyst Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window won’t display the applications that are currently available.

Step 2 At the bottom of the window, choose which applications to install.

You can either

- choose all available applications by clicking **Select All**, or
- choose individual applications by checking the check box in the corresponding application card.

Note
You can view more details about an available application by clicking **View Details** in any application card.

Step 3 Click **Install**.

Note
During installation, dependencies are checked and installed automatically.

At the top of the window, an in-progress banner message is displayed.

To view real-time, in-progress details, click **View Release Activities**. For the relevant activity, hover your cursor over the ellipsis (···) in the **Actions** column and choose **View Status**.

Step 4 Click **View Installed Applications** and confirm that the selected applications are installed.

Package download and upgrade event notifications

You can receive a notification whenever a package download or upgrade event takes place. To configure and subscribe to these notifications, complete the steps described in the *Work with Event Notifications* topic of the *Cisco Catalyst Center Platform User Guide*. When completing this procedure, ensure that you select and subscribe to the SYSTEM-SOFTWARE-UPGRADE-v2 event.

A notification is generated and sent when:

- The download of a package upgrade failed. This failure typically happens because your Catalyst Center appliance doesn't have the necessary disk space or you're attempting to download a corrupted package.
- The installation of a package upgrade failed (possibly because the service that's associated with the package is currently down).
- The download or installation of a package upgrade succeeded.

Note A notification is sent only if the previous attempt to complete the operation failed.

View an upgrade summary report

From the **Upgrade Summary Report** slide-in pane, you can view the results of the latest upgrade of Catalyst Center and its applications. This report allows you to:

- Identify the previous Catalyst Center version that was installed on your appliance.
- Determine when the upgrade took place.
- In the **Post-check** tab, see whether the post-upgrade checks Catalyst Center makes completed successfully. If a problem occurs for a particular check, click its information (**i**) icon in the **Issues** column for a description of the problem.
- In the **Packages** tab, view the application packages that were upgraded and their current version number.

Complete the following steps to open this report.

Procedure

Step 1 From the main menu, choose **System** > **Software Management**.

Step 2 Click the **Upgrade Summary Report** link.

Uninstall an application

Catalyst Center treats individual applications as separate from the core infrastructure. Specifically, individual packages for applications can be uninstalled from Catalyst Center.

You can uninstall only packages for applications that are not system critical.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Software Management**.

Step 2 Click **View Installed Applications** to view all the applications that are installed on Catalyst Center.

Step 3 For the package that you want to remove, check its **Uninstall** check box.

Note

- You can uninstall multiple packages simultaneously.
- You can uninstall only optional packages.

Step 4 Click **Uninstall** to confirm that you want to uninstall the application.

At the top of the window, an in-progress banner message is displayed. To view real-time, in-progress details, click **View Release Activities** on the **Software Management** window. For the relevant activity, hover your cursor over the ellipsis (•••) in the **Actions** column and choose **View Status**.

Step 5 Click **View Installed Applications** and confirm that the application is uninstalled.

CHAPTER 4

Manage Users

About user profiles

A user profile defines the login, password, email, and role (permissions) of a user.

You can configure both internal and external profiles for users. Internal user profiles reside in Catalyst Center, and external user profiles reside on an external AAA server.

A default user profile with SUPER-ADMIN-ROLE permissions is created when you install Catalyst Center.

About user roles

Users are assigned user roles that specify the functions that they are permitted to perform:

- **Administrator (SUPER-ADMIN-ROLE)**: Users with this role have full access to all of the Catalyst Center functions. They can create other user profiles with various roles, including those with the SUPER-ADMIN-ROLE.
- **Network Administrator (NETWORK-ADMIN-ROLE)**: Users with this role have full access to all of the network-related Catalyst Center functions. However, they do not have access to system-related functions, such as backup and restore.
- **Observer (OBSERVER-ROLE)**: Users with this role have view-only access to the Catalyst Center functions. Users with an observer role cannot access any functions that configure or control Catalyst Center or the devices it manages.
- **Customized Role**: User with SUPER-ADMIN-ROLE privileges can define custom roles that permit or restrict user access to certain Catalyst Center functions.

Create an internal user

You can create a user and assign this user a role.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **User Management**.

Step 2 Click **Add**.

Step 3 Enter a first name, last name, email address, and username for the new user.

The email address must meet the requirements for the standard Apache EmailValidator class.

Step 4 Under **Role List**, choose one of the following roles: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.

Step 5 Enter a password and confirm it.

Step 6 Click **Save**.

Edit a user

You can edit some user properties (but not the username).

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to edit.

Step 3 Click **Edit**.

Step 4 Edit the first or last name or email address, if needed.

Step 5 Under **Role List**, choose a new role, if needed: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.

Step 6 Click **Save**.

Delete a user

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to delete.

Step 3 Click **Delete**.

Step 4 At the confirmation prompt, click **Continue**.

Password policy

After you have deployed Catalyst Center, keep these points regarding password policy in mind:

- The default password for the maglev user and admin superuser is **P@ssword9**.

  You are prompted to change the admin superuser's password after you log in to the Catalyst Center GUI for the first time.

- When you change any user's password, or configure a new role-based access control (RBAC) user, their password must comply with the new requirements.

See Password requirements, on page 122 for a description of the criteria that newly created user passwords must meet.

Password requirements

Any user password you configure in Catalyst Center 2.3.7.9 or later must meet these requirements:

- It is at least nine characters in length.
- It contains characters from at least three of these categories:
  - Uppercase letters (A–Z)
  - Lowercase letters (a–z)
  - Numbers (0 through 9)
  - Special characters (such as !, $, and #)
- It doesn't use more than four consecutive characters on an English QWERTY keyboard.

  For example, `59Asdfpj!` is not a valid password because it contains the characters `a`, `s`, `d`, and `f` in succession.
- It doesn't contain two or more consecutive characters from the associated username.
- It doesn't contain a complete word found in any language or a phrase that's based on personal information.

Note You can reuse a previous password only after 24 different passwords have been used.

Reset a user password

You can reset another user's password.

For security reasons, passwords are not displayed to any user, not even to the users with administrator privileges.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user whose password you want to reset.

Step 3 From the **More Actions** drop-down list, click **Reset Password**.

Step 4 Enter a new password and confirm it.

Step 5 Click **Save**.

Change your own user password

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **Change Password**.

Step 2 Enter information in the required fields.

Step 3 Click **Update**.

Change your own user password without admin permission

The following procedure describes how to change your password without admin permission.

Procedure

Step 1 From the top-right corner, click your displayed username and choose **My Profile and Settings** > **My Account**.

Step 2 In the **Password** field, click **Update Password**.

Step 3 In the **Update Password** dialog box, enter the new password and confirm the new password.

Step 4 Click **Update**.

Reset a forgotten password

If you forgot your password, you can reset it through the CLI.

Note For added security, access to the root shell is disabled in Catalyst Center. With restricted shell, users can't access the underlying operating system and file system, which reduces operational risk. However, the commands in this section require that you contact the Cisco TAC to access the root shell temporarily.

Procedure

Step 1 Enter this command to check if the user is created in the system.

```
magctl user display <username>
```

The command returns the tenant-name, which can be used to reset the password. The output looks similar to:

```
User admin present in tenant TNT0 (where TNT0 is the tenant-name)
```

Step 2 Enter this command and the tenant-name to reset the password.

```
magctl user password update <username> <tenant-name>
```

You are prompted to enter a new password.

Step 3 Enter the new password.

You are prompted to reenter the new password to confirm.

Step 4 Enter the new password.

The password is reset, and you can log in to Catalyst Center using the new password.

Configure role-based access control

Catalyst Center supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict user access to certain Catalyst Center functions and sites.

Use this procedure to define a custom role and then assign a user to that role.

Before you begin

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

Procedure

Step 1 Define a custom role.

a) From the main menu, choose **System** > **Users & Roles** > **Role Based Access Control**.
b) Click **Create a New Role**.
c) If a task overview window opens, click **Let’s do it** to go directly to the workflow.
d) In the **Create a New Role** window, enter a name for the role and then click **Next**.
e) In the **Define the Access** window, click the **>** icon corresponding to the desired function to view the associated features.
f) Set the permission level to **Deny**, **Read**, or **Write** for the desired features and click **Next**.

   If you set the permission level of a feature to **Deny**, the user to whom you assign this role cannot view this feature in the GUI.

   For dependent features, if you override the recommended permission level settings, a warning message indicating the permission level violation of dependent features is shown in the **Summary** window.

g) Review the configuration settings. To make any changes, click **Edit**.
h) Click **Create Role**.

Step 2 To assign a user to the custom role you created, go to **Users & Roles** > **User Management**.

- To assign the custom role to an existing user:

  a. In the **User Management** window, click the radio button corresponding to the user to whom you want to assign the custom role, and then click **Edit**.

  b. In the **Update Internal User** slide-in pane, click the **Roles** drop-down list and choose the custom role.

  c. Click **Save**.

- To assign the custom role to a new user:

  a. In the **User Management** window, click **Add**.

  b. In the **Create Internal User** slide-in pane, enter the first name, last name, and username.

  c. From the **Roles** drop-down list, choose the custom role.

  d. Enter the password and then confirm it.

  e. Click **Save**.

Step 3 If you are an existing user who was logged in when the administrator was updating your access permissions, you must log out of Catalyst Center and then log back in for the new permission settings to take effect.

Catalyst Center user role permissions

Table 6: Catalyst Center user role permissions

Capability	Description	Recommended permission settings for dependent capabilities
Assurance	Assure consistent service levels with complete visibility across all aspects of your network.	—

Capability	Description	Recommended permission settings for dependent capabilities
Monitoring	Monitor and manage the health of your network with issue troubleshooting and remediation, proactive network monitoring, and insights driven by AI Network Analytics. This role lets you: • Resolve, close, and ignore issues. • Run Machine Reasoning Engine (MRE) workflows. • Analyze trends and insights. • Troubleshoot issues, including path trace, sensor dashboards, and rogue management. • Run workflows for rogue and Cisco Advanced Wireless Intrusion Prevention System (aWIPS). These workflows include AP-allowed list, vendor-allowed list, aWIPS profile creation, assigning an aWIPS profile, and so on.	• Network Management > Hierarchy: Read • Network Management > Inventory: Read • Network Design > Profiles and Settings: Read • Utilities > Machine Reasoner: Read • Utilities > Reports: Read • Utilities > App Hosting: Read • Utilities > Command Runner: Read
Settings	Configure and manage issues. Update network, client, and application health thresholds.	• Assurance > Monitoring: Read • Network Management > Hierarchy: Read • Network Management > Inventory: Read • Utilities > App Hosting: Read
Troubleshooting	Create and manage sensor tests. Schedule on-demand forensic packet captures (Intelligent Capture) for troubleshooting clients.	• Assurance > Monitoring: Read • Network Management > Hierarchy: Read • Network Management > Inventory: Read • Network Design > Profiles and Settings: Read • Utilities > Machine Reasoner: Read • Utilities > App Hosting: Read • Utilities > Command Runner: Read
Extensions	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations. **Note** This permission cannot be assigned to a site-scoped (non-global) access group if set to Read/Write.	—

Capability	Description	Recommended permission settings for dependent capabilities
Event Subscription	Subscribe to near real-time notifications of network and system events. Initiate corrective actions. **Note** This permission must be set as Write when ITSM is integrated with Visibility and Control of Configurations.	• System > System Settings: Read
ITSM	Configure and activate preconfigured bundles for ITSM integration. **Note** This permission cannot be assigned to a site-scoped (non-global) access group if set to Read/Write.	• Extensions > Intent API: Write
Intent API	Access the product through REST APIs.	—
Network Design	Configure network profiles and settings. Manage templates. Update the software image repository. Configure wireless maps for managing your sites and network devices.	—
Profiles and Settings	Manage site-wide network settings such as AAA, NTP, DHCP, and so on. Manage telemetry and profiles.	• Network Management > Hierarchy: Read
Wireless Maps	Visualize your wireless network and configure wireless maps.	• Network Management > Hierarchy: Write • Network Management > Inventory: Write • Network Design > Profiles and Settings: Write • Assurance > Monitoring: Read
Network Management	Discover and build your network.	—
Discovery	Discover new devices on your network.	• Network Management > Hierarchy: Write • Network Management > Inventory: Write • Network Design > Profiles and Settings: Read
Hierarchy	Create a network hierarchy of areas, buildings, and floors based on geographic location. This role also includes CMX server settings.	—
Inventory	Add, update, or delete devices on your network. Manage device attributes; view and manage network topology and configurations.	• Network Management > Hierarchy: Read • Network Design > Profiles and Settings: Read

Capability	Description	Recommended permission settings for dependent capabilities
License	Manage software and network assets relative to license usage and compliance. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Read/Write.	• Assurance > Monitoring: Read
Network-wide Settings	Configure network-wide settings to monitor your network and device. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Read/Write.	—
Network Operations	Manage and maintain your network devices.	—
Compliance	Monitor device compliance and out-of-band changes. Manage Cisco field notices and view EoX statuses.	• Network Management > Hierarchy: Read • Network Management > Network-wide Settings: Read • Security > Security Advisory: Read • Network Operations > SWIM: Read
LAN Automation	Provision your network through LAN automation.	• Network Management > Hierarchy: Read • Network Management > Network-wide Settings: Read • Network Management > Inventory: Read • Network Design > Profiles and Settings: Read
Plug and Play	Automatically onboard new devices, assign them to sites, and configure them with site-specific settings.	• Network Management > Hierarchy: Read • Network Management > Network-wide Settings: Read • Network Management > Inventory: Read • Network Design > Profiles and Settings: Read

Capability	Description	Recommended permission settings for dependent capabilities
RMA	Replace faulty devices in your network.	• Network Management > Hierarchy: Read • Network Management > License: Read • Network Management > Inventory: Read • Network Operations > Plug and Play: Write • Network Operations > SWIM: Write
SWIM	Manage software images. Update physical and virtual network entities.	• Network Management > Hierarchy: Read • Network Management > Inventory: Read
Network Provision	Configure, upgrade, provision, and manage network devices.	—
Device Provision	Provision devices with site-specific settings and policies that are configured for the network. This role includes Application Policy, Application Visibility, Cloud, Site-to-Site VPN, Network/Application Telemetry, Security Service Insertion, Stealthwatch, and Umbrella provisioning.	• Network Management > Hierarchy: Read • Network Management > Inventory: Read • Network Design > Profiles and Settings: Read • Network Design > Template: Write • Network Operations > Plug and Play: Write • Network Operations > Compliance: Read • Utilities > Command Runner: Write • System > System Settings: Read
Network-wide Config	Manage virtual networks, extranet policies, and other network-wide configurations. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	—

Capability	Description	Recommended permission settings for dependent capabilities
SD-Access	Configure, manage, and monitor an SD-Access Fabric.	• Network Management > Hierarchy: Read • Network Management > Inventory: Read • Network Management > Discovery: Read • Network Management > Network-wide Settings: Read • Network Provision > Device Provision: Write • Network Design > Template: Write • Network Operations > Plug and Play: Write • Network Operations > Network-wide Config: Read • Policy > Group-based Policy: Read • Network Operations > LAN Automation: Read • Network Operations > SWIM: Read • Network Operations > Compliance: Read • Network Design > Profiles and Settings: Read • Utilities > Event Viewer: Read
Policy	Configure and manage policies that reflect your organization's business intent. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Read/Write.	—
Application Policy	Manage QoS policies to make efficient use of network resources.	• Network Management > Hierarchy: Read • Network Management > Inventory: Read • Network Design > Profiles and Settings: Read • Network Operations > Compliance: Read • Utilities > Command Runner: Write • System > System Settings: Read

Capability	Description	Recommended permission settings for dependent capabilities
Group-Based Policy	Manage group-based policies that enforce network segmentation and access control. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	—
IP-Based Access Control	Manage IP-based access control lists that enforce network segmentation. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	—
Security	Manage and control secure access to the network.	—
Audit Log	View logs of changes made through the UI or API to the system, network devices, and settings.	—
Rogue and aWIPS	Monitor rogue and aWIPS threats in your network.	• Network Management > Hierarchy: Read • Network Management > Inventory: Read • Network Provision > Device Provision: Write • Assurance > Monitoring: Read • Assurance > Troubleshooting: Read • Network Design > Profiles and Settings: Write • Security > Audit Log: Write • System > System Settings: Read • Utilities > Reports: Write
Security Advisory	Scan the network for Cisco security advisories. Review the impact of published security advisories that may affect your network. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	• Network Management > Hierarchy: Read • Network Management > Inventory: Read

Capability	Description	Recommended permission settings for dependent capabilities
Stealthwatch	Configure network elements to send data to Cisco Stealthwatch to detect and mitigate threats, even in encrypted traffic. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	• Network Management > Hierarchy: Read • Network Management > Inventory: Read • Network Design > Profiles and Settings: Write • Network Provision > Device Provision: Write • System > System Settings: Read • System > System Administration: Read
Umbrella	Configure network elements to use Cisco Umbrella as the first line of defense against cybersecurity threats. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	—
System	Perform centralized administration for configuration management, network connectivity, software upgrades, and more.	—
System Administration	Manage core system administrative capabilities including HA, Disaster Recovery, and Backup and Restore. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	• System > System Settings: Write
System Settings	Manage core system connectivity settings. This role includes Integrity Verification, Integration Settings, Debugging Logs, Telemetry Collection, System EULA, IPAM, Data Platform, Cisco Credentials, Smart account, Smart Licensing, SSM Connection Mode, and Device EULA. This role also includes permissions related to certificate management. This role enables the configuration of automatic updates to the machine reasoning knowledge base. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	—
Utilities	Use common utilities to help manage your network.	—

Capability	Description	Recommended permission settings for dependent capabilities
App Hosting	Deploy, manage, and monitor virtualized and container-based applications running on devices.	—
Bonjour	Use the wide-area bonjour service to enable policy-based service discovery across your network. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	—
Command Runner	Display the running configuration of a device.	• Network Management > Inventory: Read
Event Viewer	View device and client events for troubleshooting.	—
Machine Reasoner	Scan the network for defects or bugs known by Cisco and troubleshoot various issues on your network through workflows. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	• Network Management > Inventory: Read • Network Management > Hierarchy: Read
Remote Device Support	Allow Cisco support personnel to remotely troubleshoot managed network devices. **Note** This permission set cannot be assigned to a site-scoped (non-global) access group if set to Write.	—
Reports	Use predefined reporting templates to generate reports for all areas of your network.	—

Display role-based access control statistics

You can display statistics that show how many users belong to each user role. You can also drill down to view the list of users who have a selected role.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **Role Based Access Control**.

All default user roles and custom roles are displayed.

Step 2 Click the number corresponding to each user role to view the list of users who have that role.

Configure site-based, role-based access control

Catalyst Center supports site-based, role-based access control (SRBAC), which enables you to create an access group that limits access to certain network sites. Access group is a combination of the role and site. The site can be the global site or a specific site. At any point, you can log in to one specific access group.

Catalyst Center supports these default access groups:

- **NW-ADMIN_Global** - Access group for global access to the role NW-ADMIN
- **OBSERVER_Global** - Access group for global access to the role OBSERVER
- **SUPER-ADMIN_Global** - Access group for global access to the role SUPER-ADMIN

Use this procedure to define an access group and then assign a user to the access group. You can also assign more than one access group to a user.

Procedure

Step 1 Define an access group.

a) From the main menu, choose **System** > **Users & Roles** > **Access Group**.
b) Click **Create Access Group** to create a new access group.
c) In the **Create Your Access Group** window, enter this information:

   - **Name**: Enter a unique name for the access group.
   - **Role**: Choose a role from the available list.
   - **Scope**: Choose the site hierarchy.

   Note
   External users are mapped to default access group with global scope. This option is not applicable for external users.

d) Click **Next** and review the access group composition in the **Summary** window.
e) Click **Create Access Group**.

   In the success message, click the **Back to Access Group** link to view the newly created access group in the **Access Group** window.

f) To edit the access group, choose the access group and click **Edit Access Group**.

   In the access group slide-in pane, edit the role or site hierarchy and click **Save**.

Step 2 To assign a user to the access group you created, go to **Users & Roles** > **User Management**.

- To assign the access group to an existing user:

  a. In the **User Management** window, click the radio button corresponding to the user to whom you want to assign the access group, and then click **Edit**.

  b. In the **Update Internal User** slide-in pane, click the **Access Group** drop-down list and choose the access group.

c. Click **Save**.

- To assign the access group to a new user:

a. In the **User Management** window, click **Add**.

b. In the **Create Internal User** slide-in pane, enter the first name, last name, and username.

c. From the **Access Group** drop-down list, choose the access group.

d. Enter the password and then confirm it.

e. Click **Save**.

Use case example: assign multiple access groups to an internal user

This sample use case shows how to create three different access groups and assign the access groups to a new internal user, *User1*.

Username	Access groups
User1	AG1, AG2, AG3

Access group	Role	Scope	Description
AG1	Custom-role1	Global	Access group for global access to the role Custom-role1
AG2	Custom-role2	IN-BGL	Access group for Bangalore site to the role Custom-role2
AG3	Custom-role3	US-SJ	Access group for San Jose site to the role Custom-role3

Before you begin

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

Procedure

Step 1 Define the custom roles *Custom-role1*, *Custom-role2* and *Custom-role3*.

a) From the main menu, choose **System** > **Users & Roles** > **Role Based Access Control**.

b) Click **Create a New Role**.

c) If a task overview window opens, click **Let's do it** to go directly to the workflow.

d) In the **Create a New Role** window, enter a name for the role and then click **Next**.

e) In the **Define the Access** window, click the **>** icon corresponding to the desired function to view the associated features.

f) Set the permission level to **Deny**, **Read**, or **Write** for the desired features and click **Next**.

If you set the permission level of a feature to **Deny**, the user to whom you assign this role cannot view this feature in the GUI.

For dependent features, if you override the recommended permission level settings, a warning message indicating the permission level violation of dependent features is shown in the **Summary** window.

g) Review the configuration settings. To make any changes, click **Edit**.

h) Click **Create Role**.

Step 2 Define the access groups *AG1*, *AG2*, and *AG3*.

a) From the main menu, choose **System** > **Users & Roles** > **Access Group**.

b) Click **Create Access Group** to create a new access group.

c) In the **Create Your Access Group** window, enter this information:

- **Name**: Enter a unique name for the access group.
- **Role**: Choose a role from the available list.
- **Scope**: Choose the site hierarchy.

d) Click **Next** and review the access group composition in the **Summary** window.

e) Click **Create Access Group**.

In the success message, click the **Back to Access Group** link to view the newly created access group in the **Access Group** window.

f) To edit the access group, choose the access group and click **Edit Access Group**.

In the access group slide-in pane, edit the role or site hierarchy and click **Save**.

Step 3 Assign the access groups *AG1*, *AG2*, and *AG3* to a new user, *User1*.

a) Navigate to **Users & Roles** > **User Management**.

b) In the **User Management** window, click **Add**.

c) In the **Create Internal User** slide-in pane, enter the first name, last name, and username.

d) From the **Access Group** drop-down list, choose the access groups.

e) Enter the password and then confirm it.

f) Click **Save**.

Use case example: assign multiple access groups to an external user

This sample use case shows how to create three different access groups and assign the access groups to an external user, *User-ise*, created in Cisco ISE.

Username	Access groups
User-ise	AG4, AG5, AG6

Access group	Role	Scope	Description
AG4	Custom-role4	Global	Access group for global access to the role Custom-role4
AG5	Custom-role5	IN-BGL	Access group for Bangalore site to the role Custom-role5
AG6	Custom-role6	US-SJ	Access group for San Jose site to the role Custom-role6

Before you begin

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

Procedure

Step 1 Define the custom roles *custom-role4*, *custom-role5*, and *custom-role6*.

a) From the main menu, choose **System** > **Users & Roles** > **Role Based Access Control**.
b) Click **Create a New Role**.
c) If a task overview window opens, click **Let's do it** to go directly to the workflow.
d) In the **Create a New Role** window, enter a name for the role and then click **Next**.
e) In the **Define the Access** window, click the **>** icon corresponding to the desired function to view the associated features.
f) Set the permission level to **Deny**, **Read**, or **Write** for the desired features and click **Next**.

   If you set the permission level of a feature to **Deny**, the user to whom you assign this role cannot view this feature in the GUI.

   For dependent features, if you override the recommended permission level settings, a warning message indicating the permission level violation of dependent features is shown in the **Summary** window.

g) Review the configuration settings. To make any changes, click **Edit**.
h) Click **Create Role**.

Step 2 Define the access groups *AG4*, *AG5*, and *AG6*.

a) From the main menu, choose **System** > **Users & Roles** > **Access Group**.
b) Click **Create Access Group** to create a new access group.
c) In the **Create Your Access Group** window, enter this information:

   - **Name**: Enter a unique name for the access group.
   - **Role**: Choose a role from the available list.
   - **Scope**: Choose the site hierarchy.

d) Click **Next** and review the access group composition in the **Summary** window.

e) Click **Create Access Group**.

In the success message, click the **Back to Access Group** link to view the newly created access group in the **Access Group** window.

f) To edit the access group, choose the access group and click **Edit Access Group**.

In the access group slide-in pane, edit the role or site hierarchy and click **Save**.

Step 3 Define the access groups *AG4*, *AG5*, and *AG6* in Cisco ISE server and assign the access groups to external user, *User-ise*.

For more information, see Configure external authentication, on page 143.

Impact of SRBAC on Catalyst Center features

The behavior of Catalyst Center features depends on the user role and site specified in the access group.

Table 7: SRBAC effect on Catalyst Center features

Feature	Effect of SRBAC
Discovery	**Discovery job** • Discovery jobs created by a site user are visible only to users within the site user's access group and its parent site hierarchy access group. • A parent site hierarchy user has the ability to rerun discovery jobs that were initially created by a child site hierarchy user. • The devices discovered are limited to those accessible to the user initiating the discovery. **Note** The results of the discovery jobs might differ if performed by two users due to differences in their access group site hierarchies.
	Global Credentials • **Credentials created by any site administrator are accessible to all site users in read-only mode.** • **Credentials can only be edited or deleted by the user who created them or by super users within the same hierarchy, provided they have write access.**

Feature	Effect of SRBAC
Inventory	**Add device** • Devices added by a site user will be visible only to users in the site user's access group and its parent site hierarchy access group. • If a device is added by a user with parent site hierarchy access group, it will not be visible to the users in the child site hierarchy access groups. • If a child site hierarchy user tries to re-add or import the same device, an error will occur stating that the device already exists, even though the user cannot view the device in their inventory.
Topology	**Shared custom view layouts** • Custom views created by lower-level access groups are accessible by higher-level access groups, but the reverse is not permitted. • Users can view only the devices and site hierarchy associated with their access group.

<table>
<tr><th>Feature</th><th colspan="2">Effect of SRBAC</th></tr>
<tr><td rowspan="6"><b>Plug and Play</b></td><td><b>Method of adding device</b></td><td><b>Visibility rules</b></td></tr>
<tr><td><b>Plug and Play discovery</b></td><td>Initially visible to all users.
After claiming to a site, the discovered devices are visible only to access group users and parent site hierarchy access group users.</td></tr>
<tr><td><b>Add plug and play device manually</b></td><td>Visible only to access group users and parent site hierarchy access group users.</td></tr>
<tr><td><b>Add a device from Cisco Smart Account</b></td><td>Visible only to access group users and parent site hierarchy access group users who added the devices.</td></tr>
<tr><td colspan="2"><b>Claim device to a site</b>
• <b>When a device is claimed to a site on plug and play, it will be visible to access group users of that specific site hierarchy and its parent site hierarchy.</b>
• <b>The device's plug and play history is visible to all the users in the site access group irrespective of any prior access groups of the device.</b>
• <b>All related plug and play workflows associated with the device are assigned to the specific site hierarchy to which the device was claimed.</b></td></tr>
<tr><td colspan="2"><b>After a device has been onboarded through plug and play and added to inventory:</b>
<b>If the device is assigned to a different site, the device record in plug and play is updated with the <i>siteHierarchyId</i> of the new site and is visible to access group users of the new site.</b></td></tr>
<tr><td><b>RMA and Network Refresh</b></td><td colspan="2">• Users associated with an access group can mark and unmark the devices belonging to the current access group or lower-level access group for replacement or refresh.
• To mark a fabric device faulty, the user must have access to all its neighbor devices.
• Once a user marked the device for replacement or refresh, users from the current access group or higher-level access group can trigger the replacement workflow.
• Users associated to the access group can schedule the workflow. Users from higher-level access groups can modify or cancel the workflow.</td></tr>
</table>

Feature	Effect of SRBAC
Tagging	Tags created by site users will be visible to all the other site users. However, editing of tags such as renaming and changing dynamic rules can be done only by the access group users who created the tags.
Licensing	The Licensing and System Settings permission sets cannot be assigned to site-scoped (non-global) access groups if they are configured with Read/Write access. For a site-scoped user, licensing and system settings pages will not be visible.
Network Settings	• Site profiles can only be edited or deleted from the access groups they were created in, but sites can be assigned to any profile in the system. • AAA/ISE server settings are global in nature and are allowed to be created, edited, or deleted only by users with access group of global site. • All wireless settings like SSID and RF Profile are global in nature and are allowed to be created only by user with access group of global site. • User with access group of a specific site can override the settings of that specific site.
Wireless controller provision	**Managed AP Location** • Site user can choose the Managed AP Location based on the site associated with the access group. • Catalyst Center validates the accessibility for both the wireless controller location and managed AP location. • To provision a wireless controller with multiple managed AP locations, user must have access to a site that is a parent site for all the managed AP locations. For example, if the network hierarchy includes *Area1* (parent site) with *Sub-area1* and *Sub-area2* (child sites), to provision a wireless controller that is managing APs in *Sub-area1* and *Sub-area2*, user must have access to *Area1*. If site user has access to only *Sub-area1* or *Sub-area2*, provisioning fails.

Feature	Effect of SRBAC
AP provision	• Access group user can provision APs to the sites associated with the access group. • The AP provision is allowed based on user accessibility to its associated controller physical and managed AP location. • User must have access to AP's associated controller and its managed locations. • User must have access to AP's secondary controller and its managed locations.
Certificate	Certificates are associated with a specific site or access group. Access group user can view only the certificates of devices assigned to the site associated with the access group.
Rogue and aWIPS	• Users with global site access only can enable or disable Rogue and aWIPS feature from Rogue Overview dashboard. • The Threats table in the Overview dashboard shows the only the rogues which are strongly detected by the APs present in the current logged in user owned site. Basically, the Detecting AP site in the table should be one of the sites owned by the logged in user. • Wireless Rogue containment operation is allowed only if the user is able to access the strongest detecting wireless controller for that rogue. Wired Rogue containment operation is allowed only if the user is able to access the switch where the rogue is detected. • Access group users with access to global site can create or remove the MAC addresses from Allowed List. • Users can view all the profiles created by others. However, users can edit, delete, or assign site only if they own all the sites that are part of the profile. If users do not own all the sites that are part of the profile, only read-only details will be displayed when they click on the profile name.
	aWIPS profile configuration **• Any admin can create the profile but can only map it to the devices under the sites they own.** **• Edit or delete of mapped profile is only allowed if the user has access to all the wireless controllers mapped on that profile. If the user has mapped a profile to one of the devices and then later the device is moved to another site which the user doesn't have access to, the user cannot edit or delete that profile.** **• In the profile assignment screen, only the devices which are accessible to the current user will be displayed.**

Feature	Effect of SRBAC
SD-Access	**REP** A REP ring created by a site user is visible to: • Users in the site user's access group • Users in the parent site's hierarchy access group, and • Users in the access group that is the closest common parent of all ring members in the site hierarchy.
	PRP • **User having access to both LAN-A and LAN-B fabric sites will be allowed to configure and view PRP.** • **User having access to only LAN-A site will see partial data along with banner message indicating limited access.**
	MRP • **User having access to all ring members can see the complete MRP ring details.** • **User having access to partial ring members will see partial data along with banner message indicating limited access.**

Configure external authentication

If you are using an external server for authentication and authorization of external users, you should enable external authentication in Catalyst Center.

Before you begin

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 119.
- You must configure at least one authentication server.
- For SRBAC, you must define the access group on the Cisco ISE server.

  Configure the Cisco ISE server similar to how roles are configured in Catalyst Center. For example, <AAA attribute name>=rds=<comma separated list of rd names>. The first rd can be treated as the default access group profile.

Note If Catalyst Center is deployed on a physical appliance, review this note.

When external authentication is enabled, Catalyst Center does not fall back to local users if the AAA server is unreachable or the AAA server rejects an unknown username.

By default, external authentication fallback is enabled and supported only for local admins. With it enabled, local admins can log in to Catalyst Center.

To re-enable external authentication fallback, SSH to the Catalyst Center instance and enter this CLI command:

```
magctl rbac external_auth_fallback enable
```

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **External Authentication**.

Step 2 To enable external authentication in Catalyst Center, check the **Enable External User** check box.

Step 3 (Optional) Configure the AAA attribute.

For TACACS authentication, the following AAA attributes are supported:

Catalyst Center	TACACS
Empty	cisco-av-pair
cisco-av-pair	cisco-av-pair
Cisco-AVPair	Cisco-AVPair

For RADIUS authentication, the following AAA attributes are supported:

Catalyst Center	RADIUS
Empty	cisco-av-pair
Cisco-AVPair	cisco-av-pair

a) In the **AAA Attribute** field, enter the appropriate attribute for your use case, as described in the preceding tables. The default value of the **AAA Attribute** field is null.

b) Click **Update**.

Step 4 (Optional) Configure the AAA server or servers.

Configure these settings only if you want to swap the current primary or secondary AAA servers or define different AAA servers. From the main menu, choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers** to open the **Authentication and Policy Servers** window.

a) From the **Primary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.

b) From the **Secondary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.

c) (Optional) If you are using a Cisco ISE server, you can update the settings, if necessary.

For information about Cisco ISE policies, see "Segmentation" in the *Cisco Identity Services Engine Administrator Guide*.

Table 8: Cisco ISE server settings

Name	Description
Shared Secret	Key for device authentications. The shared secret can contain up to 100 characters. The shared secret must be provided before the AAA address can be updated.
Username	Name that is used to log in to the Cisco ISE CLI.
Password	Password for the Cisco ISE CLI username.
FQDN	Fully qualified domain name (FQDN) of the Cisco ISE server. The FQDN consists of two parts, a hostname and the domain name, in the following format: *hostname.domainname.com* For example, the FQDN for a Cisco ISE server might be ise.cisco.com.
Subscriber Name	A unique text string—for example, `acme`—that is used during Catalyst Center-to-Cisco ISE integration to set up a new pxGrid client in Cisco ISE.
Virtual IP Address(es)	Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

d) (Optional) To update advanced settings, click **View Advanced Settings** and update the settings, if necessary.

Table 9: AAA server advanced settings

Name	Description
Protocol	TACACS or RADIUS.
Authentication Port	Port used to relay authentication messages to the AAA server. • For RADIUS, the default is UDP port 1812. • For TACACS, the port is 49 and can't be changed.
Accounting Port	Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. • For RADIUS, the default UDP port is 1813. • For TACACS, the port is 49 and can't be changed.
Retries	Number of times that Catalyst Center can attempt to connect with Cisco ISE.
Timeout	Length of time that Catalyst Center waits for Cisco ISE to respond. The maximum timeout value is 60 seconds.

e) Click **Update**.

Two-factor authentication

Two-factor authentication, also known as 2FA, adds another layer of security to user verification by using an identifier method in addition to a user's name and password. The identifier method is generally something that only the actual intended user possesses (such as a phone app or keyfob) and is intentionally separated from the original login method.

The Catalyst Center implementation of two-factor authentication supports the use of a token client (that generates single-use token codes after the appropriate PIN is entered), a token server (that validates token codes), and an authentication server to manage user access. Authentication can be handled using either the RADIUS or TACACS+ protocol.

Prerequisites for two-factor authentication

The following prerequisites must be in place to set up two-factor authentication for use with Catalyst Center:

- An authentication server that is able to return attribute-value pairs to convey RBAC role authorizations for authenticated Catalyst Center users. In our example, we use Cisco Identity Services Engine (Cisco ISE) 2.3 Patch 1.
- A two-factor token server that you will integrate with your authentication server. In our example, we use RSA Authentication Manager 7.2.
- A token card application on the client’s machine that generates software tokens. In our example, we use RSA SecurID Software Token.

Two-factor authentication workflow

Here is a summary of what happens when a user logs in to a Catalyst Center appliance on which two-factor authentication has been configured:

1. In an RSA SecurID token client, a user enters their PIN to get a token code.
2. In the Catalyst Center login page, they enter their username and token code.
3. Catalyst Center sends the login request to Cisco ISE using either the RADIUS or TACACS+ protocol.
4. Cisco ISE sends the request to the RSA Authentication Manager server.
5. RSA Authentication Manager validates the token code and informs Cisco ISE whether the user has been authenticated successfully.
6. If the user has been authenticated, Cisco ISE matches the authenticated user with their configured authorization profile and returns the **role=NETWORK-ADMIN-ROLE** attribute-value pair.
7. Catalyst Center grants access to the features and pages associated with the user's role-based access control (RBAC) role.

Configure two-factor authentication

To configure two-factor authentication on your Catalyst Center appliance, complete the following procedure.

Procedure

Step 1 Integrate RSA Authentication Manager with Cisco ISE:

a) In RSA Authentication Manager, create two users: `cdnac_admin` (for the Admin user role) and `cdnac_observer` (for the Observer role).

   For more information, see the "Add a User to the Internal Database" topic in the RSA Self-Service Console Help. To access this topic, do the following:

   1. Open the *RSA Self-Service Console Help*.
   2. In the **Search help** field, enter `Add a User to the Internal Database` and then click **Search help**.

b) Create a new authentication agent.

   For more information, see the "Add an Authentication Agent" topic in the *RSA Self-Service Console Help*.

c) Generate the Authentication Manager agent configuration file (sdconf.rec):

   1. From the RSA Security Console, choose **Access** > **Authentication Agents** > **Generate Configuration File**.

      The **Configure Agent Timeout and Retries** tab opens.

   2. For the **Maximum Retries** and **Maximum Time Between Each Retry** fields, use the default values.
   3. Click **Generate Configuration File**.

      The **Download Configuration File** tab opens.

   4. Click the **Download Now** link.
   5. When prompted, click **Save to Disk** to save a local copy of the zip file.
   6. Unzip the file and use this version of the sdconf.rec file to overwrite the version that is currently installed on the agent.

d) Generate a PIN for the `cdnac_admin` and `cdnac_observer` users that you created in Step 1a.

   For more information, see the "Create My On-Demand Authentication PIN" topic in the *RSA Self-Service Console Help*.

e) Start Cisco ISE, choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**, and then click **Add**.

f) In the **RSA SecurID Identity Sources** page, click **Browse**, choose the sdconf.rec file you downloaded, and then click **Open**.

g) Check the **Reauthenticate on Change PIN** check box, then click **Submit**.

Step 2 Create two authorization profiles, one for the Admin user role and one for the Observer user role.

a) In Cisco ISE, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

b) For both profiles, enter the following information:

   - **Name**: Enter the profile name.

- **Access Type**: Choose **ACCESS_ACCEPT**.
- **Advanced Attributes Settings** area: Choose **Cisco:cisco-av-pair** from the first drop-down list.

  If you are creating an authorization profile for the Admin user role, choose **Role=NETWORK-ADMIN-ROLE** from the second drop-down list.

  If you are creating an authorization profile for the Observer user role, choose **Role=OBSERVER-ROLE** from the second drop-down list.

Step 3 Create an authentication policy for your Catalyst Center appliance.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authentication Policies" topic.

Step 4 Create two authorization policies, one for the Admin user role and one for the Observer user role.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authorization Policies" topic.

Step 5 In the RSA Authentication Manager Security Console, verify that software tokens have been assigned to both users.

For more information, see the "View a Token" topic in the *RSA Self-Service Console Help*.

Note
If you need to assign tokens, complete the steps described in the "Assign a Software Token to a User" topic.

Enable two-factor authentication using RADIUS

To enable two-factor authentication that uses a Cisco ISE server configured for RADIUS, complete the following procedure:

Procedure

Step 1 Integrate Cisco ISE with Catalyst Center.

In the *Catalyst Center Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.

Step 2 Configure Catalyst Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important
Ensure that you specify the same shared secret for both Cisco ISE and Catalyst Center.

Enable two-factor authentication using TACACS+

To enable two-factor authentication that uses a Cisco ISE server configured for TACACS+, complete the following procedure:

Procedure

Step 1 In Cisco ISE, choose **Administration** > **Network Resources** > **Network Devices** to open the **Network Devices** window.

Step 2 Click **TACACS Authentication Settings** to view its contents. Ensure that a shared secret has already been configured for the Catalyst Center device that you added previously.

Step 3 Choose **Work Centers** > **Device Administration** > **Policy Elements** to open the **TACACS Profiles** window.

Step 4 Create TACACS+ profiles for the example_admin and example_observer user roles:

a) Click **Add**.

b) Complete the following tasks:

- Enter the profile name.
- After clicking the **Raw View** tab, enter the following text into the **Profile Attributes** text box:
  - For the example_admin user role, enter `Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE`
  - For the example_observer user role, enter `Cisco-AVPair=ROLE=OBSERVER-ROLE`

c) Click **Save**.

Step 5 Integrate Cisco ISE with Catalyst Center.

In the *Catalyst Center Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.

Step 6 Configure Catalyst Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important
Ensure that you specify the same shared secret for both Cisco ISE and Catalyst Center.

Log in using two-factor authentication

To log in to Catalyst Center using two-factor authentication, complete the following procedure:

Procedure

Step 1 From the Catalyst Center login page, enter the appropriate username.

Step 2 Open the RSA SecurID token client and enter the PIN you configured previously to generate a one-time token.

Step 3 Copy this token and paste it into the **Password** field of the Catalyst Center login page.

Step 4 Click **Log In**.

Display external users

You can view the list of external users who have logged in through RADIUS or TACACS for the first time. The information that is displayed includes their usernames and roles.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **External Authentication**.

Step 2 Scroll to the bottom of the window, where the **External Users** area lists the external users.

CHAPTER 5

Manage Licenses

License Manager overview

The Catalyst Center License Manager feature helps you visualize and manage all your Cisco product licenses, including Smart Account licenses. From the main menu, choose **Tools** > **License Manager**. The **License Manager** window contains tabs with information, including:

- **Overview**:
    - Switch: Shows purchased and in-use license information for all switches.
    - Router: Shows purchased and in-use license information for all routers.
    - Wireless: Shows purchased and in-use license information for all wireless controllers and APs.

  - ISE: Shows purchased and in-use license information for devices managed by Cisco Identity Services Engine (ISE).

- **Licenses**: The **License Summary** shows the total licenses purchased from Cisco Smart Software Management (CSSM), the number of licenses that are about to expire, and out-of-compliance details for all types of licenses for all Cisco devices.
- **Devices**: The **Devices** table shows the license type, license expiry, license mode, virtual account, associate site, and registration status of each device managed by Catalyst Center.
- **Reporting**: The **Smart License Compliance** card allows you to launch the **Smart License Compliance** workflow.
- **Sync Status**: In a table, the Smart License Policy (SLP) compliance shows the devices and timeline graph of license usage reports sent from Catalyst Center to CSSM.

To manage licenses, you can use the controls shown above the table listings in each tab. This table describes each of the controls.

Note Not all controls are available in every tab.

Table 10: License management controls

Control	Description
Filter	Click **Filter** to specify one or more filter values and then click **Apply**. You can apply multiple filters. To remove a filter, click the **x** icon next to the corresponding filter value.
Change Cisco License	Select one or more licenses and choose **Actions** > **Change Cisco License** to change the level of a selected license to Essentials or Advantage. You can also use this control to remove a license. For more information, see Change license level, on page 160.
Change Virtual Account	Select one or more licenses and choose **Actions** > **Change Virtual Account** to specify the Virtual Account used to manage these licenses.
Manage Smart License > Register	Select one or more Smart License-enabled devices and choose **Actions** > **Manage Smart License** > **Register** to register the Smart License-enabled devices.
Manage Smart License > Deregister	Select one or more Smart License-enabled devices and choose **Actions** > **Manage Smart License** > **Deregister** to unregister the Smart License-enabled devices.
Manage License Reservation > Enable License Reservation	Choose the device for which you want to apply Specific License Reservation (SLR) or Permanent License Reservation (PLR), then choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.
Manage License Reservation > Update License Reservation	The device must be in the SLR registered state. You can update the SLR applied to a wireless device or switch with a wireless controller package. Choose the device for which you want to update the SLR, then choose **Actions** > **Manage License Reservation** > **Update License Reservation**.

Control	Description
Manage License Reservation > Cancel/Return License Reservation	Choose the device and choose **Actions** > **Manage License Reservation** > **Cancel/Return License Reservation** to cancel or return the SLR or PLR applied to the device.
Manage License Reservation > Factory License Reservation	Choose the device and choose **Actions** > **Manage License Reservation** > **Factory License Reservation** to enable the factory-installed SLR on the device.
Recent Tasks	Click **Recent Tasks** to see a list of all 50 of the most recently performed Catalyst Center tasks. Use the drop-down to filter the list to show only those tasks with a status of **Success**, **Failure**, or **In Progress**.
License Usage	Click **License Usage** to see the license utilization percentage for all types of licenses.
Refresh	Click **Refresh** to reload the window with current data.
Find	Enter a search term in the **Find** field to find all licenses in the list that have that term in any column. Use the asterisk (*) character as a wildcard anywhere in the search string.
Show Records	Select the total number of records to display in each page of the table.

The Licenses table displays the information shown for each device. All of the columns support sorting. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

Note Not all columns are used in every tab. Also, some of the columns are hidden in the default column view setting. To view the hidden columns, click the gear icon and under **Edit Table Columns**, choose the columns you want displayed in the table.

Table 11: License use information

Column	Description
Device Type: Device Series	Name of the device product series (for example, Catalyst 3850 Series Ethernet Stackable Switch). For more information, see View license details, on page 159.
Device Type: Total Devices	The total number of devices in this product series that are under active management by Catalyst Center.
Purchased Cisco Licenses	The total number of purchased Catalyst Center subscription licenses for the devices in this product series.
Purchased Licenses: Network/Legacy	The total number of purchased perpetual licenses for the devices in this product series: • Network • Legacy
Used Licenses	The total number of Catalyst Center subscription licenses applied to the devices in this product series.

Column	Description
Used Licenses: Network/Legacy	The total number of perpetual licenses for the devices in this product series: • Network • Legacy
Feature Licenses (applicable only for Routers)	The number of licenses purchased for specific features such as security, AVC, and so on.

Table 12: All license information

Column	Description
Device Name	Name of the device. For more information, see View license details, on page 159.
Device Family	The category of the device, such as Switches and Hubs, as defined by Catalyst Center.
IP Address	IP address of the device.
Device Series	The full name of the Cisco product series to which the listed device belongs (for example, Cisco Catalyst 3850 Series Ethernet Stackable Switch).
Cisco License	The Catalyst Center license level.
Cisco License Expiry	The expiration date of the Catalyst Center license.
License Mode	The Catalyst Center license mode.
Network License	The type of network license.
Virtual Account	The name of the Cisco Virtual Account managing the license for the device. The Virtual Account and the site hierarchy are distinct entities and aren’t interconnected. Licensing operations might fail if the virtual account name contains any of these characters: /, \, =. We recommend that you remove these characters from your virtual account name through the Cisco SSM portal (software.cisco.com) and then perform a refresh from the **License Manager Overview** window.
Site	The Catalyst Center site where the device is located.
Registration Status	The registration status of the device.
Authorization Status	The authorization status of the device.
Reservation Status	The reservation status of the device.
Last Updated Time	The last time this entry in the table was updated.
MAC Address	The MAC address of the licensed device.
Term	The total term during which the Catalyst Center subscription license is in effect.
Days to Expiry	The number of days remaining until the Catalyst Center license term expires.

Column	Description
Software Version	The version of the network operating system currently running on the device.

Integration with Cisco Smart Accounts

Catalyst Center supports Cisco Smart Accounts, an online Cisco service that provides simplified, flexible, automated software- and device-license purchasing, deployment, and management across your organization. You can add multiple Cisco Smart Accounts.

When there are multiple Cisco Smart Accounts, one account is designated as the default, which the License Manager uses for visualization and licensing operations (such as registration, license level changes, and so on).

Virtual Accounts serve as subdivisions within a Cisco Smart Account, offering enhanced control over licenses and entitlements associated with the Smart Account. Virtual Accounts and the site hierarchy are distinct entities and are not interconnected.

After changing the default Cisco Smart Account, it takes several minutes to retrieve the data from CSSM and display it on the License Manager Overview and All License windows.

You can delete any Cisco Smart Accounts.

If you already have a Cisco Smart Account, you can use Catalyst Center to:

- Track your license consumption and expiration
- Apply and activate new licenses, without intervention
- Promote each device's license level from Essentials to Advantage (or vice versa) and reboot the device with the newly changed level of feature licensing
- Identify and reapply unused licenses

You can accomplish this automatically, without leaving Catalyst Center.

Set up License Manager

You must set up access to your Cisco Smart Account before you can use the Catalyst Center License Manager tools.

Before you begin

- Ensure that you have SUPER-ADMIN-ROLE permissions or the appropriate RBAC scope to perform this procedure.
- Collect the Cisco user ID and password for your Smart Account.
- If you have multiple Smart Accounts, select the Smart Account that you want to use with Catalyst Center, and collect that account's user ID and password.
- To apply licenses to a device in Catalyst Center, the device must be present in Inventory, must have a site assigned to it, and must have connectivity to the following domains:

  - id.cisco.com
  - apx.cisco.com
  - commerce.cisco.com, and
  - smartreceiver.cisco.com.

- Ensure that all allowed ports, FQDNs, and URLs listed in the *Cisco Catalyst Center Installation Guide* are allowed on any firewall or proxy.

Procedure

Step 1 Log in using a Catalyst Center system administrator username and password.

Step 2 From the main menu, choose **System** > **Settings** > **Cisco.com Credentials**.

Step 3 Under **Cisco.com Credentials**, enter the username and password for your cisco.com account.

Step 4 From the main menu, choose **System** > **Settings** > **Smart Account**.

Step 5 Under **Smart Account**, click **Add** and enter the username and password for your Smart Account.

Step 6 Click **Save**.

Step 7 If you have multiple Smart Accounts, click **Add** and enter your additional accounts.

Step 8 If you have multiple Smart Accounts, select one account to be the default. The License Manager uses the default account for visualization and licensing operations. To change the default Smart Account:

a) Click **Change** next to the selected Smart Account name.

b) Change the active Smart Account and select a Smart Account to be the default.

c) Click **Apply**.
After changing the default account, it takes several minutes to retrieve the data from CSSM and display it on the License Manager Overview and All License windows.

Step 9 To edit a Smart Account, click the three dots in the Actions column and select **Edit**.

Step 10 To delete a Smart Account, click the three dots in the Actions column and select **Delete**.

Step 11 To access your Smart Account using a virtual or subordinate Smart Account name and password, under **Link Your Smart Account**, select:

- **Use Cisco.com user ID** if your cisco.com and Smart Account credentials are the same.
- **Use different credentials** if your cisco.com and Smart Account credentials are different, and then enter your Smart Account credentials.

Step 12 Click **View all virtual accounts** to view all virtual Smart License Accounts.

What to do next

Register the Catalyst Center controller as a controller for Cisco Plug and Play Connect in a Cisco Smart Account, for redirection services. This also allows you to synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Catalyst Center Plug and Play. For more information, see "Register or Edit a Virtual Account Profile" in the *Cisco Catalyst Center User Guide*.

Cisco Networking Subscription licenses

With the release of Wi-Fi 7 APs, Catalyst Center License Manager supports Cisco Networking Subscription (CNS) licenses. You have visibility to the AP license status, compliance, and reason for noncompliance. After synchronizing the wireless controller with CSSM, the Wi-Fi7 AP is compliant and displays the CNS Essentials or Advantage subscription.

License Manager reports include all devices; you can filter by compliant and noncompliant devices. Banners across Catalyst Center show which APs aren't registered with a required subscription and navigate back to License Manager to remediate.

To comply with CNS licensing, you must:

- Configure Smart Accounts.
- Choose the Cisco Smart Software Management connection mode.

  Registration of next-generation devices, including Wi-Fi 7, isn't supported in Cisco Smart Software Manager On-Prem connection mode.
- Enable Assurance telemetry for the device.
- Assign the device to a site.
- Enable NTP.

Visualize license use and expiration

Catalyst Center can display graphical representations of your purchased licenses, how many of them are in use (that is, assigned to devices), and their duration.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager**.

Step 2 In the **Overview** tab, Catalyst Center displays the name of the active Smart Account. From the **Virtual Account** drop-down list, choose a virtual account to display the license details.

Step 3 Click a device category button to view the corresponding license usage details: **Switches**, **Routers**, **WLC**, or **ISE**.

The license usage pie charts display the aggregate number of purchased licenses and the number of licenses currently in use for the selected device category. The charts also indicate the proportion of Essentials and Advantage licenses within each total.

The number of purchased licenses is obtained from the Cisco Smart Software Manager (CSSM). The number of used licenses is sourced from the devices managed by Catalyst Center.

The license usage table shows the subtotals for used and available licenses, listed alphabetically by product family name.

Step 4 To see details for a particular product family, click the name of the product family under the **Device Series** column.

Catalyst Center displays details about the product family that you selected.

Step 5 To see a graphical representation of license duration, scroll down to the **Cisco License Timeline** section. The timeline graph for each product family is a visual representation of when the licenses in the configured Smart Account expires for that product family.

Note
This section isn't available for the **ISE** device category.

View historical trends for license consumption

Catalyst Center allows you to view historical trends for all purchased and consumed licenses in CSSM on a daily, weekly, and monthly basis. CSSM stores historical information for up to one year.

Use this procedure to view the historical trends for license consumption.

Before you begin

Register Catalyst Center to a smart account in CSSM. For more information, see Integration with Cisco Smart Accounts, on page 155.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Licenses**.

- In the **License Summary** area, view the total number of purchased Catalyst Center subscription licenses from CSSM .
- In the **Smart Account** area, view details about the smart account.
- In these areas, view the corresponding total number, expiring, and noncompliant subscription licenses:
  - **CNS ESSENTIALS**
  - **CNS ADVANTAGE**
  - **DNA ESSENTIALS**
  - **DNA ADVANTAGE**
  - **NETWORK ESSENTIALS**
  - **NETWORK ADVANTAGE**
- In the **License** window, a table displays your discovered devices and their licenses. You can choose the required view from the **Focus** drop-down list:
  - Virtual account view
  - Licenses view
  - Device series view
  - Device type view

- License type view

Step 2 To view the historical information of a chosen license, click the license link in the row for that device.

The license details slide-in pane shows the complete license details and license history of the chosen device.

Note
The title of the license details slide-in pane matches the title of the chosen device.

Step 3 In the license-details slide-in pane, choose the frequency of historical information from the **Frequency** drop-down list.

The available options include:

- **Daily**: Displays the license data snapshot on the first day.
- **Weekly**: Displays the license data snapshot on Monday.
- **Monthly**: Displays the license data snapshot on the first day of the month.

Depending on the frequency selection, a graph is displayed that shows the license data for **Purchased**, **In Use**, and **Balance** licenses.

Depending on the frequency selection, the **License History** table filters the license historical information based on **Date**, **Purchased**, **In Use**, and **Balance**.

Note
License historical information is always one day old because CSSM provides only the data from the previous day. Catalyst Center periodically retrieves the license historical information from CSSM daily.

View license details

There are many ways to find and view license details in Catalyst Center. For example, you can click the license usage and term graphs displayed in the **Switches**, **Routers**, **Wireless**, **ISE**, or **Devices** tabs in the **License Manager** window. Each graph displays pop-ups with aggregated facts about licenses for each of these product families.

This method provides the comprehensive license details for a single device using the **Devices** table in the License Manager.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Devices**.

The License Manager window displays a table listing all of your discovered devices and their licenses. Information in the table includes only basic device and license information, such as device type, license expiration dates, and so on.

Step 2 Scroll through the table to find the device whose license details you want to see. If you are having trouble finding the device you want, you can:

- Filter: Click and then enter your filter criteria in the appropriate field. (For example, enter all or part of the device name in the **Device Name** field.) You can enter filter criteria in multiple fields. When you click **Apply**, the table displays only the rows displaying information that matches your filter criteria.

  If you want to view the devices that belong to a particular site, navigate to the site in the left pane, and click the site. The devices are filtered accordingly. A site marker indicating the site hierarchy is displayed at the top of the page.

- Find: Click in the **Find** field and enter the text you want to find in any of the table columns. When you press **Enter**, the table scrolls to the first row with text that matches your entry in the **Find** field.

- Customize: Click the gear icon and under **Edit Table Columns**, choose the columns you want displayed in the table. For example, deselect **Device Series** or select **Days to Expiry**. When you click **Apply**, the table displays only the columns you selected.

Step 3 When you find the device that you want, click the **Device Name** link in the row for that device.

Catalyst Center displays the **License Details** slide-in pane with complete license details and license history for the device that you selected. **Actions** displays actions that can be performed on the device or its licenses.

When you are finished, click to close the **License Details** slide-in pane.

Change license level

You can upgrade or downgrade your device license level to Essentials or Advantage for these license types:

- DNA
- CNS

Note

- You can't change the license type for a device. You can only change the license level for the corresponding license type.
- Network license conversion is available only for products in the Cisco Catalyst 9000 device family. This conversion is handled implicitly when the Catalyst Center license level is changed.
- You can change the license level for devices from only one family at a time, such as routers, switches, or wireless controllers.

You can update the license level with Catalyst Center subscription licenses. When you change the license level of a device, Catalyst Center automatically downloads and applies your licenses behind the scenes, using your Smart Account.

After you change the license level, the change takes effect when the device reboots. However, reboot isn’t necessary for devices such as Cisco Catalyst 3560-CX Series Switches and Cisco AireOS Wireless Controller.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Devices**.

The **License Manager** window displays a table listing the discovered devices and their licenses.

Step 2 Use **Find** or scroll through the table to find the devices whose license level you want to change. If you're having trouble finding the device you want, or want to choose multiple devices, see View license details, on page 159 to change the table to display only the devices you want.

Step 3 Check the check box next to the devices for which you want to change the license level.

Step 4 Choose **Actions** > **Change License** > **Change Cisco License**.

Step 5 If you chose devices from more than one device family (for example, switches and wireless controllers), complete these steps.

a) Click the radio button next to the device family for which you want to change the license level: **Routers**, **Switch**, or **Wireless**.

b) Click **Continue**.

Step 6 Choose the required license level.

a) Click the required license level for the devices.

Based on the current license level, Catalyst Center displays only the available license level: **Essentials** or **Advantage**.

To remove the license from the device, click **Remove**.

Note
You can't remove the CNS license from a device. When you remove the CNS license, the device uses the CNS Advantage license by default.

b) Click the required license type:

- **All**
- **DNA**
- **CNS**

c) Click **Continue**.

Step 7 Check the **Reboot device on update** check box to reboot the device when its license level is updated.

Step 8 (Optional) In the **Task Name** field, update the task name.

Step 9 Choose a schedule for updating the license level for your devices.

- **Now**: Immediately update the license level and reboot the devices.
- **Later**: Schedule the date and time to update the license level and reboot the devices.

Step 10 Click **Confirm**.

Step 11 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the license level change task status in the **Recent Tasks** window.

Auto registration of Smart License-enabled devices

You can enable auto registration of Smart License (SL)-enabled devices. When auto registration is enabled, any SL-enabled devices (but not Smart License Policy [SLP]-enabled devices) added to Catalyst Center are automatically registered to the chosen virtual account.

Note Auto registration is not supported in Smart Proxy mode.

Procedure

Step 1 Log in using a Catalyst Center system administrator username and password.

Step 2 From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **Smart Account**.

Step 3 Click **License**.

Step 4 Check the **Auto register smart license enabled devices** check box.

Step 5 Choose a virtual account.

Step 6 Click **Apply**.

Day-zero configuration for Smart License-enabled devices

Devices that are already added to Catalyst Center before enabling auto registration are not automatically registered. You can view the Smart License-enabled devices that are not registered in the **All Licenses** window.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Devices**.

The **License Manager** window displays a banner message with the number of SL-enabled devices that are not auto registered and a table listing all of your discovered devices and their licenses with a link to set up auto registration.

Alternatively, you can filter the unregistered devices by using the **Registration Status** column.

Step 2 Choose the SL-enabled devices that you want to register and choose **Actions** > **Manage Smart License** > **Register**.

Step 3 Choose the virtual account and click **Continue**.

Step 4 To register the devices:

- If you want to register the devices immediately, choose **Now** and click **Confirm**.
- If you want to register the devices later, choose **Later** and specify a date and time. After specifying the schedule parameters, click **Confirm**.

Configure licenses for worldwide safe mode-enabled devices

Worldwide safe mode (WWSM)-enabled devices are in WWSM on day zero and when they don't meet the license requirements. To disable WWSM, enable the CNS licenses on the devices.

Use this procedure to configure licenses and disable WWSM on WWSM-enabled devices.

Before you begin

Ensure that a CNS license is available for the device in the smart account.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Reporting**.

Step 2 Click **Smart License Compliance**.

Alternatively, instead of the first two steps, click the menu icon and choose and choose **Workflows** > **Smart License Compliance**.

Step 3 In the **Smart License Compliance** dialog box, click **Let's Do It**.

To skip the task overview in the future, check the **Don't show this to me again** check box.

Step 4 In the **Select Smart Account** window, do these steps:

a) (Optional) In the **Workflow Name** field, update the task name.
b) From the **Smart Account** drop-down list, choose the smart account that contains the CNS licenses.
c) From the **Virtual Account** drop-down list, choose the virtual account.
d) Click **Next**.

Step 5 In the **Choose Sites and Devices** window, do these steps:

a) (Optional) In the left pane, choose the required site.
b) Check the check box next to the devices for which you want to configure the licenses.

   You can use the **Search** field to search for devices by their name.

   You can click the filter icon (▽) to filter the devices in the table based on the column headers.

c) Click **Next**.

Step 6 In the **Modify Policy** window, do these steps:

a) Review the CSSM policy.

   (Optional) To modify the reporting interval, click **Modify**, and do these steps in the **Change Reporting Interval** dialog box:

   1. In the **Reporting Interval in Days** field, enter the reporting interval at which devices report their resource usage to CSSM.
   2. Click **Save**.

b) Click **Next**.

Step 7 In the **Sync Data with Cisco** window, click **Submit**.

Step 8 In the **Summary** window, click **Finish**.

Apply specific license reservation or permanent license reservation to devices

Smart Licensing requires a smart device instance to regularly sync with Cisco Smart Software Management (CSSM) so that the latest license status is refreshed and compliance is reported. Some customers have devices that are within highly secured networks with limited internet access. In these types of networks, devices cannot regularly sync with CSSM and show out of compliance. To support these customer environments, Specific License Reservation (SLR) and Permanent License Reservation (PLR) have been introduced. The License Manager enables Catalyst Center customers to reserve licenses securely from CSSM using an API-based workflow. In Catalyst Center, it requires a one-time connectivity to CSSM in the staging environment, then the devices never need to connect to Cisco in SLR or PLR mode. If no connectivity to CSSM or staging is possible, you can resort to the manual SLR/PLR workflow available in CSSM.

SLR lets you install a node-locked license file (SLR authorization code) on a product instance. This license file enables individual (specific) licenses (entitlement tags).

PLR lets you install an authorization code that enables all licensed features on the product.

Both SLR and PLR require preapproval at the Smart Account level. Contact licensing@cisco.com for support.

To enable SLR or PLR when both the device and Catalyst Center are connected to CSSM, see Enable SLR or PLR when the devices and Catalyst Center are connected to CSSM, on page 164.

To enable SLR or PLR when the device and Catalyst Center do not have connectivity to CSSM, see Enable SLR or PLR when the devices and Catalyst Center are not connected to CSSM, on page 165.

Enable SLR or PLR when the devices and Catalyst Center are connected to CSSM

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Devices**.

Step 2 Select the devices for which you want to apply SLR or PLR, and choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.

Step 3 Choose **Specific License Reservation (SLR)** or **Permanent License Reservation (PLR)** and click **Continue** to obtain the request codes for the selected devices.

Step 4 After the request codes are generated for the selected devices, click **Continue**.

Step 5 Choose a virtual account from which you want to reserve licenses and click **Continue** to generate the authorization codes for the selected devices.

Step 6 After the authorization codes are generated, do any of the following:

- To apply SLR immediately, choose the devices and click **Continue**.

- To apply SLR later, click **Apply Later**.

Step 7 Click **Confirm** to apply SLR/PLR to the selected device.

You can now view the updated status of the devices under **Reservation Status** on the **All Licenses** window.

Enable SLR or PLR when the devices and Catalyst Center are not connected to CSSM

Use this procedure to enable SLR or PLR for the devices that are not connected to CSSM.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Devices**.

Step 2 Select the devices for which you want to apply SLR or PLR, and choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.

Step 3 Choose **Specific License Reservation (SLR)** or **Permanent License Reservation (PLR)** and click **Continue** to obtain the request codes for the selected devices.

You also can connect to the device through Telnet to obtain the request code.

Step 4 After the request codes are generated for the selected devices, click **Export**. This downloads the requestcodes.csv file, which contains the IP address, serial number of the device, and the request code.

Step 5 Save the file to your preferred location.

Step 6 Obtain the authorization code for each device from CSSM and update it in the CSV file. See Generate Authorization Code from CSSM.

Step 7 Click the **Upload CSV** link.

Step 8 Click the **Select a file from your computer** link to select the saved CSV file.

Step 9 Click **Continue**.

Step 10 Choose a virtual account from which you want to reserve licenses and click **Continue**. SLR or PLR is applied to the selected devices.

You can now view the updated status of the devices under **Reservation Status** on the **All Licenses** window.

Generate the authorization code from CSSM

Before you begin

You must have Smart Account credentials to log in to CSSM.

Procedure

Step 1 Log in to **CSSM**.

Step 2 Choose **Inventory** > **Licenses** > **License Reservation**. The Smart License Reservation wizard appears.

The **License Reservation** button is visible on the **Licenses** tab only if you have specific license reservation enabled for your Smart Account.

Step 3 In the **Step 1: Enter Request Code** tab, enter the request code in the **Reservation Request Code** field and click **Next**.

Step 4 In the **Step 2: Select Licenses** tab, check the **Reserve a specific license** check box.

Step 5 In the **Quantity to Reserve** field, enter the number of licenses that you want to reserve and click **Next**.

Step 6 In the **Step 3: Review and Confirm** tab, click **Generate Authorization Code**.

Step 7 Get the authorization code from the **Step 4: Authorize Code** tab.

Cancel SLR or PLR applied to devices

You can cancel or return the SLR or PLR that is applied to a device.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Licenses**.

Step 2 Click the device and choose **Actions** > **Manage License Reservation** > **Cancel/Return License Reservation**.

Step 3 Click **Cancel** to return the licenses.

You can view the updated status of the devices under **Reservation Status** on the **All Licenses** window.

Install the authorization code and enable the high security license

Cisco offers a throughput of 250 Mbps by default. To increase the device throughput to more than 250 Mbps, you must get the authorization code from Cisco. You can install the authorization code and enable the High Security (HSEC) license in a single workflow or in separate workflows, as required.

Before you begin

Ensure that the device is running Cisco IOS XE Release 17.3.2 or later.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Reporting**.

Alternatively, you can use **Workflows** > **Smart License Compliance**.

Step 2 Click the **Smart License Compliance** card.

Step 3 In the **Smart License Compliance** window, click **Let's Do It**.

To skip this window in the future, check **Don't show this to me again**.

Step 4 In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.

Step 5 Click **Next**.

Step 6 In the **Choose Sites and Devices** window, choose the devices on which you want to install the authorization code and click **Next**.

Step 7 In the **Policy Settings** window, review the CSSM policies and click **Next**.

Step 8 In the **Choose Device Features** window, do these steps:

a) Choose the devices.
b) From the **Auth Codes** drop-down list, choose **Install**.
c) From the **HSEC** drop-down list, choose **Enable**.
d) Click **Next**.

Step 9 In the **Review Device Features** window, click **Next**.

Step 10 In the **Installing Device Features** window, view the authorization code and HSEC installation status and click **Next**.

Step 11 In the **Sync Data with Cisco** window, click **Next**.

Step 12 In the **Summary** window, review the authorization code and HSEC installation status; then, click **Finish**.

Disable the high security license

You can disable the HSEC license from a device if you don't want to consume the HSEC license unnecessarily.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Reporting**.

Step 2 Click the **Smart License Compliance** card.

Step 3 In the **Smart License Compliance** window, click **Let's Do It**.

To skip this window in the future, check **Don't show this to me again**.

Step 4 In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.

Step 5 Click **Next**.

Step 6 In the **Choose Sites and Devices** window, choose the devices from which you want to disable the HSEC license and click **Next**.

Step 7 In the **Policy Settings** window, click **Next**.

Step 8 In the **Choose Device Features** window, do these steps:

a) Choose the devices.
b) From the **HSEC** drop-down list, choose **Disable**.
c) Click **Next**.

Step 9 In the **Review Device Features** window, click **Next**.

Step 10 In the **Installing Device Features** window, view the HSEC disable operation status and click **Next**.

Step 11 In the **Sync Data with Cisco** window, click **Next**.

Step 12 In the **Summary** window, click **Finish**.

Upload resource use details to CSSM

You can upload resource use details to CSSM instantly or schedule an upload.

To upload resource use details to CSSM, devices don't have to have NETCONF enabled, and devices don't have to be added to the site.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Reporting**.

Step 2 Click the **Smart License Compliance** card.

Step 3 In the **Smart License Compliance** window, click **Let's Do It**.

To skip this window in the future, check **Don't show this to me again**.

Step 4 In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.

Step 5 Click **Next**.

Step 6 In the **Choose Sites and Devices** window, choose the devices from which you want to retrieve the resource utilization details and click **Next**.

Step 7 To upload the resource utilization details instantly, click **Next** in the **Modify Policy** window. To modify the scheduled reporting frequency:

a) Under **Policy Settings**, click **Modify** corresponding to the **Reporting Interval** field.
b) In the **Change Reporting Interval** window, enter the value.

   The reporting interval (in days) denotes the frequency of scheduled upload of resource utilization details from Catalyst Center to CSSM. The frequency of uploads can be increased but cannot be reduced below the minimum reporting frequency.

c) Click **Save**.

Step 8 In the **Sync Data with Cisco** window, click **Next**.

Step 9 In the **Summary** window, click **Finish**.

After successful synchronization of data with CSSM, Catalyst Center sends an acknowledgment to the devices.

What to do next

The number of devices for which the license usage reporting has failed is shown in a separate **Smart License Compliance** card with the **Retry** option. Click the **Smart License Compliance** card and redo the above procedure to send the license usage reports from the failed devices to CSSM.

Change device throughput

You can change the throughput of Smart License-enabled routers.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Reporting**.

Step 2 Choose the device that you want to change.

Step 3 Click **More Actions** and choose **Change Throughput**.

Step 4 In the **Choose Throughput** window, choose the throughput value and click **Next**.

Step 5 In the **Apply Throughput** window, click **Next**.

Step 6 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the **Change Throughput** task status in the **Recent Task** window.

Transfer licenses between virtual accounts

You can transfer licenses between virtual accounts.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Licenses**.

Step 2 Choose the licenses that you want to transfer and click **Transfer Licenses**.

Step 3 In the **Transfer Licenses** window, choose the virtual account.

Step 4 Enter the **Transfer License Count** for each of the chosen licenses and click **Transfer**.

Step 5 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the **License Transfer** task status in the **Recent Task** window.

Manage customer tags on Smart License-enabled devices

You can add a maximum of four customer tags to a Smart License-enabled device to help identify telemetry data for a product instance. You can also update and delete the customer tags.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Reporting**.

Step 2 Choose the devices on which you want to add customer tags.

Step 3 Click **More Actions** and choose **Manage Free Form Fields** to add, update, or delete customer tags.

Step 4 To add or update customer tags, in the **Free Form Fields** window:

a) Enter the customer tags.
b) Click **Save**.

Step 5 To delete customer tags, in the **Free Form Fields** window:

a) Click the delete icon for the customer tags that you want to delete.
b) Click **Save**.
c) In the **Warning** window, click **Continue**.

Step 6 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the **Manage Customer Tags** task status in the **Recent Task** window.

Modify license policy

You can modify the reporting interval at which network devices report their feature usage to CSSM.

Procedure

Step 1 From the main menu, choose **Tools** > **License Manager** > **Reporting**.

Step 2 In the **Smart License** table, click **Modify Policy**.

The **Modify Policy** window shows the policy settings and CSSM policy details.

Step 3 Under **Policy Settings**, click **Modify**.

Step 4 In the **Change Reporting Interval** window, enter the reporting interval value.

Step 5 Click **Save**.

CHAPTER 6

Backup and Restore

About backup and restore

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 automation data only or both automation and Assurance data.

Important NetFlow data is not backed up when you back up Catalyst Center's automation and Assurance data.

- Automation data consists of Catalyst Center databases, credentials, file systems, and files. The automation backup is a full backup.
- The Assurance data consists of network assurance and analytics data. The first backup of Assurance data is a full backup. After that, backups are incremental.

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.

- Catalyst Center 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, on page 173.
- 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.
- We recommend:
  - 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.
- When you restore the backup files, Catalyst Center removes and replaces the existing database and files with the backup database and files. While a restore is being performed, Catalyst Center is unavailable.
- You cannot do a backup from one version of Catalyst Center and restore it to another version of Catalyst Center. You can only restore a backup to an appliance that is running the same Catalyst Center software release with the same first four digits and the same application versions as the appliance from which the backup was taken. To view the current applications and versions, choose **System** > **Software Management** and click **Currently Installed Applications**.
- You can restore a backup to a Catalyst Center appliance with a different IP address. This situation could happen if the IP address is changed on Catalyst Center and you need to restore from an older system.

Important After a backup and restore of Catalyst Center:

- You must access the **Integration Settings** window and update (if necessary) the **Callback URL Host Name** or **IP Address**. For more information, see Configure Integration Settings.
- Integration with Cisco Spaces is interrupted if the Catalyst Center member ID changes. This occurs, for example, when restoring on a different hardware appliance, or migrating from a hardware appliance to a virtual appliance. For more information, see "Integrate Cisco Spaces with Catalyst Center" in the *Cisco Spaces Configuration Guide*.

- You can restore a backup file to an appliance with the same machine profile, such as restoring a backup from a medium appliance to another medium appliance.
- You can restore a backup file from a lower-end appliance to a higher-end appliance. For example, you can restore the backup file from a medium appliance to a large or extra-large appliance.

- You *cannot* restore a backup file from a higher-end appliance to a lower-end appliance. So, these scenarios are not supported:
  - Restoring a large appliance's backup file to a medium appliance.
  - Restoring an extra-large appliance's backup file to either a large or medium appliance.
- You can restore a standalone node's backup file to a three-node cluster or vice versa, provided that the target appliance has the same machine profile or is a higher-end appliance. The one exception is that you can't restore the backup file from a three-node cluster consisting of extra-large appliances to a standalone extra-large appliance.

Backup and restore event notifications

You can receive a notification whenever a backup or restore event takes place. To configure and subscribe to these notifications, complete the steps described in the "Work with Event Notifications" topic of the *Cisco Catalyst Center Platform User Guide*. When completing this procedure, ensure that you select and subscribe to the SYSTEM-BACKUP-v2 and SYSTEM-RESTORE-v2 events.

A notification is generated and sent whenever an event listed in this table occurs:

Operation	**Event**
Backup	The process to create a backup file for your system has started.
	A backup file could not be created for your system. This event typically happens because: • The necessary disk space is not available on remote storage. • You can't retrieve the status of your system's server, which is a precheck for the backup operation. • You encountered connectivity issues or latency while creating a backup file on your system.
Restore	The process to restore a backup file has started.
	The restoration of a backup file failed. This event typically happens because: • The backup file is corrupted. • You encountered connectivity issues or latency while creating a backup file from your system.

Backup server requirements

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 automation data backup

To support automation data backups, the server must meet these requirements:

- Must use SSH (port22)/remote sync (rsync). Catalyst Center 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, the following line 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 backup server directory. A cascaded NFS mount adds a layer of latency and is therefore not supported.

Server requirements for assurance backup

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

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

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

Requirements for multiple Catalyst Center deployments

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

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

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

Backup server directory layout

To simplify backups, we recommend that you use this directory layout for your backup server:

Single Catalyst Center cluster deployment

- Full backup (Automation and Assurance):
  - cluster1: /data/automation/cluster1
  - cluster1: /data/assurance/cluster1
- Automation-only backup:

  cluster1: /data/automation/cluster1

Multiple Catalyst Center cluster deployment

- Full backup (Automation and Assurance):
  - cluster1: /data/automation/cluster1
  - cluster1: /data/assurance/cluster1
  - cluster2: /data/automation/cluster2
  - cluster2: /data/assurance/cluster2
- Automation-only backup:
  - cluster1: /data/automation/cluster1
  - cluster2: /data/automation/cluster2

Backup storage requirements

Catalyst Center stores backup copies of Assurance data on an external NFS device and automation data on an external remote sync (rsync) target location. You must allocate enough external storage for your backups to cover the required retention. We recommend this storage:

Machine profile	Machine profile alias	Cisco part number	NFS storage (14 days incremental)
medium	medium	Second-generation appliance: • DN2-HW-APL • DN2-HW-APL-U (promotional)	1.7 TB
		Third-generation appliance: DN3-HW-APL	
t2_large	large	Second-generation appliance: • DN2-HW-APL-L • DN2-HW-APL-L-U (promotional)	3 TB
		Third-generation appliance: DN3-HW-APL-L	
t2_2xlarge	extra large	Second-generation appliance: • DN2-HW-APL-XL • DN2-HW-APL-XL-U (promotional)	8.4 TB
		Third-generation appliance: DN3-HW-APL-XL	

Add a physical disk for backup and restore

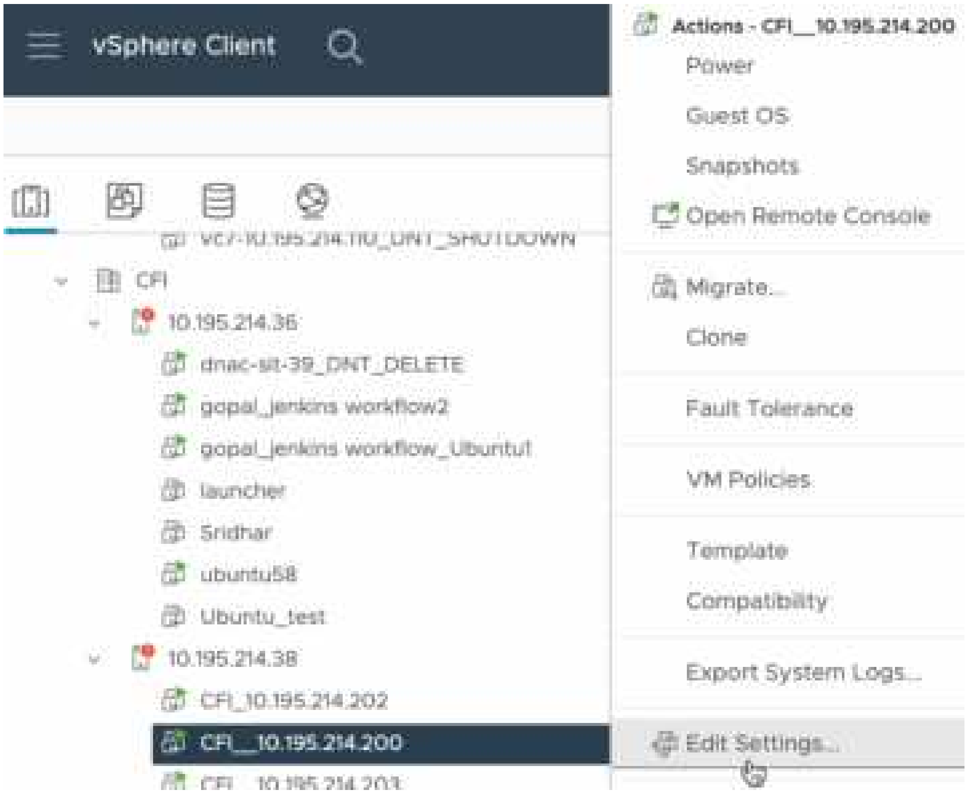
Use this procedure to add a physical disk that can be used for backup and restore operations.

Procedure

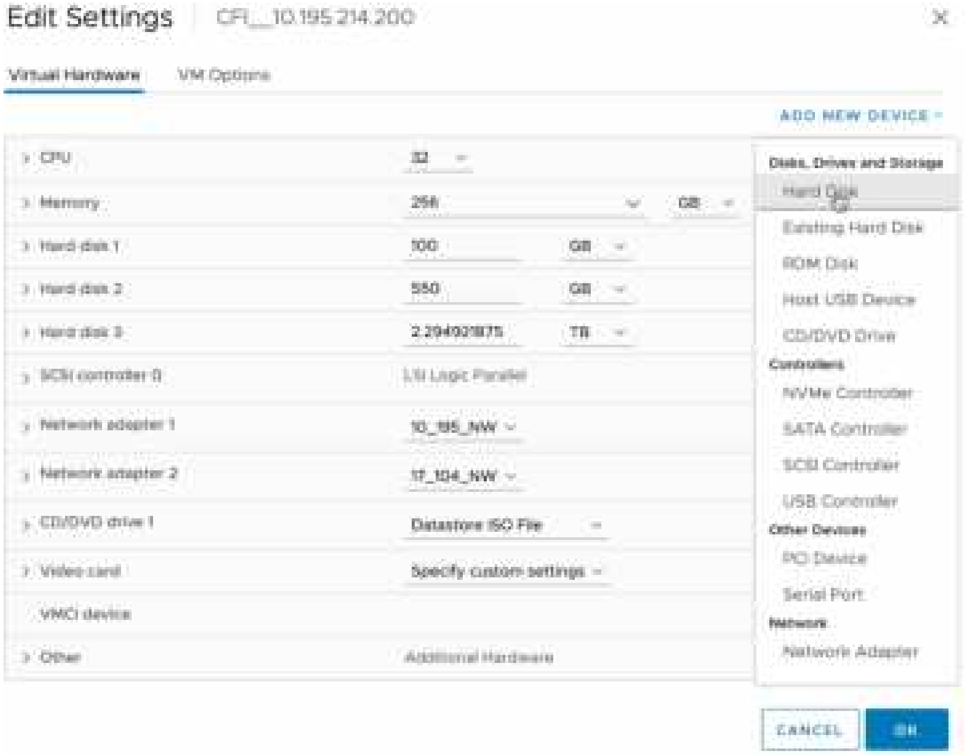
Step 1 If your appliance is running on the machine that's hosting Catalyst Center, power off the appliance's virtual machine.

Step 2 Log in to VMware vSphere.

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



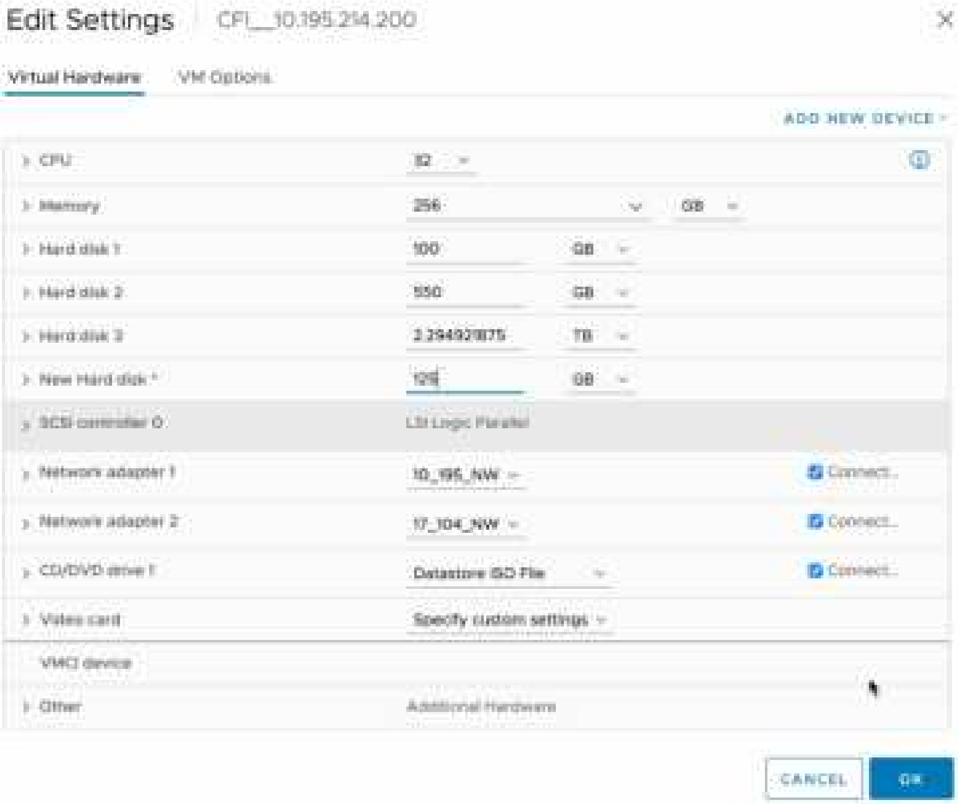
Step 4 In the **Edit Settings** dialog box, click **Add New Device** and then choose **Hard Disk**.



Edit Settings | CFI__10.195.214.200

CPU	32	
Memory	256	GB
Hard disk 1	100	GB
Hard disk 2	550	GB
Hard disk 3	2.294921875	TB
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	10_195_NW	
Network adapter 2	17_104_NW	
CD/DVD drive 1	Datastore ISO File	
Video card	Specify custom settings	
VMCI device		
Other	Additional Hardware	

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



Edit Settings | CFL__10.195.214.200

Virtual Hardware | VM Options

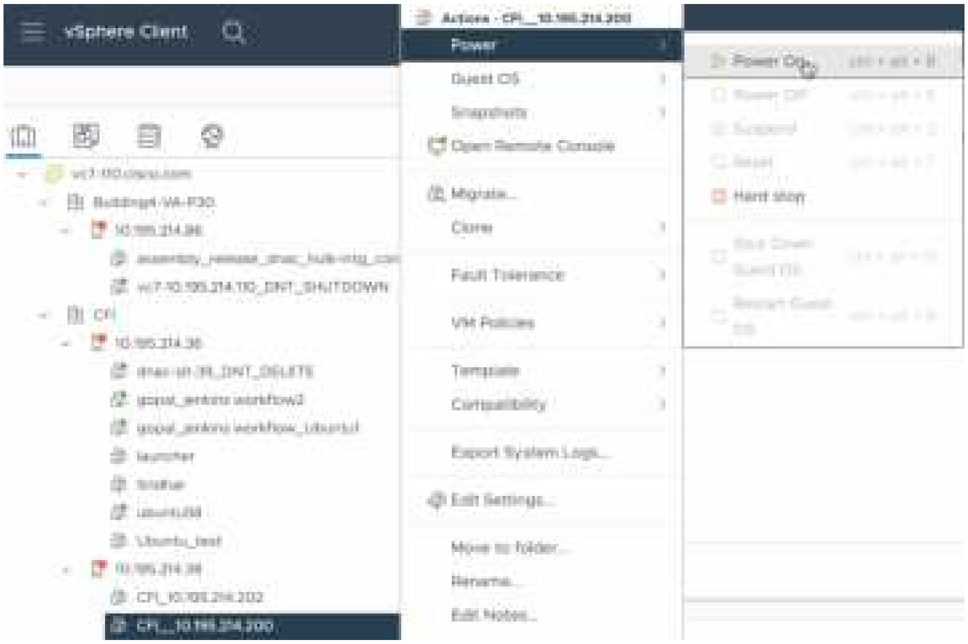
CPU	32	
Memory	256 GB	
Hard disk 1	100 GB	
Hard disk 2	550 GB	
Hard disk 3	2.294921875 TB	
New Hard disk *	128 GB	
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	10_195_NW	☑ Connect...
Network adapter 2	17_104_NW	☑ Connect...
CD/DVD drive 1	Datastore ISO File	☑ Connect...
Video card	Specify custom settings	
VMCI device		
Other	Additional Hardware	

Note

For information on the recommended storage space for backup, see Backup storage requirements, on page 176.

Step 6 Click **OK**.

Step 7 Power on the appliance's virtual machine.



What to do next

You can now configure the added physical disk for backup. For information on how to configure the physical disk, see Configure the location to store backup files, on page 180.

Add the NFS server

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

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Backup Configuration**.

Step 2 Click **Add NFS**.

Step 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**.

Step 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.

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

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

What to do next

Configure the added NFS server for backup. For more information, see Configure the location to store backup files, on page 180.

Configure the location to store backup files

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

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

Before you begin

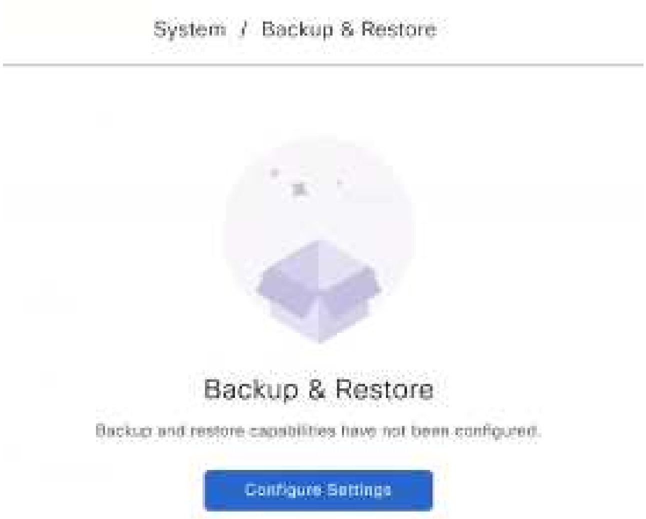
Make sure that the following requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in Backup server requirements, on page 173.

Procedure

Step 1 From the main menu, choose **System** > **Backup and Restore**.

You can view this window:



System / Backup & Restore

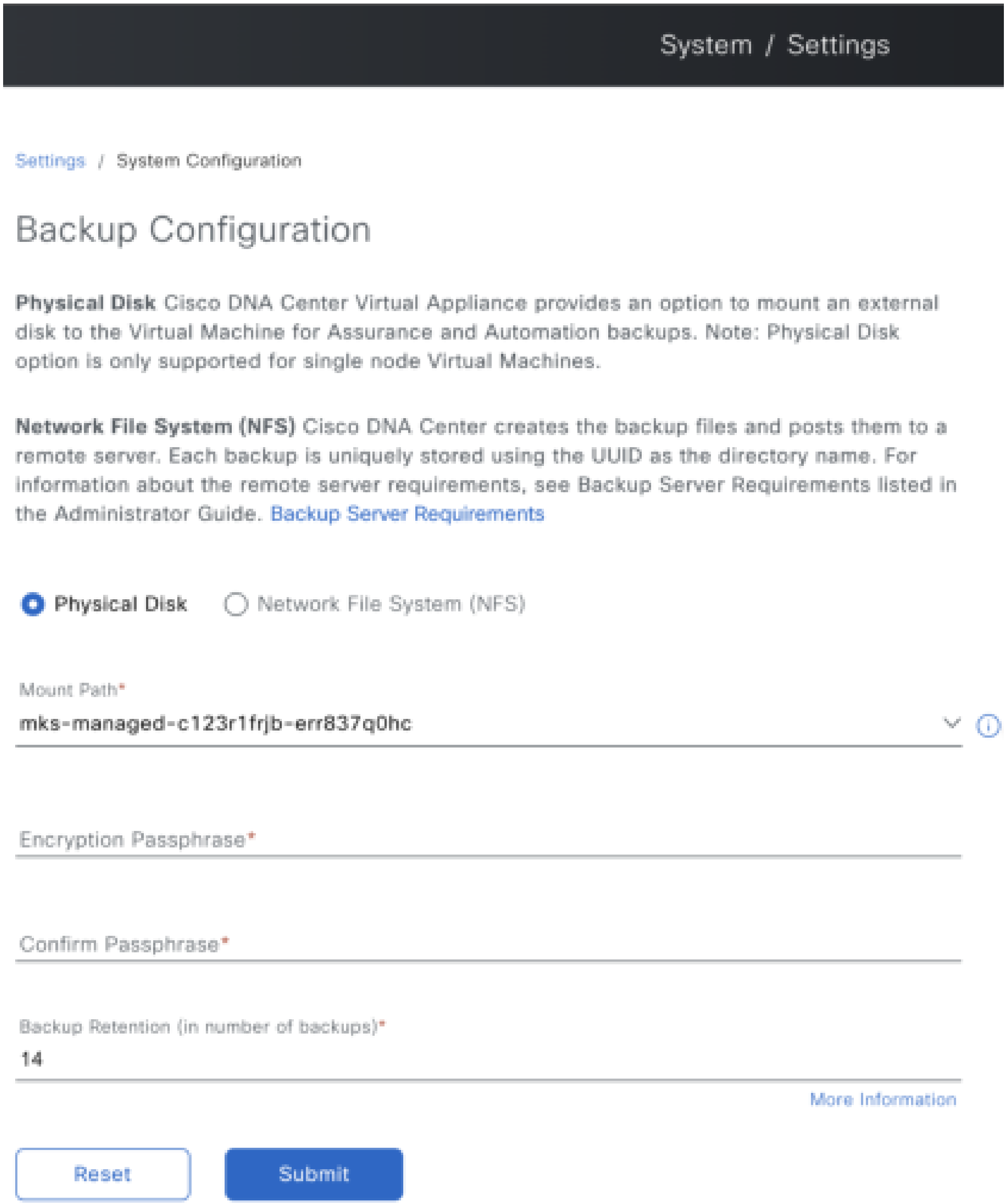
Backup & Restore

Backup and restore capabilities have not been configured.

Step 2 Click **Configure Settings**.

Alternatively, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

Step 3 Choose the **Physical Disk** or **NFS** server option.



System / Settings

Settings / System Configuration

Backup Configuration

Physical Disk Cisco DNA Center Virtual Appliance provides an option to mount an external disk to the Virtual Machine for Assurance and Automation backups. Note: Physical Disk option is only supported for single node Virtual Machines.

Network File System (NFS) Cisco DNA Center 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 listed in the Administrator Guide. Backup Server Requirements

● Physical Disk ○ Network File System (NFS)

Mount Path*: mks-managed-c123r1frjb-err837q0hc

Encryption Passphrase*

Confirm Passphrase*

Backup Retention (in number of backups)*: 14

More Information

Step 4 **Physical Disk**: Catalyst Center provides an option to mount an external disk to the virtual machine, to store a backup copy of Assurance and automation data. To configure a physical disk, click the **Physical Disk** radio button and define 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.

Step 5 **NFS**: Catalyst Center creates the backup files and posts them to a remote NFS server. For information about the remote server requirements, see Backup server requirements, on page 173. 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.

Step 6 Click **Submit**.

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

Create a backup

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

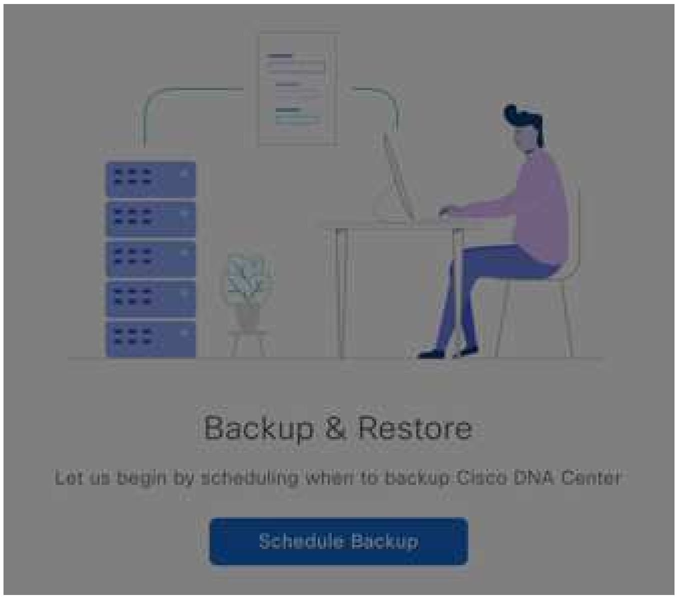
Before you begin

You must configure the backup location. For more information, see Configure the location to store backup files, on page 180.

Procedure

Step 1 From the main menu, choose **System** > **Backup & Restore**.

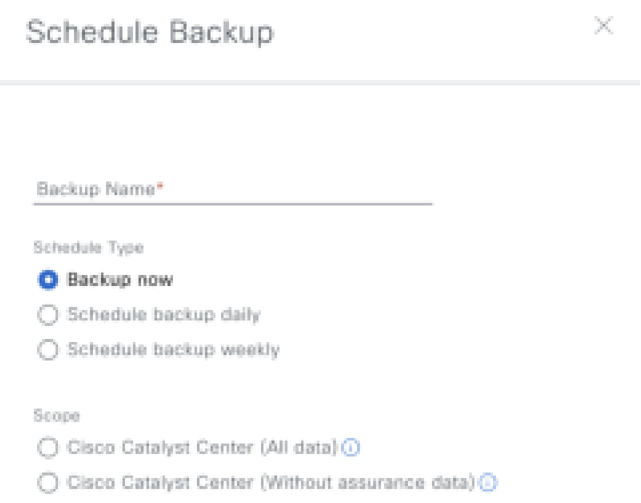
Step 2 Click **Schedule Backup**.



Backup & Restore

Let us begin by scheduling when to backup Cisco DNA Center

The **Schedule Backup** slide-in pane opens.



Schedule Backup

Backup Name*

Schedule Type

● Backup now
○ Schedule backup daily
○ Schedule backup weekly

Scope

○ Cisco Catalyst Center (All data)
○ Cisco Catalyst Center (Without assurance data)

Do the following in the **Schedule Backup** slide-in pane:

a. Enter a unique name for the backup.

b. In the **Schedule Type** area, choose one of the following options:

- **Backup Now**: To immediately create a backup.

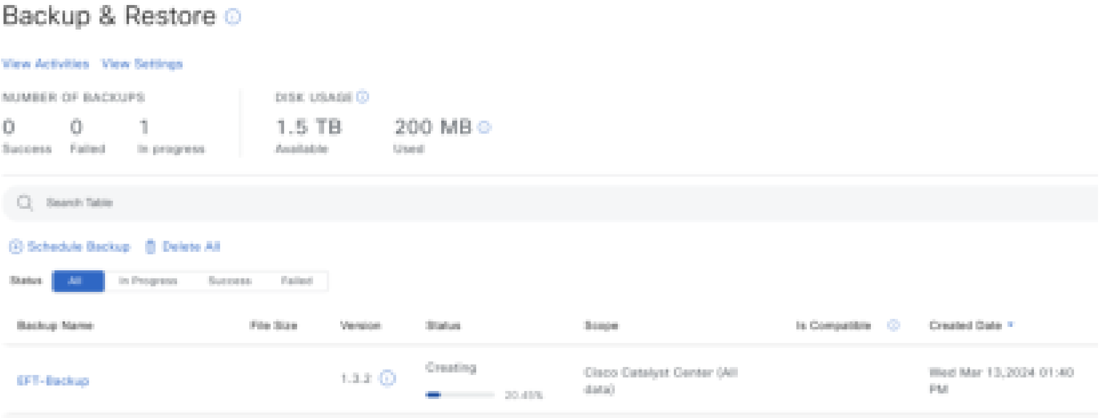
- **Schedule Backup Daily**: To schedule the backup on a daily basis.
- **Schedule Backup Weekly**: To schedule the backup on a weekly basis.

c. In the **Scope** area, choose one of the following options:

- **Cisco Catalyst Center (All Data)**: Choose this option to create a backup for automation and Assurance data.
- **Cisco Catalyst Center (Without Assurance Data)**: Choose this option to create a backup only for automation data.

d. Click **Save**.

Step 3 Catalyst Center begins the backup process. An entry for the backup is added to the **Backup & Restore** window.

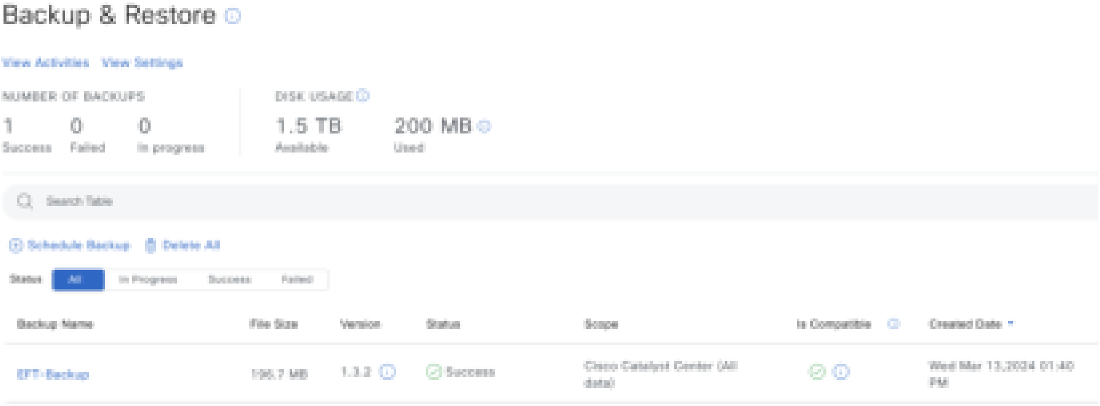


NUMBER OF BACKUPS: 0 Success, 0 Failed, 1 In progress

DISK USAGE: 1.5 TB Available, 200 MB Used

Backup Name	File Size	Version	Status	Scope	Is Compatible	Created Date
EFT-Backup		1.3.2	Creating 20.45%	Cisco Catalyst Center (All data)		Wed Mar 13,2024 01:40 PM

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



NUMBER OF BACKUPS: 1 Success, 0 Failed, 0 In progress

DISK USAGE: 1.5 TB Available, 200 MB Used

Backup Name	File Size	Version	Status	Scope	Is Compatible	Created Date
EFT-Backup	196.7 MB	1.3.2	✓ Success	Cisco Catalyst Center (All data)	✓	Wed Mar 13,2024 01:40 PM

Restore data from backups

Use this procedure to restore backup data from your virtual appliance. To restore backup data from a failed or faulty virtual appliance, see Restore data from a physical disk for a faulty virtual appliance, on page 187.

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

Before you begin

Make sure that the following requirements are met:

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

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

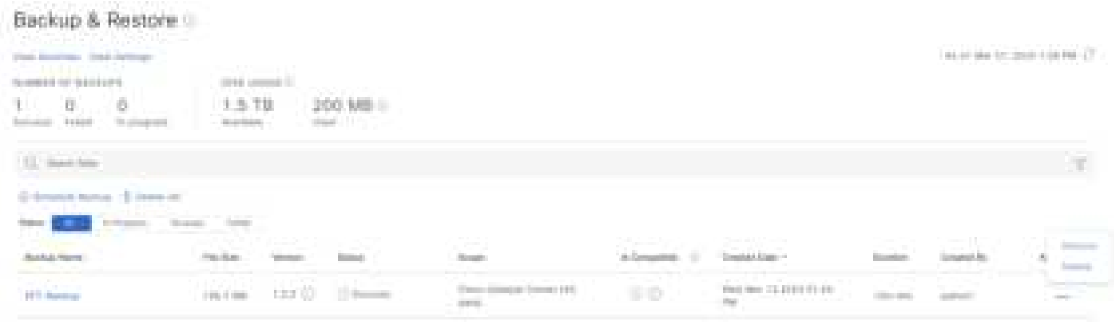
Procedure

Step 1 From the main menu, choose **System** > **Backup & Restore**.

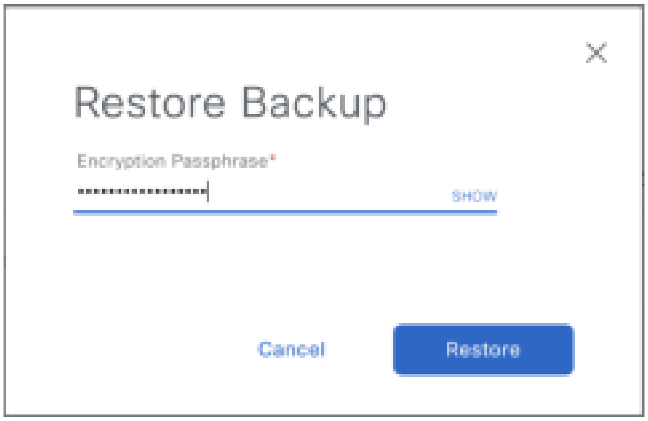
If you have created a backup, it appears in the **Backup & Restore** window.

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

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



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


Restore Backup

Encryption Passphrase*

••••••••••••••••••

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

Maintenance in progress...

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

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

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

Restore data from a physical disk for a faulty virtual appliance

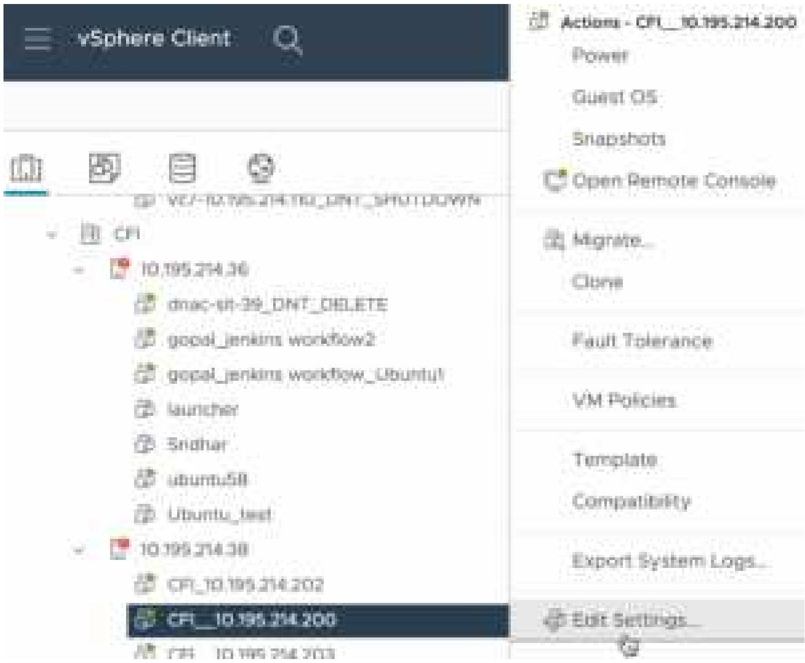
Use this procedure to restore data from a physical disk for a virtual appliance that has failed or is faulty.

Procedure

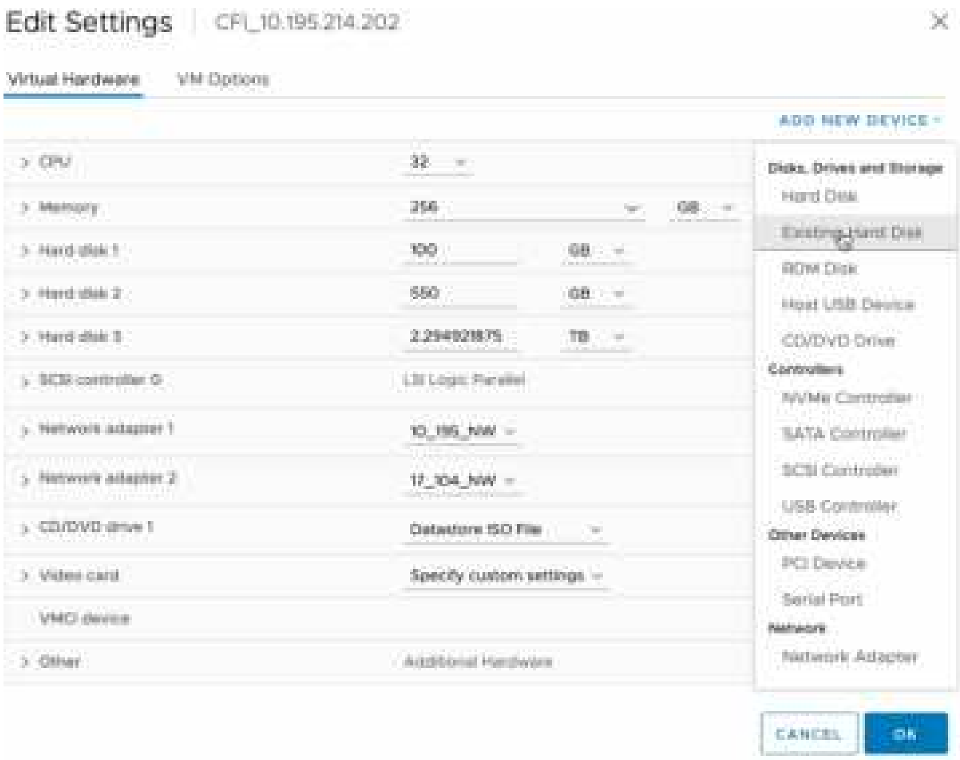
Step 1 For your new virtual appliance, complete these steps to configure Catalyst Center to use the storage disk that you configured for the faulty virtual appliance:

a. Power OFF the appliance's virtual machine.

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



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

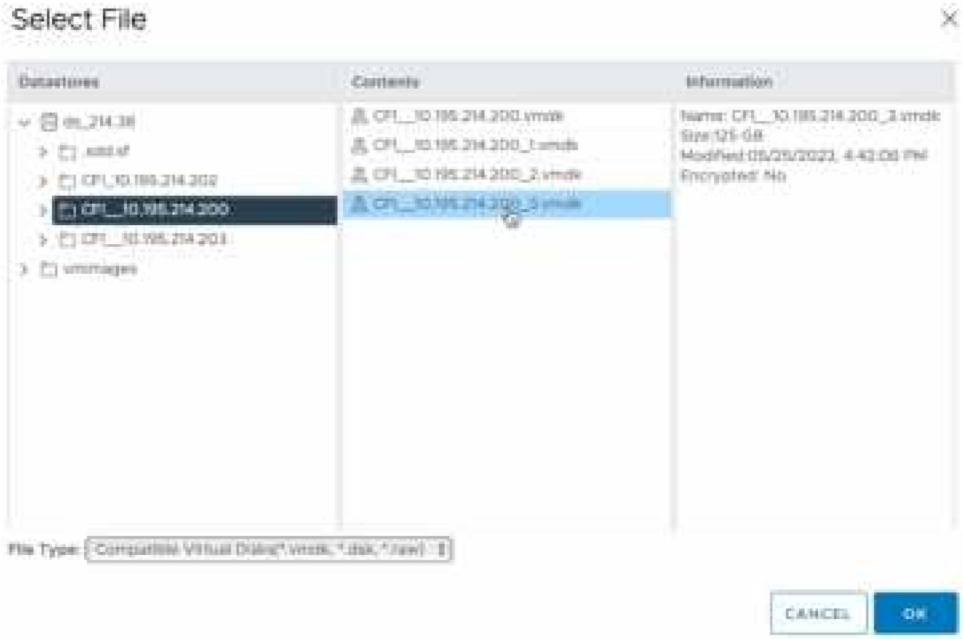


Edit Settings | CFI_10.195.214.202

Virtual Hardware | VM Options

CPU	32	
Memory	256	GB
Hard disk 1	100	GB
Hard disk 2	550	GB
Hard disk 3	2.294921875	TB
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	10_195_NW	
Network adapter 2	17_104_NW	
CD/DVD drive 1	Datastore ISO File	
Video card	Specify custom settings	
VMCI device		
Other	Additional Hardware	

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

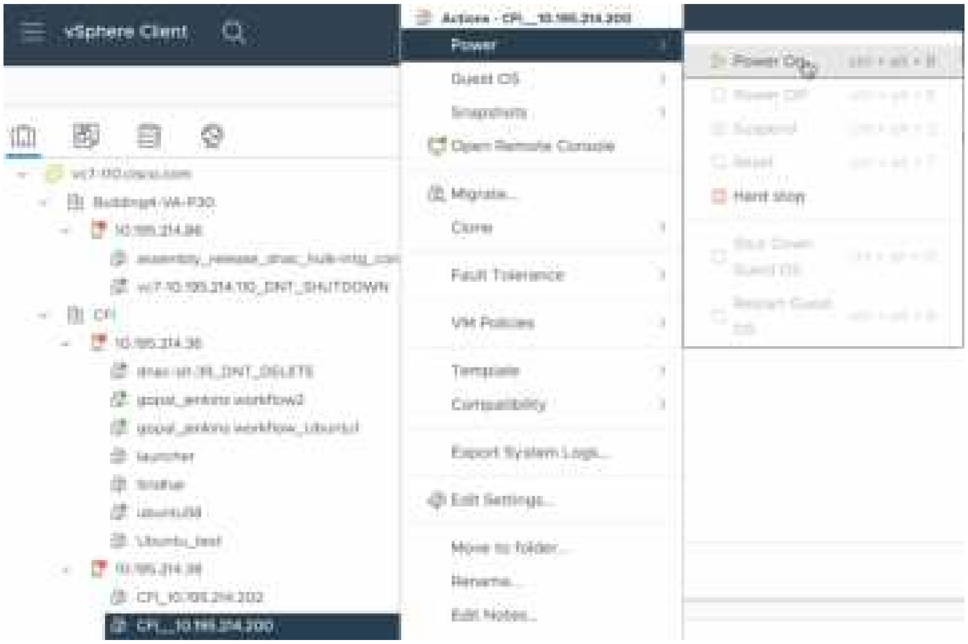


Select File

Datastores	Contents	Information
ds_214.38	CFI__10.195.214.200.vmdk	Name: CFI__10.195.214.200_3.vmdk
add.sf	CFI__10.195.214.200_1.vmdk	Size:125 GB
CFI_10.195.214.202	CFI__10.195.214.200_2.vmdk	Modified:05/25/2023, 4:42:00 PM
CFI__10.195.214.200	CFI__10.195.214.200_3.vmdk	Encrypted: No
CFI__10.195.214.203		
vmimages		

File Type: Compatible Virtual Disks(*.vmdk, *.dsk, *.raw)

e. Power on the appliance's virtual machine.

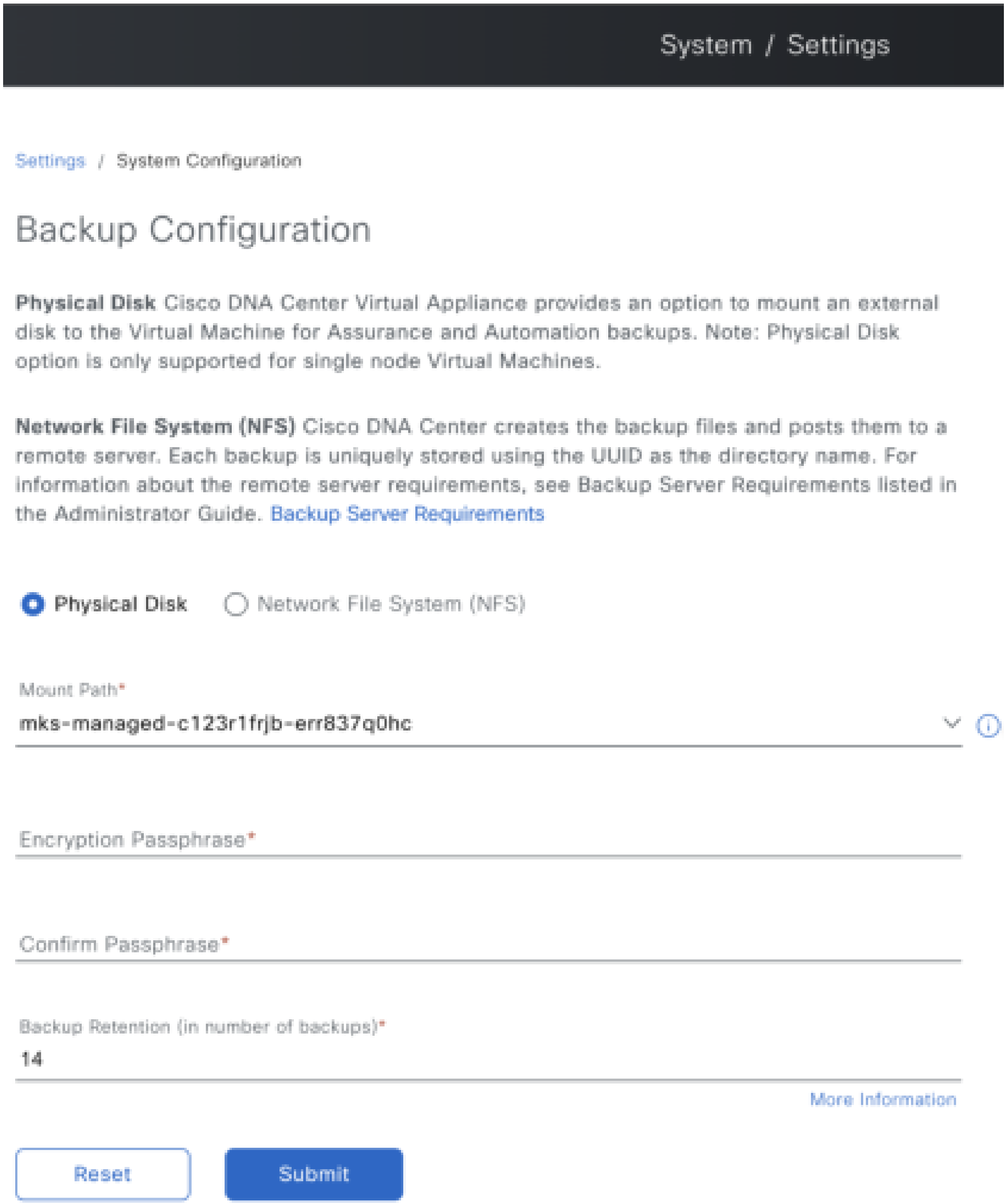


It takes approximately 45 minutes for all the services to restart.

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

Step 2 To configure the storage location for the backup, complete these steps:

a) From the Catalyst Center menu, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.
b) Click the **Physical Disk** radio button.
c) Choose the physical disk from the **Mount Path** drop-down list.



System / Settings

Settings / System Configuration

Backup Configuration

Physical Disk Cisco DNA Center Virtual Appliance provides an option to mount an external disk to the Virtual Machine for Assurance and Automation backups. Note: Physical Disk option is only supported for single node Virtual Machines.

Network File System (NFS) Cisco DNA Center 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 listed in the Administrator Guide. Backup Server Requirements

● Physical Disk ○ Network File System (NFS)

Mount Path*
mks-managed-c123r1frjb-err837q0hc

Encryption Passphrase*

Confirm Passphrase*

Backup Retention (in number of backups)*
14

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

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

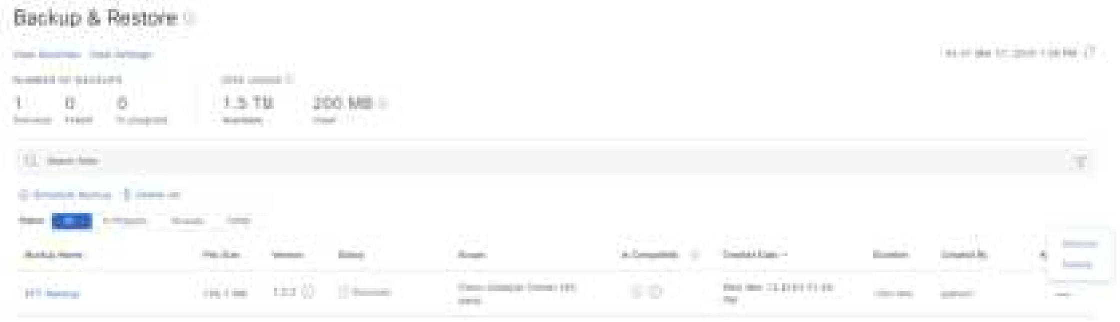
e) Set how long backup files are kept before they are deleted.

f) Click **Submit**.

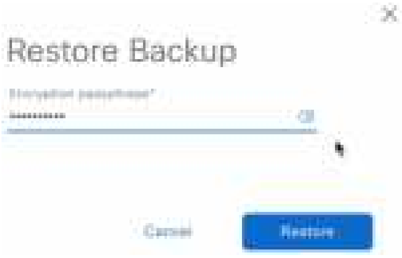
Step 3 To restore the backup, complete these steps:

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

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



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



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

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

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

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

Restore data from an NFS server for a faulty virtual appliance

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

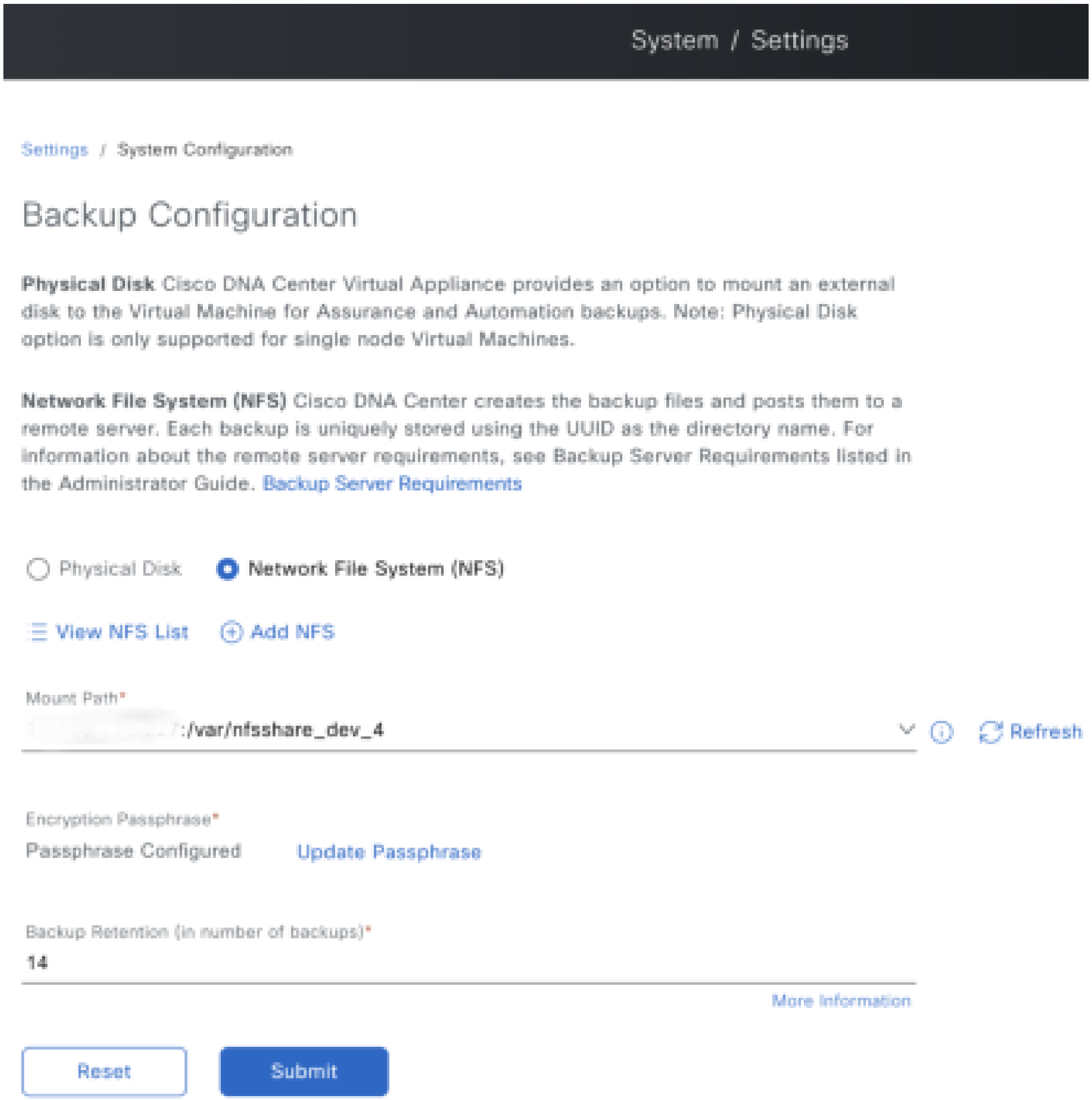
Procedure

Step 1 For your new virtual appliance, complete these steps to configure Catalyst Center to use the NFS server that you configured for the faulty virtual appliance:

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

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

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



Backup Configuration

Physical Disk Cisco DNA Center Virtual Appliance provides an option to mount an external disk to the Virtual Machine for Assurance and Automation backups. Note: Physical Disk option is only supported for single node Virtual Machines.

Network File System (NFS) Cisco DNA Center 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 listed in the Administrator Guide. Backup Server Requirements

○ Physical Disk ● Network File System (NFS)

Mount Path*
[redacted]:/var/nfsshare_dev_4

Encryption Passphrase*
Passphrase Configured

Backup Retention (in number of backups)*
14

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

After the passphrase is configured, if you want to change the passphrase, click **Update Passphrase**.

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

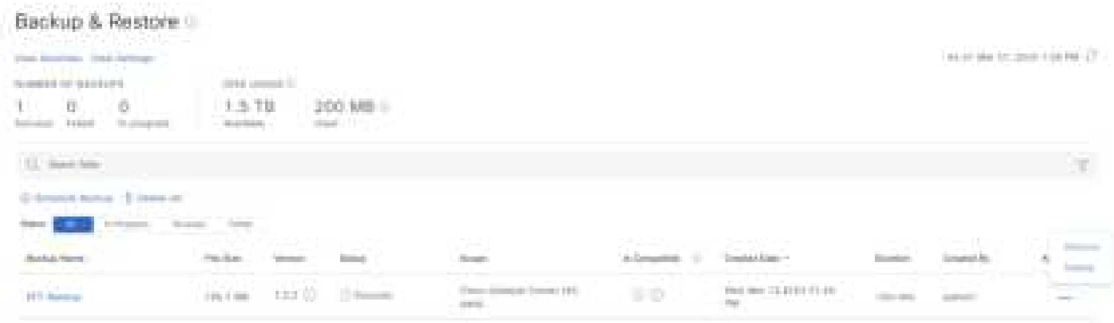
e) Set how long backup files are kept before they are deleted.

f) Click **Submit**.

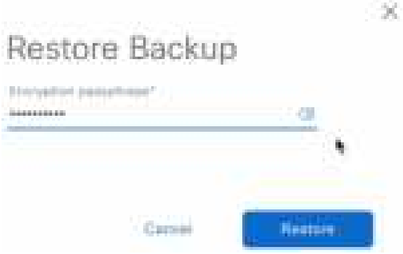
Step 2 To restore the backup, complete these steps:

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

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



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



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

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

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

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

Schedule data backup

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

Before you begin

Make sure that the following requirements are met:

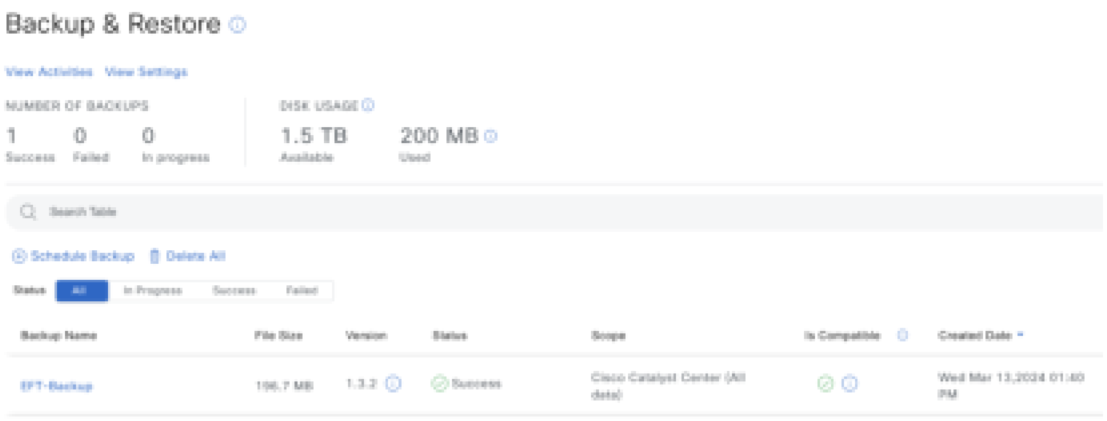
- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in Backup server requirements, on page 173.
- Backup servers have been configured in Catalyst Center. For more information, see Configure the location to store backup files, on page 180.

Procedure

Step 1 From the main menu, choose **System** > **Backup & Restore**.
The **Backup & Restore** window is displayed.

Step 2 Click **Schedule Backup**.

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



Backup & Restore

View Activities View Settings

NUMBER OF BACKUPS: 1 Success, 0 Failed, 0 In progress

DISK USAGE: 1.5 TB Available, 200 MB Used

Search Table

Schedule Backup Delete All

Status: All | In Progress | Success | Failed

Backup Name	File Size	Version	Status	Scope	Is Compatible	Created Date
EFT-Backup	196.7 MB	1.3.2	Success	Cisco Catalyst Center (All data)	✓	Wed Mar 13,2024 01:40 PM

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

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

b. Choose a schedule option:

- **Schedule 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. Define the scope of the backup:

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

d. Click **Save**.

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

Step 4 (Optional) Click **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.

Step 5 (Optional) Click **Edit Schedule** to edit the schedule.

Step 6 (Optional) Click **Delete Schedule** to delete the schedule.

Step 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.

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

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

CHAPTER 7

Implement Disaster Recovery

Overview

Disaster recovery adds another layer of redundancy to safeguard against network downtime. It responds to a cluster failure by handing off network management duties to a connected cluster (referred to as a site going forward). Disaster recovery implementation on Catalyst Center consists of three components: the main site, the recovery site, and the witness site. At any given time, the main and recovery sites are operating in either the active or standby role. The active site manages your network while the standby site maintains a continuously updated copy of the active site's data and managed services. Whenever an active site goes down, Catalyst Center automatically initiates a failover, completing the tasks necessary to designate the former standby site as the new active site.

The following topics provide information about how to set up and use disaster recovery in your production environment.

Key terms

Terms key for understanding disaster recovery implementation on Catalyst Center include:

- **Main Site**: The first site you configure when setting up your disaster recovery system. By default, it operates as the active site that manages your network. For information about how to configure the sites in your system, see Set up disaster recovery, on page 212.

- **Recovery Site**: The second site you configure when setting up your disaster recovery system. By default, it acts as your system's standby site.
- **Witness Site**: The third site you configure when setting up your disaster recovery system. This site, which resides on a virtual machine or separate server, is not involved with the replication of data or managed services. Its role is to give the current active site the quorum it needs to carry out disaster recovery tasks. If a site fails, this site prevents the split brain scenario from taking place. This scenario can occur in a two-member system when the sites cannot communicate with each other. Each site believes that it should become active, creating two active sites. Catalyst Center uses the witness site to arbitrate between the active and standby sites, allowing only one active site at any given time. For information about witness site requirements, see Prerequisites, on page 204.
- **Register**: To add a site to a disaster recovery system, you must first register it with the system by providing information such as your main site's VIP. When registering your recovery or witness site, you will also need to provide the token that is generated when you register your main site. For more information, see Set up disaster recovery, on page 212.
- **Configure Active**: The process of establishing a site as the active site, which involves tasks such as exposing the appropriate managed service ports.
- **Active site**: The site that is currently managing your network. Catalyst Center continuously replicates its data to your standby site.
- **Configure Standby**: The process of establishing a site as the standby site, which involves tasks such as configuring the replication of the active site's data and disabling the services which manage the network on the standby site.
- **Standby Ready**: When an isolated site meets the prerequisites to become a standby site, Catalyst Center moves it to this state. To establish this site as your system's standby site, click **Rejoin** in the **Action** area.
- **Standby site**: The site that maintains an up-to-date copy of your active site's data and managed services. If your active site goes down, your system initiates a failover and your standby site takes over as the active site.

Note A message will indicate when you are currently viewing your system's standby site. You need to initiate all disaster recovery tasks from the active site.

- **Failover**: Catalyst Center supports two types of failover:
  - System-triggered: As soon as Catalyst Center recognizes that your active site has gone down, it automatically carries out the tasks required to establish your standby site as the new active site. You can monitor these tasks from the Event Timeline.
  - Manual: You can initiate a manual failover to designate the current standby site as the new active site. For more information, see Initiate a manual failover, on page 229.

Important

- After a failover, Assurance restarts and processes a fresh set of data on the new active site. Historical Assurance data from the former active site is *not* migrated over.
- After a failover, the Catalyst Center inventory service triggers a full device sync. This can take anywhere from a few minutes to a few hours, depending on the number of devices that are managed. As is the case when Catalyst Center's normally scheduled device sync is running, you will not be able to provision devices on the newly activated cluster until the device sync triggered by a failover completes.

- **Isolate**: During a failover, the former active site is separated from the disaster recovery system. Catalyst Center suspends its services and stops advertising its virtual IP address (VIP). From here, Catalyst Center completes the tasks necessary to establish the former standby site as the new active site.
- **Pause**: Temporarily suspend your disaster recovery system in order to separate the sites that make up your system and stop data and service replication. For more information, see Pause your disaster recovery system, on page 225.
- **Rejoin**: From the **Disaster Recovery** > **Monitoring** tab, click this button in the **Action** area in order to add a Standby Ready or Paused site back into a disaster recovery system as the new standby site (after a failover has taken place). You would also click this button in order to restart a disaster recovery system that is currently paused.
- **Activate DR**: User-initiated operation that creates your system's active and standby sites. This operation entails setting up intracluster communication, verifying that the sites meet disaster recovery prerequisites, and replicating data between the two sites.
- **Deregister**: Click this button in the **Action** area to remove the three sites you have configured for your disaster recovery system. You must do so in order to make changes to any of the site settings you have entered previously.
- **Retry**: In the **Action** area, click this button in order to reinitiate any action that failed previously.
- **VIP Promotion**: When this option is enabled, the Enterprise interface VIP configured for your Catalyst Center deployment is promoted for use as your system's disaster recovery VIP. For more information, see the "VIP Promotion" section in Main site registration considerations, on page 212.

Data replication overview

The data replication process syncs data between your disaster recovery system's main site and recovery site. Its duration depends on a few factors: the amount of data that needs to be replicated, your network's effective bandwidth, and the amount of latency that exists between the main and recovery sites. When disaster recovery is active for your Catalyst Center deployment, data replication will *not* impact any operations or application use on the current active site (which is managing your network).

Important

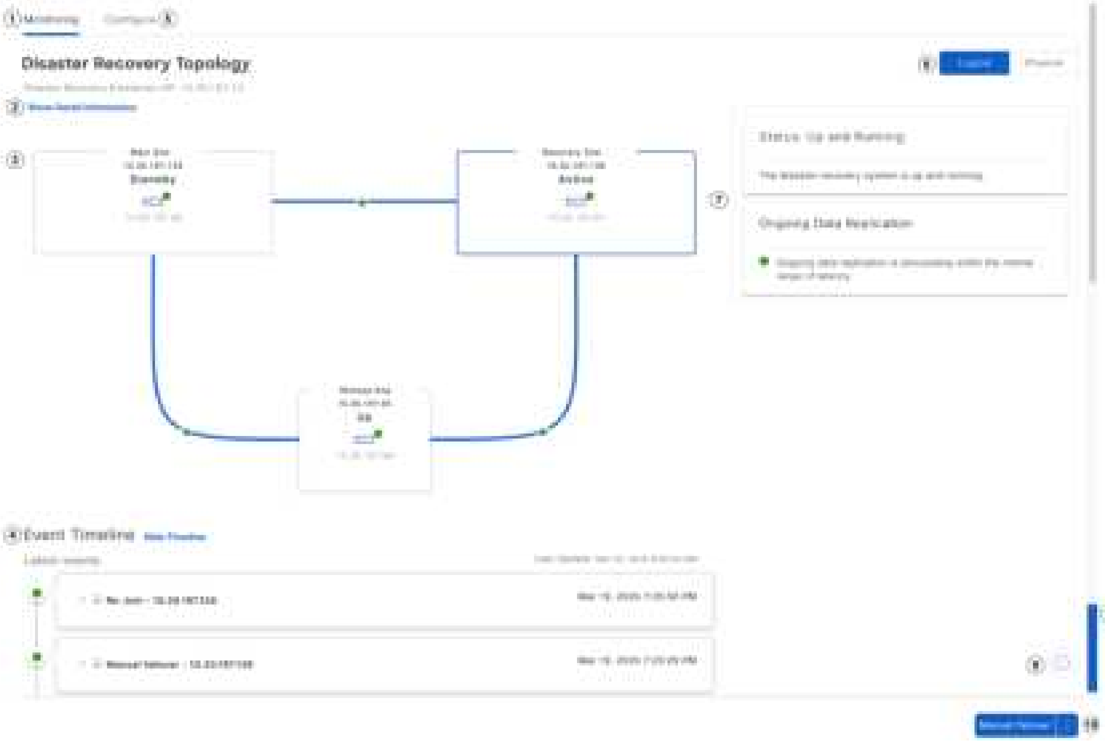
After a failover takes place, Assurance data from the site that failed is *not* replicated. The site that takes over as your system's active site will collect a new set of Assurance data.

Either a full or incremental replication of data takes place, depending on which of these scenarios is applicable:

- **After initial activation**: After the initial configuration and activation of your disaster recovery system, the recovery site does not have any data. In this scenario, a full replication of data between the main and recovery sites happens.
- **After a failover**: Whenever the current active site fails, the disaster recovery system triggers a failover. In this scenario, a full data replication between the main and recovery sites occurs after the failed site rejoins the system.
- **During normal operation**: This scenario will typically apply to your system. During its day-to-day operation, changes that take place on the current active site are continuously synced with the current standby site.

Navigate the disaster recovery GUI

The table describes the components that make up Catalyst Center's disaster recovery GUI and their function.



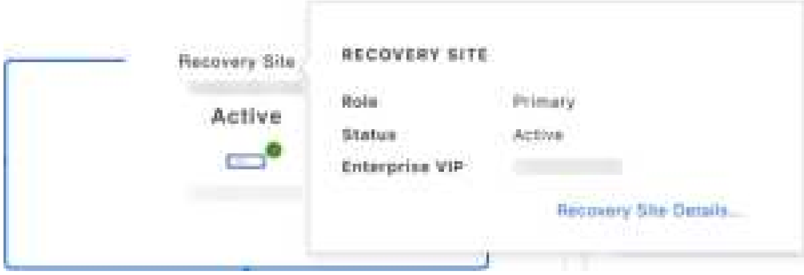
Callout	Description
1	**Monitoring** tab: Click to do the following: • View a topology of the sites that make up your system. • Determine the current status of your system. • Perform disaster recovery tasks. • View a listing of the tasks that have been completed to date.

Callout	Description
2	**Show Detail Information** link: Click to open the **Disaster Recovery System** slide-in pane. See View disaster recovery system status, on page 203 for more information.
3	**Topology**: Displays either a logical or physical topology of your system that indicates the current status of your sites and their members. • In both the logical and physical topologies, a blue box indicates the site that's currently acting as your system's active site. • In the logical topology, a blue line indicates that the IPSec tunnel connecting two sites is operational, and a red line indicates that the tunnel is currently down. • To view a description of the possible site states, see System and site states, on page 241.
4	**Event Timeline**: Lists every disaster recovery task that is currently in progress or has been completed for your system. For more information, see Monitor the event timeline, on page 237.
5	**Configure** tab: Click to enter the settings necessary to establish a connection between your disaster recovery system's sites. See Set up disaster recovery, on page 212 for more information.
6	**Logical** and **Physical** tabs: Click the appropriate tab to toggle between a logical and physical topology of your system.
7	• **Status** area: Indicates the current status of your system. To view a description of the possible system states, see System and site states, on page 241. • **Ongoing Data Replication** area: Indicates the replication status of GlusterFS, MongoDB, and Postgres data between your system's sites. For more information, see Monitor managed services replication, on page 240.
8	**Interactive Help** button: Click to open a slide-in pane that provides links to walkthroughs that provide on-screen guidance to help you complete specific tasks in Catalyst Center.
9	**Legend**: Indicates what the topology icons represent. To view the legend, click ○ in the bottom right corner of the **Disaster Recovery** window.
10	**Action** area: Displays the disaster recovery tasks that are currently available for you to initiate. The tasks you can choose from vary, depending on whether you have configured your sites and your system's status.

View disaster recovery system status

The topology provides a graphical representation of your disaster recovery system's current status. If you want to view this information in a tabular format, you can do so in the **Disaster Recovery System** slide-in pane. To open this pane, do one of these tasks:

- Click the **Show Detail Information** link. Then expand the site for which you want to view the status in the slide-in pane.
- In the topology, place your cursor over a site's Enterprise virtual IP address or a particular node's icon. In the dialog box that opens, click the link in the bottom-right corner.



Recovery Site

Active

RECOVERY SITE

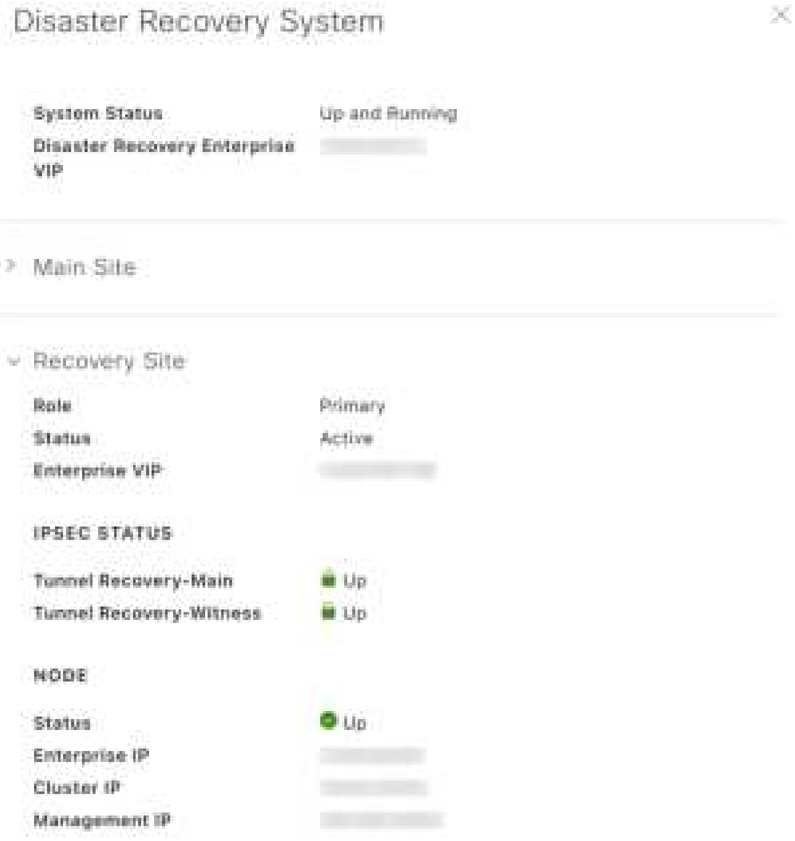
Role Primary

Status Active

Enterprise VIP [redacted]

Recovery Site Details...

The slide-in pane opens and displays the relevant site information.



Disaster Recovery System

System Status Up and Running

Disaster Recovery Enterprise VIP [redacted]

Main Site

Recovery Site

Role Primary

Status Active

Enterprise VIP [redacted]

IPSEC STATUS

Tunnel Recovery-Main Up

Tunnel Recovery-Witness Up

NODE

Status Up

Enterprise IP [redacted]

Cluster IP [redacted]

Management IP [redacted]

Prerequisites

Before you enable disaster recovery in your production environment, ensure that the prerequisites are met.

Witness Prerequisites

Important

- If you plan to upgrade to the latest Catalyst Center version, you must complete several steps to ensure that disaster recovery works properly after the upgrade. See Configure disaster recovery on an upgraded Catalyst Center appliance, on page 209.
- Disaster recovery does not support IPv6.

General Prerequisites

- Catalyst Center supports two disaster recovery setups:
  - **1+1+1 setup**: One Catalyst Center appliance functions as your Main Site, a second appliance serves as your Recovery Site, and a third system (residing on a virtual machine) acts as your Witness Site. These appliances and versions support this setup:
    - DN2-HW-APL (44-core second-generation appliance): Catalyst Center 2.2.2.x and later
    - DN3-HW-APL (32-core third-generation appliance): Catalyst Center 2.3.7.6 and later
    - DN2-HW-APL-L (56-core second-generation appliance): Catalyst Center 2.2.1.x and later
    - DN3-HW-APL-L (56-core third-generation appliance): Catalyst Center 2.3.7.6 and later
    - DN2-HW-APL-XL (112-core second-generation appliance): Catalyst Center 2.2.1.x and later
    - DN3-HW-APL-XL (80-core third-generation appliance): Catalyst Center 2.3.7.6 and later
  - **3+3+1 setup**: One three-node Catalyst Center cluster functions as your Main Site, a second three-node cluster serves as your Recovery Site, and a third system (residing on a virtual machine) acts as your Witness Site. These appliances and versions support this setup:
    - DN2-HW-APL (44-core second-generation appliance): Catalyst Center 2.2.2.x and later
    - DN3-HW-APL (32-core third-generation appliance): Catalyst Center 2.3.7.6 and later
    - DN2-HW-APL-L (56-core second-generation appliance): Catalyst Center 2.1.2.x and later
    - DN3-HW-APL-L (56-core third-generation appliance): Catalyst Center 2.3.7.6 and later
    - DN2-HW-APL-XL (112-core second-generation appliance): Catalyst Center 2.1.2.x and later
    - DN3-HW-APL-XL (80-core third-generation appliance): Catalyst Center 2.3.7.6 and later
- You have configured a VIP for the Enterprise port interface on your Catalyst Center appliances. This is required because disaster recovery uses the Enterprise network for intrasite communication. In the Catalyst Center Appliance Installation guide, refer to these topics:
  - For more information about the Enterprise port, see the "Interface Cable Connections" topic.
  - For more information about Enterprise port configuration, see either the "Configure the Primary Node Using the Maglev Wizard" or "Configure the Primary Node Using the Advanced Install Configuration Wizard" topic.
- You have assigned a super-admin user to carry out disaster recovery tasks. Only users with this privilege level can access this functionality.
- You have confirmed that the links connecting the following sites are 1 Gbps with at most 350 ms RTT latency.
  - Main and recovery sites
  - Main and witness sites
  - Recovery and witness sites

Note Although a one Gbps link is recommended for connections with the witness site, the actual bandwidth the witness site uses is 50 Mbps. As long as the link speed is faster than this, you should not encounter any issues.

Main and Recovery Site Prerequisites

- Both your main and recovery site must consist of the same number of nodes. Catalyst Center does not allow you to register and activate a disaster recovery system that does not meet this requirement.

- Both your main and recovery site must consist of Catalyst Center appliances that have the same hardware profile. For example, a site can consist of second-generation 112-core and third-generation 80-core appliances. This table lists the appliances that support disaster recovery and their corresponding Cisco part number:

  Table 13: Supported Catalyst Center appliances

Machine Profile	Machine Profile Alias	Cisco Part Number	Number of Cores
medium	medium	First-generation: • DN1-HW-APL • DN1-HW-APL-U (promotional)	44
		Second-generation: • DN2-HW-APL • DN2-HW-APL-U (promotional)	
		Third-generation: DN3-HW-APL	32
t2_large	large	Second-generation: • DN2-HW-APL-L • DN2-HW-APL-L-U (promotional)	56
		Third-generation: DN3-HW-APL-L	
t2_2xlarge	extra large	Second-generation: • DN2-HW-APL-XL • DN2-HW-APL-XL-U (promotional)	112
		Third-generation: DN3-HW-APL-XL	80

  Also ensure that your main and recovery site are running the same Catalyst Center version.

- Catalyst Center 2.3.7.9 adds support for mixed three-node clusters that have HA enabled. A valid mixed cluster meets these requirements:

  - It consists of second- and third-generation Catalyst Center appliances. First-generation appliances are not supported.
  - Its three appliances have the same machine profile. For example, a cluster with two second-generation large appliances and one third-generation large appliance is a valid mixed cluster.

- You have configured and enabled high availability (HA) on both your main and recovery site. Otherwise, the registration of these sites fails. For more information, see the latest Catalyst Center High Availability guide.

Important This is applicable to three-node setups only.

- Ensure that the main and recovery site have the same Federal Information Processing Standards (FIPS) mode setting. If FIPS mode is enabled on one site and disabled on the other, the registration of your disaster recovery system fails because of a validation error. For more information on FIPS mode, see the description of the **IP addressing mode used for the services** screen (located in the Catalyst Center Appliance Installation guide's "Configure the Primary Node Using the Maglev Wizard" topic).

- If you want to use Border Gateway Protocol (BGP) to advertise your system's virtual IP address routes, you need to configure your system's Enterprise virtual IP address on each of the main and recovery site's neighbor routers. The configuration you need to enter will look similar to one the following examples:

  Interior BGP (iBGP) Configuration Example

```
router bgp 64555
 bgp router-id 10.30.197.57
 neighbor 172.25.119.175 remote-as 64555
 neighbor 172.25.119.175 update-source 10.30.197.57
 neighbor 172.25.119.175 next-hop-self
```

  where:

  - `64555` is the neighbor router local and remote AS number.
  - `10.30.197.57` is the neighbor router IP address.
  - `172.25.119.175` is your system Enterprise virtual IP address.

  Exterior BGP (eBGP) Configuration Example

```
router bgp 62121
 bgp router-id 10.30.197.57
 neighbor 172.25.119.175 remote-as 64555
 neighbor 172.25.119.175 update-source 10.30.197.57
 neighbor 172.25.119.175 next-hop-self
 neighbor 172.25.119.175 ebgp-multihop 255
```

  where:

  - `62121` is the neighbor router local AS number.
  - `64555` is the neighbor router remote AS number.
  - `10.30.197.57` is the neighbor router IP address.
  - `172.25.119.175` is your system Enterprise virtual IP address.

- If you enable BGP route advertisement (as described in the previous bullet), we recommend that you filter routes towards Catalyst Center in order to improve its performance. To do so, enter this configuration:

  ```
  neighbor system's-Enterprise-virtual-IP-address route-map DENY_ALL out
  !
  ip prefix-list DENY_ALL seq 5 deny 0.0.0.0/0 le 32
  !
  route-map DENY_ALL permit 10
  match ip address prefix-list DENY_ALL
  ```

Witness Site Prerequisites

- You have confirmed that the virtual machine that hosts your witness site is running (at a minimum) VMware ESXi hypervisor version 7.0 or later with a 2.1-GHz core and two virtual CPUs, 4 GB of RAM, and 15 GB of hard drive space.
- Confirm that the hostname of the witness site's VM contains a maximum of 20 characters. Configuration of the witness site and disaster recovery system might fail if the witness site's hostname exceeds this limit.
- Witness site deployment in a public cloud is not supported.
- You have set up your witness site in a different location than your main and recovery sites and confirmed that it is reachable from both of these sites.
- You have configured an NTP server that is accessible by the witness site. You must synchronize this NTP server with the NTP servers that are used by the main and recovery sites.
- The witness site utilizes approximately 50 Mbps of actual bandwidth. This bandwidth is used primarily for monitoring the connections (WAN, LAN, private circuits) between the witness site and the primary/standby sites.

Certificate Prerequisites

- You have generated one third-party certificate and installed the same certificate on both the main and recovery sites. Otherwise, site registration fails.

  Note Catalyst Center copies this certificate to the witness site automatically during the registration process.

  Ensure that all of the IP addresses (especially the Enterprise port's virtual IP address) and fully qualified domain names (**FQDN**) that the main and recovery sites use are included in this certificate. Also ensure that **digitalSignature** is specified for the certificate's **keyUsage** parameter. For a description of how to generate a third-party certificate, see Generate a Certificate Request Using Open SSL in the *Catalyst Center Security Best Practices Guide*.

- In the certificates installed on the main and recovery sites, make sure that the first non-wildcard DNS name specified in each certificate match. If you use the same certificate for Catalyst Center, confirm that its certificate's first non-wildcard DNS name also matches.
- If you are using an FQDN-only certificate, ensure that the same **cluster_hostname**—that is, the FQDN for Catalyst Center (set in the Catalyst Center configuration wizard)—is configured on both the main and recovery sites, as well as Disaster Recovery's VIP.

Configure disaster recovery on an upgraded Catalyst Center appliance

To successfully configure disaster recovery after upgrading your system to the latest Catalyst Center version, complete these steps:

Procedure

Step 1 Install the witness site, on page 210.

Step 2 Set up disaster recovery, on page 212.

Add the disaster recovery certificate

Catalyst Center supports the import and storage of an X.509 certificate and private key into Catalyst Center. The disaster recovery certificate is used for intracluster communications.

You must obtain a valid X.509 certificate that is issued by your internal CA and the certificate must correspond to a private key in your possession.

Note

- If you want your disaster recovery system to use the same certificate that Catalyst Center uses, you can skip this procedure. When you configure the certificate, make sure that you check the **DR** check box (see Update the Catalyst Center server certificate, on page 93).
- For more information about the disaster recovery certificate requirements, reference the Security Best Practices Guide.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **System Certificates**.

Step 2 Open the **Import Certificate** slide-in pane by clicking **Import Certificate**.

Step 3 In the **Add Certificate** area, choose the file format type for the certificate that you are importing into Catalyst Center:

- **PEM**: Privacy-enhanced mail file format
- **PKCS**: Public-Key Cryptography Standard file format

Step 4 If you chose **PEM**, perform the following tasks:

a) Import the certificate by dragging and dropping the PEM file into the highlighted area.

Note
A PEM file must have a valid PEM format extension (.pem). The maximum file size for the certificate is 10 MB.

After the upload succeeds, the system certificate is validated.

b) In the **Private Key** area, import the private key by dragging and dropping it into the highlighted area.

Note
Private keys must have a valid private key format extension (.key). The maximum file size for the private key is 10 MB.

After the upload succeeds, the private key is validated.

c) Specify whether the private key will be encrypted by clicking the appropriate radio button.
d) If the private key will be encrypted, enter its password in the **Password** field.

Step 5 If you chose **PKCS**, do these tasks:

a) Import the certificate by dragging and dropping the PKCS file into the highlighted area.

Note
A PKCS file must have a valid PKCS format extension (.pfx or .p12). The maximum file size for the certificate is 10 MB.

After the upload succeeds, the system certificate is validated.

b) In the **Password** field, enter the certificate's password (a PKCS requirement).
c) Specify whether the private key will be encrypted by clicking the appropriate radio button.
d) If the private key will be encrypted, enter its password in the **Password** field.

Step 6 Click **Save**.

After the Catalyst Center server’s SSL certificate is replaced, you are automatically logged out and you must log in again.

Install the witness site

Complete this procedure to set up the virtual machine to serve as the witness site for your disaster recovery system.

Procedure

Step 1 Download the OVF package that's specific to the Catalyst Center version that the witness site is running:

a) Open https://software.cisco.com/download/home/286316341/type.

Note
You need a Cisco.com account to access this URL. See the following page for a description of how to create an account: https://www.cisco.com/c/en/us/about/help/registration-benefits-help.html

b) In the **Select a Software Type** area, click the Catalyst Center software link.

The **Software Download** page updates, listing the software available for the latest Catalyst Center release.

c) Do one of these:

- If the OVF package (*.ova) you need is already listed, click its **Download** icon.
- Enter the relevant version number in the **Search** field, click its link in the navigation pane, and then click the **Download** icon for that version's OVF package.

Step 2 Copy this package to a local machine running VMware vSphere 7.0 or later.

Step 3 From the vSphere client, choose **File** > **Deploy OVF Template**.

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

a) Follow the instructions in the **Source** screen:

1. Click **Browse**.
2. Navigate to the witness site OVF package (.ova).
3. Click **Open**.
4. In the **Deploy from a file or URL** field, verify that the package path displays and then click **Next**.

   The **OVF Template Details** screen opens.

b) Click **Next >**.

c) Following the instructions in the **Name and Location** screen:

- In the **Name** field, enter the name you want to set for the package.
- In the **Inventory Location** field, select the folder that you want the package to reside in.
- Click **Next >**.

The **Host/Cluster** screen opens.

d) Click the host or cluster on which you want to run the deployed template and then click **Next >**.

The **Storage** screen opens.

e) Click the storage drive for the virtual machine files to reside on and then click **Next >**.

The **Disk Format** screen opens.

f) Click the **Thick Provision** radio button and then click **Next**.

g) Follow the instructions in the **Network Mapping** screen and then click **Next**:

1. Click the IP address that is listed in the **Destination Networks** column.
2. In the resulting drop-down list, choose the network that the deployed template should use.

The **Ready to Complete** screen opens, displaying all of the settings that you have entered.

h) Check the **Power on after deployment** check box and then click **Finish**.

i) When the **Deployment Completed Successfully** dialog box opens, click **Close**.

Step 5 Enter the network settings for your witness site:

a) Open a console to the virtual machine you just created by doing one of these tasks:

- Right-click the virtual machine from the vSphere Client list and choose **Open Console**.
- Click the **Open Console** icon in the vSphere Client menu.

The **Witness User Configuration** window opens.

b) Enter and confirm the desired password for the admin user (*maglev*), then press **N** to proceed.

c) Enter these settings, then press **N** to proceed:

- Its IP address

- The netmask associated with the virtual machine IP address
- The IP address of your default gateway
- **(Optional)** The IP address of the preferred DNS server

d) Enter one or more NTP server addresses or hostnames (separated by spaces), then press **S** to submit your settings and begin the configuration of the witness site.

At least one NTP address or hostname is required.

e) Verify that configuration has completed by using SSH port 2222 to log in to the IP address you configured for the witness site.

Note
Later, if you need to change the password configured for the **maglev** user on the witness site's VM, use the standard Linux **passwd** utility. You don't need to pause the disaster recovery system before doing this, and the password change will have no functional impact on disaster recovery operation.

Set up disaster recovery

Setting up disaster recovery in your Catalyst Center deployment is a two-step process. The first step is to register the sites that will comprise your disaster recovery system. The second step is to activate your system, enabling disaster recovery. Refer to this section's topics for a description of the steps you need to complete, as well as information on the errors you may encounter during this process and how to deal with them.

Main site registration considerations

Before you register your disaster recovery system's main site, you'll need to decide how to make use of the following features.

VIP Promotion

You'll need to decide whether you want to use the Enterprise interface VIP configured for your Catalyst Center deployment as your system's disaster recovery VIP. VIP promotion is suitable only if all of these items are applicable:

- You have a brownfield deployment, where an existing Catalyst Center instance is managing the network and all devices are configured with the instance's Enterprise VIP. This instance will act as your disaster recovery system's main site.
- The existing Enterprise interface VIP address is allowed to float between the two data centers where your main and recovery sites will reside. This is usually applicable in the case of an extended L2 network that spans multiple data centers.
- You don't want the existing devices to be reconfigured when the new disaster recovery system's Enterprise interface VIP.

If you want to use VIP promotion, complete Steps 2b through 2e in Register the main site, on page 213, clicking the **Yes** radio button in Step 2b.

Route Advertisement Options

You'll then need to decide the route advertisement option your deployment will use. One of disaster recovery's main objectives is to enable continuous network operation after a failover takes place without the need for device reprovisioning. This is achieved by specifying a floating VIP that's automatically configured on the disaster recovery system's current active site. Whenever a failover occurs, this VIP (referred to as the disaster recovery VIP in this chapter) is cleared from the previous active site and set on the new active site. This ensures that your network's devices can continue to communicate with Catalyst Center, regardless of which site is currently active. There are three route advertisement option to choose from when you complete Step 2g in Register the main site, on page 213:

- **Border Gateway Protocol (BGP)**: This option, which is recommended for most disaster recovery systems, is selected by default. BGP route advertisement ensures that you can access your system's current active site, which is critical after a failover takes place.

Important If you want to use this option, first complete the steps described in the last two bullets of the "Main and Recovery Site Prerequisites" section (which can be found in the Prerequisites, on page 204 topic).

- **Disaster recovery VIPs without route advertisement**: Choose this option if you want to configure virtual IP addresses for your system whose routes are not advertised using BGP. This option is suitable for data centers where both the main and recovery sites can access the subnet that the system's global virtual IP addresses reside within.

- **No disaster recovery VIPs**: When this option is selected, the virtual IP address that's configured for a site is automatically configured on the devices that belong to that site. Each time a failover takes place, this virtual IP address is reconfigured on the devices.

Register the main site

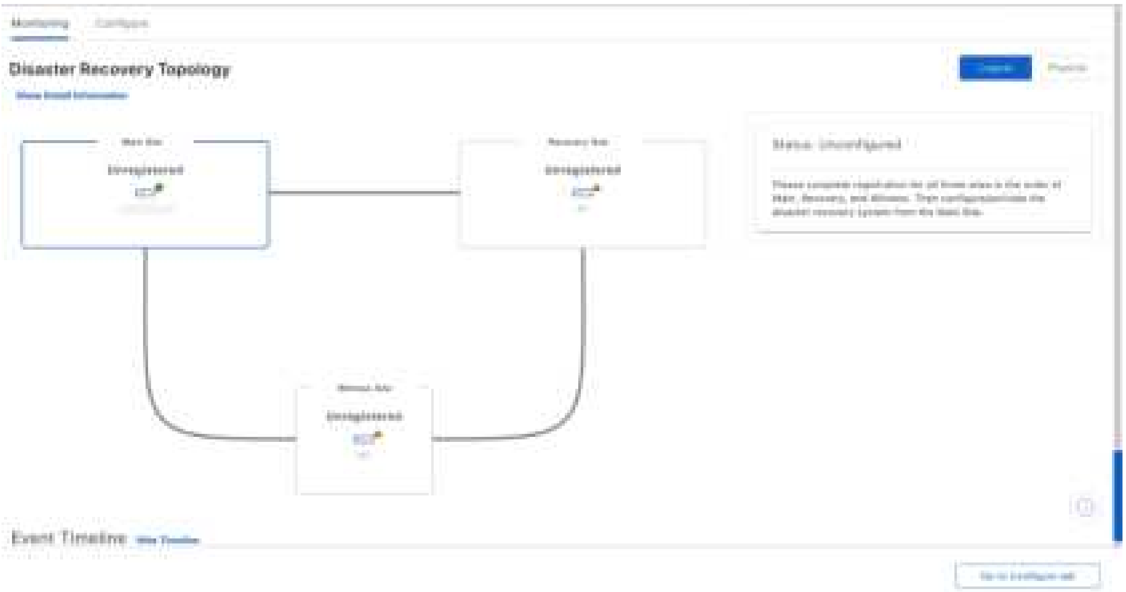
Complete this procedure to register your system's main site.

Before you begin

- Ensure that you've reviewed Main site registration considerations, on page 212.
- On the Catalyst Center appliances or clusters where your disaster recovery system's main and recovery site will reside, do these tasks:
  - Configure the same backup schedule and proxy server. If you don't take care of this before you activate your system, you'll need to specify these two settings again after a failover occurs and the recovery site becomes the active site.
  - Configure an NFS backup configuration where each site points to a different NFS device.

Procedure

Step 1 From the main menu, choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

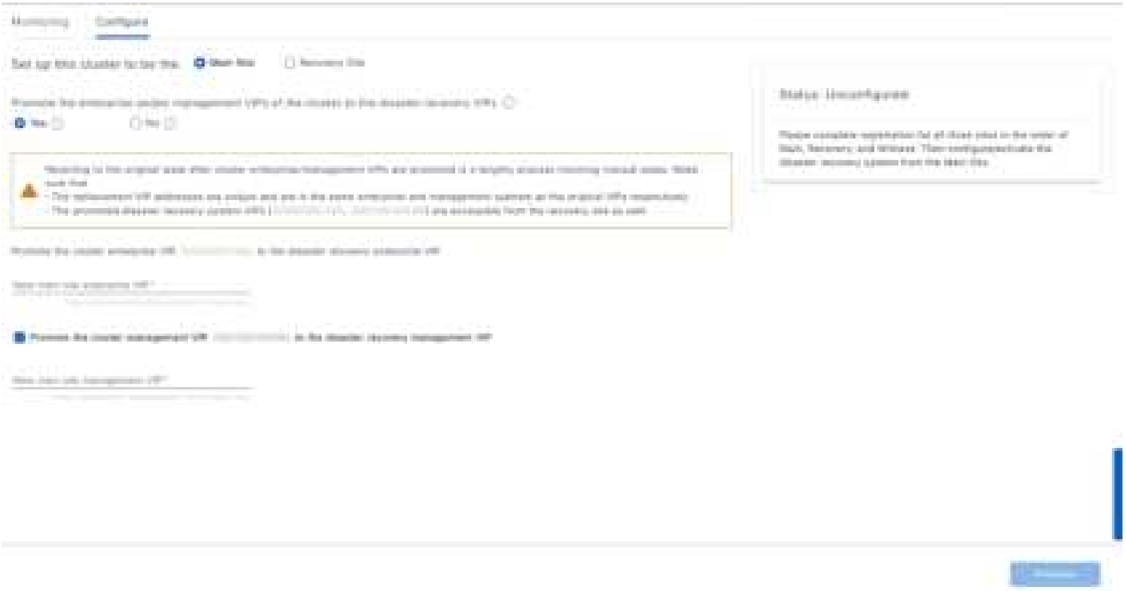


The **Monitoring** tab is selected, by default.

Step 2 Register your main site:

a) Click the **Configure** tab.

The **Main Site** radio button should already be selected.



b) In the **Promote the enterprise and/or management VIPs of the cluster to the disaster recovery VIPs** area, click one of these radio buttons:

- Click **Yes** to set up a cluster as the main site and automatically propagate virtual IP address changes to the devices that are connected to this cluster. This is accomplished by promoting the virtual IP addresses that are currently configured for the cluster and assigning them as your disaster recovery system's global virtual IP addresses. We recommend choosing this option if you are enabling disaster recovery on a cluster that has a lot of connected devices. Otherwise, these devices will need to be reconfigured to communicate with the new disaster recovery virtual IP address. If you choose this option:

1. In the **New main site enterprise VIP** field, enter a new virtual IP address for the site's Enterprise network. This will replace the address that is going to be promoted. Ensure that it is a unique address that is not already used and that it resides in the same subnet as the previous virtual IP address.

2. (Optional) Check the **Promote the cluster management VIP, <*IP-address*>, to the disaster recovery management VIP** check box.

3. (Optional) In the **New main site management VIP** field, enter a new virtual IP address for the site's Management network. This will replace the address that is going to be promoted. Ensure that it is a unique address that is not already used and that it resides in the same subnet as the previous virtual IP address.

- Click **No** to set up a cluster as the main site without propagating virtual IP address changes to connected devices. We recommend this option for a brand-new cluster that isn't connected to any devices yet or is only connected to a few devices. If you choose this option, skip ahead to Step 2f.

c) In the **Action** area, click **Promote**.

The **Disaster Recovery VIP Promotion** dialog opens.

d) Click **Continue**.

Catalyst Center validates the virtual IP addresses you entered.

e) In the **VIP Promotion Status** area, view the validation status:

- If any of the addresses you entered are invalid (likely because it doesn't reside in the same subnet as the address it's replacing), make the necessary corrections and repeat Step 2c.

- If the addresses you entered are successfully validated, the **VIP Promotion Status** area lists all of the virtual IP addresses that will be configured for your disaster recovery system. Proceed to the next step.

f) Enter this information in the **Site VIP/IP addresses** area:

- **Main Site VIP**: The virtual IP address that manages traffic between the active site's cluster nodes and your Enterprise network. Catalyst Center prepopulates this field, based on your system's information.

- **Recovery Site VIP**: The Enterprise virtual IP address that manages traffic between the recovery site's cluster nodes and your Enterprise network.

- **Witness Site IP**: The IP address that manages traffic between the witness site's virtual machine and your Enterprise network.

Important
Ensure that the addresses that you enter are currently reachable. Otherwise, the registration of your system's sites will fail.

Note
At any point between Steps 2f and Step 2j, you can click **Reset** to clear all of the settings that you have entered. You will then need to repeat Step 2f and enter the correct settings before you register the main site.

g) Click one of these radio buttons in the **Route advertisement** area:

- **Border Gateway Protocol (BGP)**: This is the recommeded option.

- **Disaster recovery VIPs without route advertisement**
- **No disaster recovery VIPs**: Skip ahead to Step 2k if you click this radio button.

h) If you clicked either of the first two radio buttons in the previous step, enter a value in the **Enterprise VIP for Disaster Recovery** field.

When configured, this floating virtual IP address automatically moves to and operates on the site that is currently acting as your network's active site. This address manages traffic between your disaster recovery system and your Enterprise network.

Note

- If you clicked the **Border Gateway Protocol (BGP)** radio button and don't want to configure a Management virtual IP address, skip ahead to Step 2j.
- If you clicked the **Disaster recovery VIPs without route advertisement** radio button and don't want to configure a Management virtual IP address, skip ahead to Step 2k.

i) (Optional) Enter a value in the **Management VIP for Disaster Recovery** field.

When configured, this floating virtual IP address automatically moves to and operates on the site that is currently acting as your network's active site. This address manages traffic between your disaster recovery system and your Management network.

j) If you clicked the **Border Gateway Protocol (BGP)** radio button, enter the information required to enable route advertisement:

- In the **Border Gateway Protocol Type** area, specify whether your BGP peers will establish exterior (**Exterior BGP (eBGP)**) or interior (**Interior BGP (iBGP)**) sessions with one another.
- In the **Main Site Router Settings for Enterprise Network** and **Recovery Site Router Settings for Enterprise Network** areas, enter the IP address of the remote router that Catalyst Center will use to advertise the Enterprise virtual IP address that's configured for the disaster recovery system's Main and Recovery sites. Also enter the router's remote and local AS numbers.

  Note these points:

  - Click the **Add** (**+**) icon if you want to configure an additional remote router. You can configure a maximum of two routers for each site.
  - When entering an AS number, ensure that it's a 32-bit unsigned number that falls within the 1–4,294,967,295 range.
  - When the **iBGP** option is selected, Catalyst Center will automatically set the local AS number to the value you enter as the remote AS number.
  - If you configured a Management virtual IP address in the previous step, the **Main Site Router Settings for Management Network** and **Recovery Site Router Settings for Management Network** areas are also displayed. Enter the appropriate information for the remote router that Catalyst Center will use to advertise this virtual IP address.

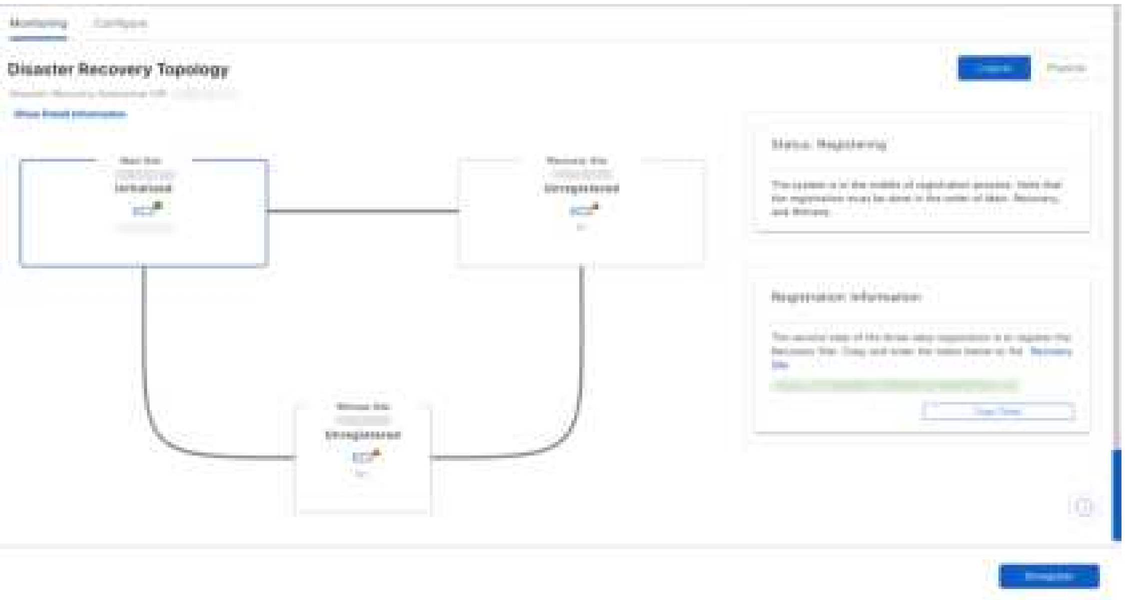
k) From the **Action** area, click **Register**.

The **Disaster Recovery Registration** dialog opens.

l) Click **Continue**.

The token that your recovery and witness sites need to use in order to register with your main site is generated.

Step 3 In the **Registration Information** area, click **Copy Token**.



Main site registration errors

You may encounter errors when registering your system's main site. This topic describes these errors and how to deal with them.

Validation Type	Validation Made	Error Resolution
VIP reachability	Checks whether a TCP socket can be opened on the recovery site's port 443.	Make sure the recovery site's VIP matches the Enterprise VIP configured for the recovery site's Catalyst Center instance and that it's reachable from the main site.
	Checks whether a TCP socket can be opened on the witness site's port 2222.	Make sure the witness site's IP address is configured correctly and reachable from the main site.

Validation Type	Validation Made	Error Resolution
Enterprise and Management interface VIP reachability	Confirms whether the disaster recovery system's VIP can be reached via the Enterprise interface by looking for these items: • A static route defined on the Enterprise interface for the disaster recovery system's VIP • A default gateway configured on the Enterprise interface If neither of these items are present, the validation fails.	Define either a static route on the Enterprise interface for the disaster recovery system's Enterprise VIP or a default gateway on the Enterprise interface.
	Confirms whether the disaster recovery system's VIP can be reached via the Management interface by looking for these items: • A static route defined on the Management interface for the disaster recovery system's VIP • A default gateway configured on the Management interface If neither of these items are present, the validation fails.	Define either a static route on the Management interface for the disaster recovery system's Management VIP or a default gateway on the Management interface.
Certificate upload	Confirms whether a third-party certificate has been uploaded. If so, Catalyst Center also confirms that the certificate is not self-signed.	
	In the **System Certificates** page (**System** > **Settings** > **Certificates** > **System Certificates**), checks that one of these is true: • The **Use System Certificate for Disaster Recovery as well** option is selected. • A certificate that's specific to disaster recovery has been uploaded. In both cases, the certificate must have a nonwildcard DNS name specified as the first entry in its **SAN** field.	

For errors not described above, their cause will be identified in the Status area. Make the necessary corrections and proceed by choosing one of these options from the **Action** area:

- **Retry**: If the cause of the error is fixed or the error was caused by an intermittent issue (such as the restart of a dependent service during the registration process), try this option to continue registration.
- **Deregister**: If you want to change any configuration or start over with the registration, use this option so that you can enter the details and options from the beginning.

Register the recovery site

Complete these steps to register the recovery site.

Note At any point before Step 4, you can click **Reset** to clear all of the settings that you have entered. You will then need to repeat this procedure from the beginning and enter the correct settings before you register the recovery site.

Before you begin

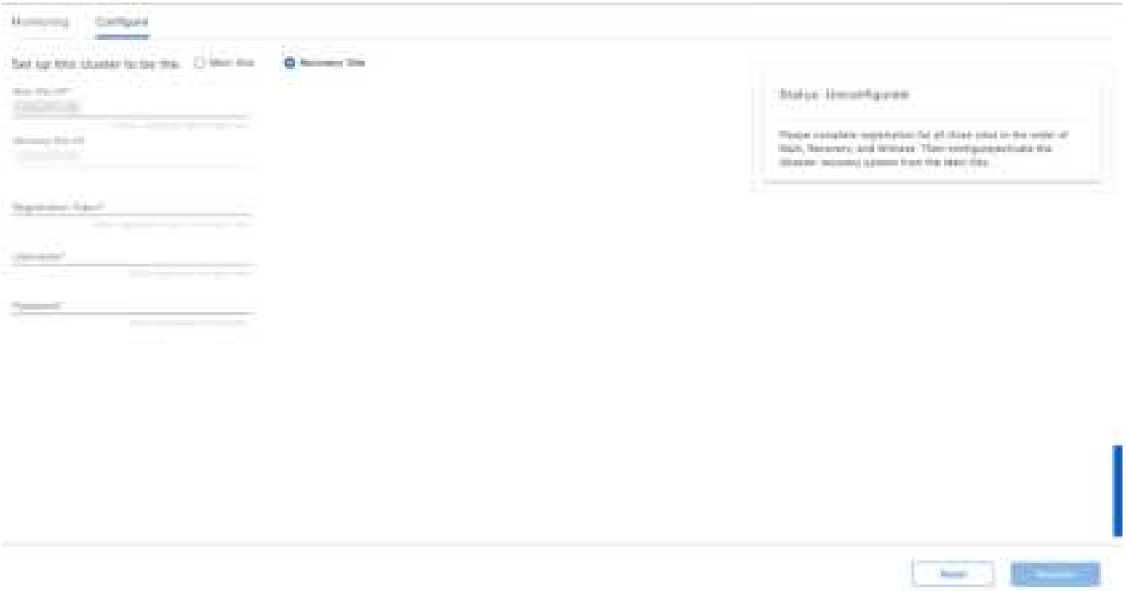
View the Prerequisites, on page 204 topic and ensure that the requirements described in the "Main and Recovery Site Prerequisites" section have been met.

Procedure

Step 1 From the **Registration Information** area, right-click the **Recovery Site** link and open the resulting page in a new browser tab.

Step 2 If necessary, enter the appropriate username and password to log in to your recovery site.

The **Disaster Recovery** page's **Configure** tab opens, with the **Recovery Site** radio button already selected.



Please complete registration for all three sites in the order of Main, Recovery, and Witness. Then configure/activate the disaster recovery system from the Main Site.

Step 3 Enter this information:

- **Main Site VIP**: The virtual IP address that manages traffic between the active site's cluster nodes and your Enterprise network.
- **Recovery Site VIP**: The virtual IP address that manages traffic between the recovery site's cluster nodes and your Enterprise network. Catalyst Center prepopulates this field, based on your system's information.

  Note
  After a IPSec tunnel has been configured between the main and recovery sites, Enterprise traffic on the node(s) hosting the VIP will be sourced via the Enterprise VIP (UDP/TCP/ICMP).

- The registration token that you generated while registering the main site.
- The username and password configured for your active site's super-admin user.

Step 4 From the **Action** area, click **Register**.

The **Disaster Recovery Registration** dialog opens.

Step 5 Click **Continue**.

The topology updates the status for the main and recovery sites after they have been connected.

Register the witness site

Complete these steps to register the witness site.

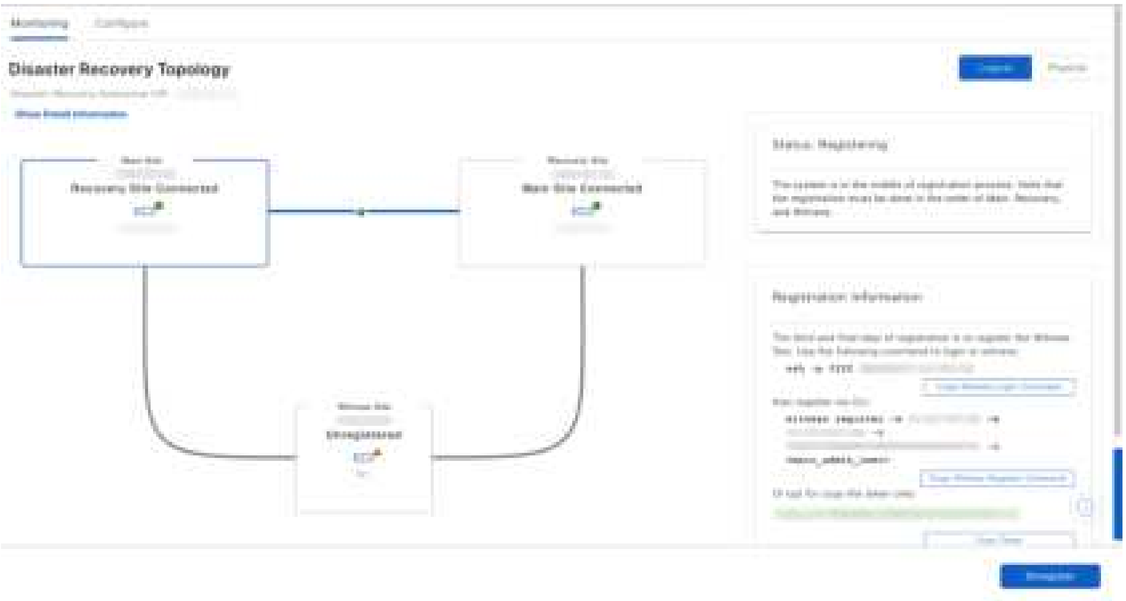
Before you begin

Ensure that these conditions are true before you register your disaster recovery system's witness site:

- The witness site is reachable from both the main and recovery site.
- The VIPs configured for the main and recovery site are reachable from the witness site.

Procedure

Step 1 Return to the main site's browser tab.



Step 2 From the **Registration Information** area, click **Copy Witness Login Command**.

Step 3 Open an SSH console to the witness site, paste the command you just copied, and then run it to log in.

Step 4 When prompted, enter the default (maglev) user's password.

Step 5 Return to the **Registration Information** area and click **Copy Witness Register Command**.

Step 6 In the SSH console, paste the command you just copied.

Step 7 Replace `<main_admin_user>` with the super-admin user's username and then run the command.

Step 8 When prompted, enter the super-admin user's password.

Witness site registration errors

This topic describes errors you may encounter when registering the witness site and how to deal with them.

Error Type	Validation Made	Resolution
IP validation	Validates that the witness site IP address entered during main site registration matches the IP address entered during witness site registration.	Ensure that you enter the same IP address for the witness site when registering the main and witness sites.

Error Type	Validation Made	Resolution
Version validation	Validates that the witness site's OVA package is the correct version for the Catalyst Center version that's installed on your system's main and recovery sites. Each Catalyst Center version supports only one OVA version.	Deploy the witness site OVA package version listed in the error message.

For errors that don't involve validation checks, their cause is identified in the **Status** area. Make the necessary corrections and proceed by doing one of these tasks:

- After logging in to the witness site, run the **witness reset** command.
- To make any registration setting changes or restart the process from the beginning, click **Deregister** from the **Action** area.

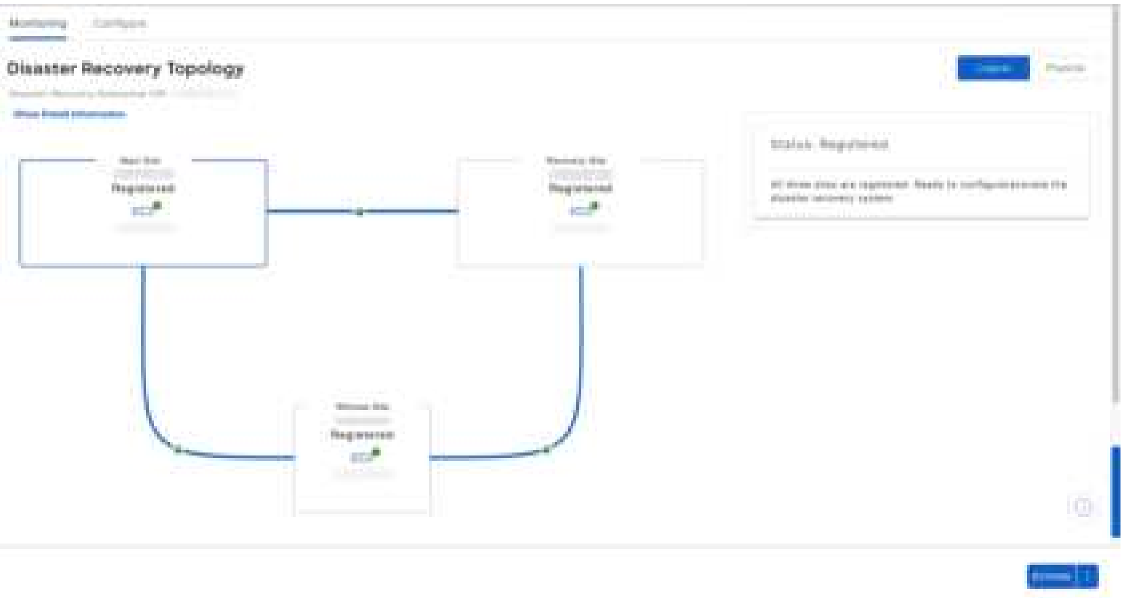
Activate your disaster recovery system

After registering your system's sites, complete this procedure to activate the system for use in your Catalyst Center deployment.

Procedure

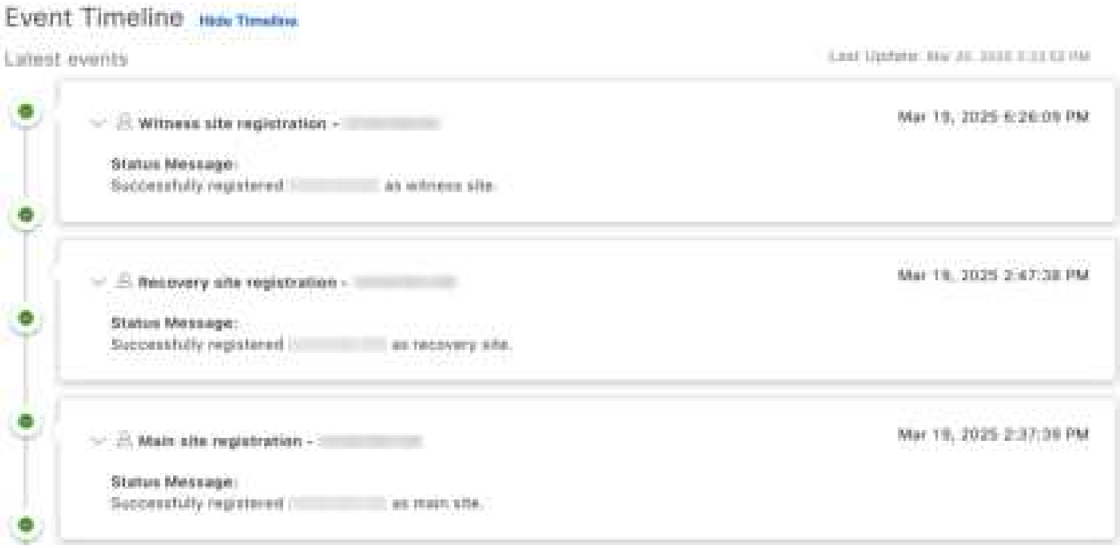
Step 1 Verify that your main, recovery, and witness sites registered successfully:

a) Return to the main site's browser tab and click **Monitoring** to view the Disaster Recovery **Monitoring** tab.



b) In the **Logical Topology** area, confirm that the three sites are displayed and their status is **Registered**.

c) In the **Event Timeline** area, confirm that the registration of each site is listed as an event and that each task completed successfully.



Event Timeline Hide Timeline

Latest events

Last Update: Mar 20, 2025 3:33:52 PM

Witness site registration - [redacted] Mar 19, 2025 6:26:09 PM

Status Message:
Successfully registered [redacted] as witness site.

Recovery site registration - [redacted] Mar 19, 2025 2:47:38 PM

Status Message:
Successfully registered [redacted] as recovery site.

Main site registration - [redacted] Mar 19, 2025 2:37:39 PM

Status Message:
Successfully registered [redacted] as main site.

Step 2 In the **Action** area, click **Activate**.

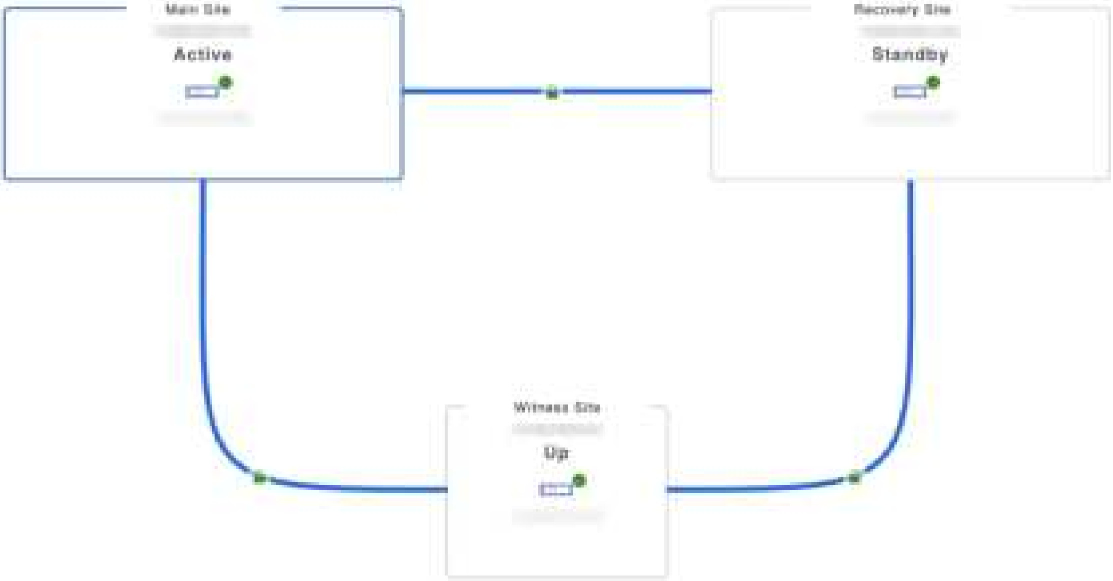
A dialog box opens, indicating that all the data that currently resides in your recovery site will be erased.

Step 3 To begin the configuration of your disaster recovery system and the replication of your main site's data to the recovery site, click **Continue**.

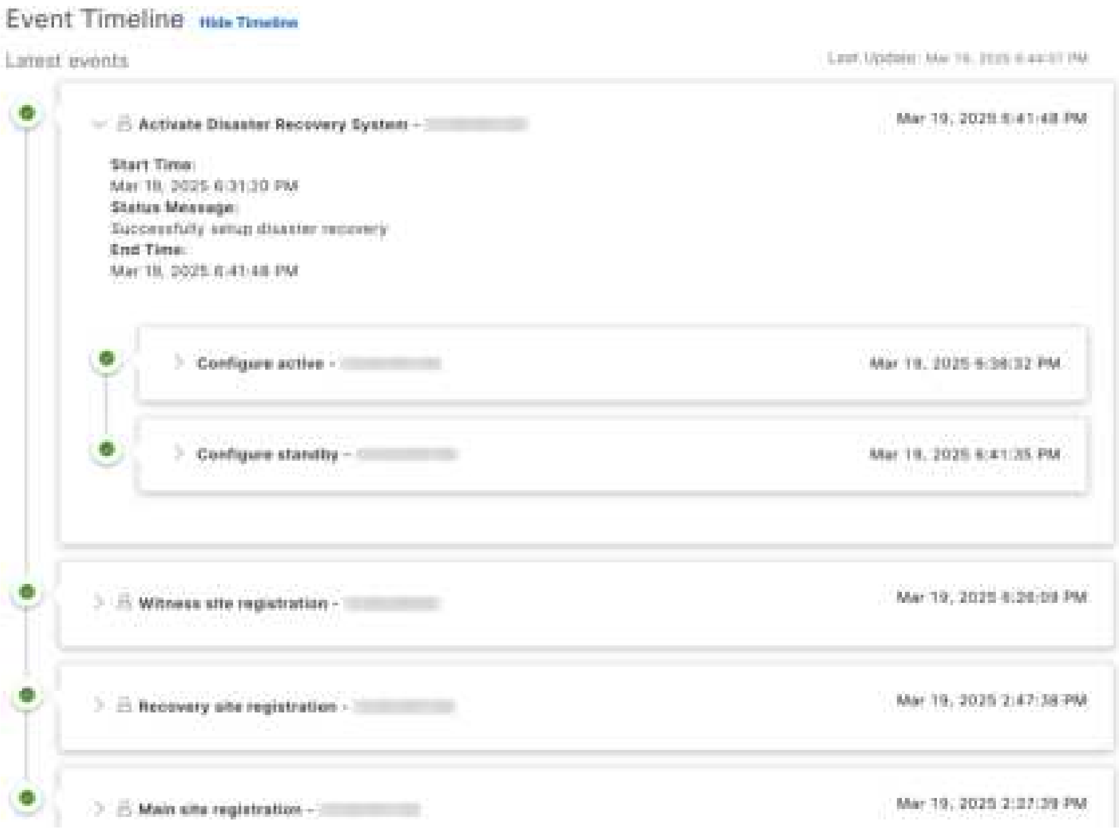
Note
The activation process may take some time to complete. View the Event Timeline in order to monitor its progress.

Step 4 After Catalyst Center has completed the necessary tasks, verify that your system is operational:

a. View its topology and confirm that the following status is displayed for your respective sites:



b. View the Event Timeline and confirm that the **Activate Disaster Recovery System** task completed successfully.



Event Timeline

Latest events Last Update: Mar 19, 2025 6:44:57 PM

Activate Disaster Recovery System - [redacted] Mar 19, 2025 6:41:48 PM

Start Time:
Mar 19, 2025 6:31:30 PM
Status Message:
Successfully setup disaster recovery
End Time:
Mar 19, 2025 6:41:48 PM

Configure active - [redacted] Mar 19, 2025 6:36:32 PM

Configure standby - [redacted] Mar 19, 2025 6:41:35 PM

Witness site registration - [redacted] Mar 19, 2025 6:26:09 PM

Recovery site registration - [redacted] Mar 19, 2025 2:47:38 PM

Main site registration - [redacted] Mar 19, 2025 2:27:39 PM

c. Verify that your sites are reachable by pinging them from the main site.

Disaster recovery system validations

This table describes the validations that the disaster recovery system makes after the **Activate** and **Rejoin** operations have been initiated.

Validation	Description
Package match	Confirms whether the packages installed on both the main and recovery sites are the same version.
Key services health	Checks the health of managed services and other key services that are critical for disaster recovery operations.
IPsec status and transmission	Confirms whether the IPSec tunnel is up for all of the disaster recovery system's sites.
Consul connectivity	Determines if the consul (the distributed database shared by the main, recovery and witness sites) is able to communicate with all of the sites.

Pause your disaster recovery system

By pausing your main and recovery sites, you are effectively breaking up your disaster recovery system. The sites will no longer be connected and instead will act as standalone clusters. You would want to pause your system to temporarily disable the replication of data from the active site to the standby site if you plan to break up your system for an extended period of time. You would also pause the disaster recovery system to do one of these tasks:

- Complete any administrative tasks, such as upgrade the clusters or install additional packages.
- Replace the system or disaster recovery certificate.
- Perform maintenance on the main, recovery, or witness site clusters.
- Prepare for a planned network or power outage.

Place your system on pause

To pause your disaster recovery system temporarily, which you would typically do before performing maintenance on a system component, complete this procedure:

Procedure

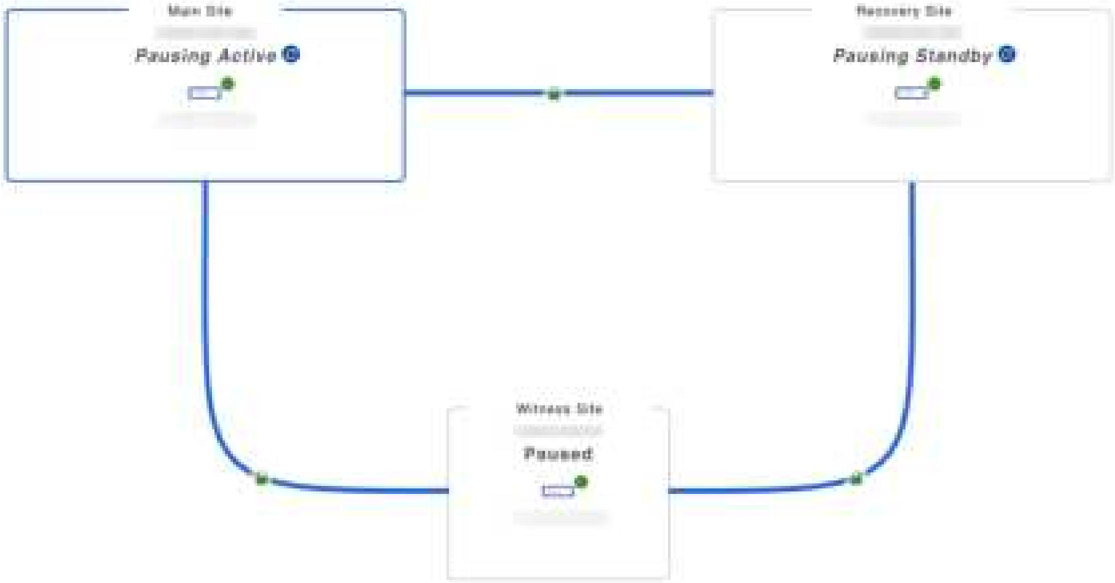
Step 1 From the main menu, choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology.

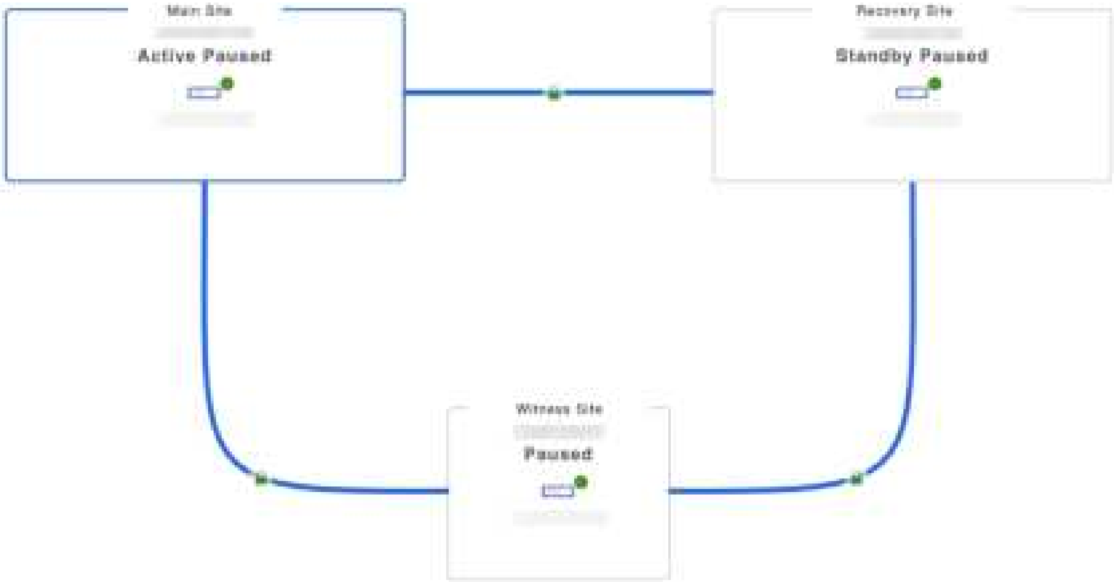
Step 2 In the **Action** area, click ⋮ and then click **Pause**.

Step 3 In the resulting dialog, click **Continue** to proceed.

A message is displayed in the bottom-right corner of the page, indicating that the process to pause your system has started. To pause your system, Catalyst Center disables data and service replication. It also reinstates the services that were suspended on your recovery site. As this is taking place, the status for your main and recovery sites is set to **Pausing** in the topology.



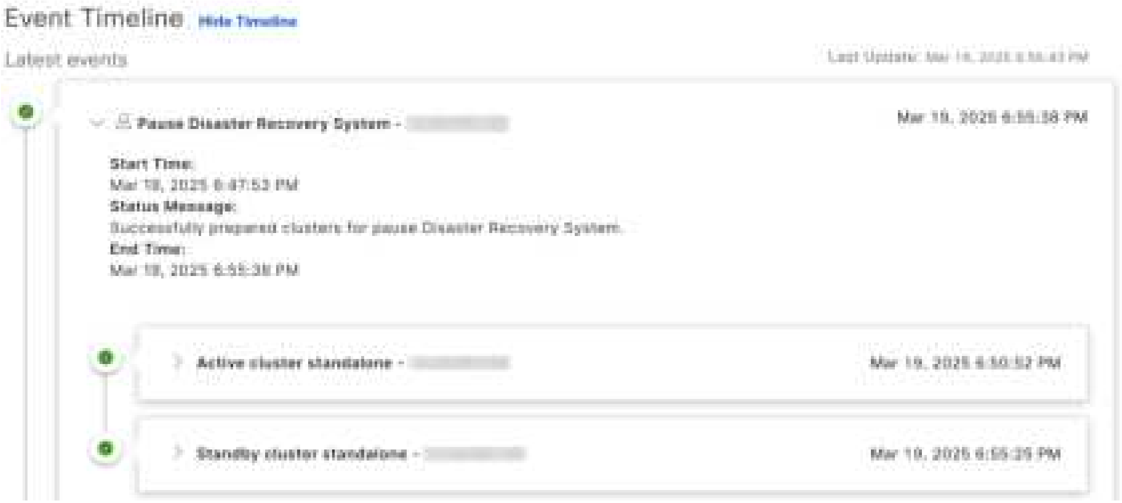
After Catalyst Center completes the necessary tasks, the topology updates and sets the status for your main, recovery, and witness sites as **Paused**.



Step 4 Confirm that your disaster recovery system has been paused:

a. Verify that your system's status is listed as **Paused** in the **Status** area.

b. In the Event Timeline, verify that the **Pause Disaster Recovery System** task completed successfully.



Event Timeline Hide Timeline

Latest events Last Update: Mar 19, 2025 6:56:43 PM

Pause Disaster Recovery System - [redacted] Mar 19, 2025 6:55:38 PM

Start Time:
Mar 19, 2025 6:47:53 PM
Status Message:
Successfully prepared clusters for pause Disaster Recovery System.
End Time:
Mar 19, 2025 6:55:38 PM

Active cluster standalone - [redacted] Mar 19, 2025 6:50:52 PM

Standby cluster standalone - [redacted] Mar 19, 2025 6:55:25 PM

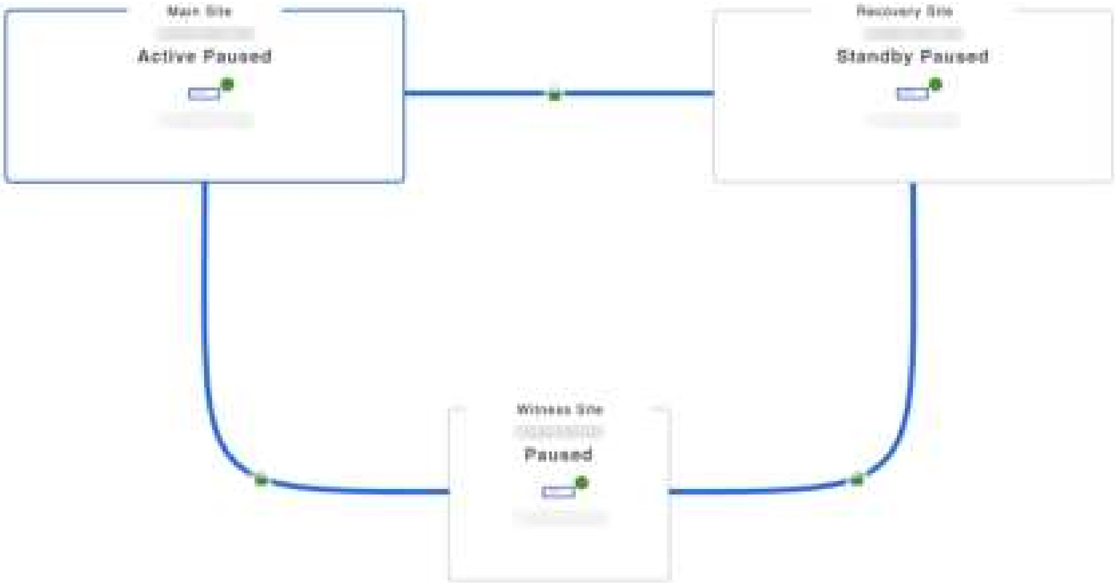
Rejoin your system

Complete this procedure to restart a disaster recovery system that is currently on pause.

Procedure

Step 1 From the main menu, choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default, and displays your disaster recovery system topology.

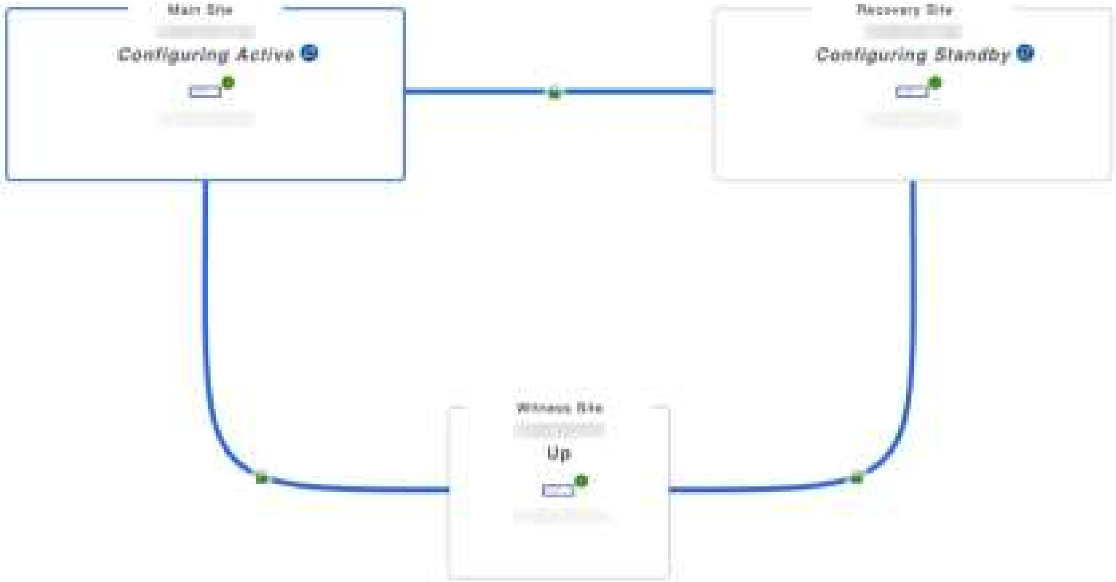


Step 2 In the **Action** area, click **Rejoin**.

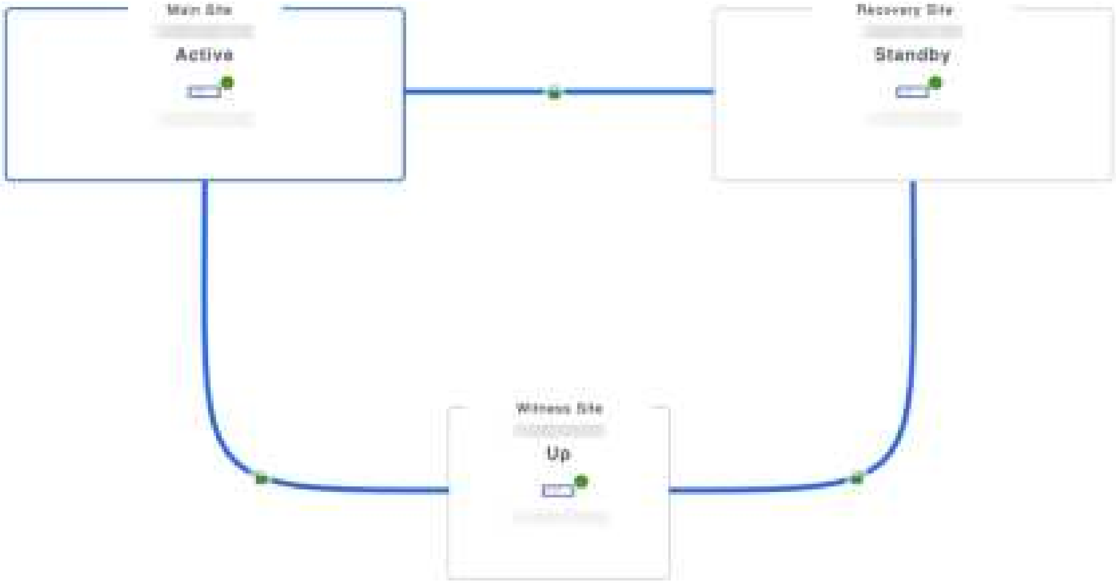
A dialog opens, indicating that all the data on your standby site will be erased.

Step 3 Click **Continue** to proceed.

A message is displayed in the bottom-right corner of the page, indicating that the process to reconnect your main, recovery, and witness sites has started. As this is taking place, the status for your main and recovery sites is set to **Configuring** in the topology.



After Catalyst Center completes the necessary tasks, the topology updates the status for your main, recovery, and witness sites.



Step 4 Confirm that your disaster recovery system is operational again by verifying that its status is listed as **Up and Running** in the **Status** area.

Failovers: an overview

A failover takes place when your disaster recovery system's standby site takes over the responsibilities of the former active site and becomes the new active site. Catalyst Center supports two types of failover:

- System-triggered: Occurs when your system's active site experiences an issue that brings it offline (such as a hardware failure or network outage). When Catalyst Center recognizes that the active site has not been able to communicate with the rest of the Enterprise network (and the standby and witness sites) for seven minutes, it completes the tasks necessary for your standby site to assume its role so that network operations can continue without interruption.
- Manual: Occurs when a super-admin user instructs Catalyst Center to swap the roles that are currently held by your system's active and standby sites. You would typically do this before you update the Catalyst Center software that is installed on a site's appliances or perform routine site maintenance.

After either type of failover has taken place and the former active site has come back online, your disaster recovery system automatically moves the site to the **Standby Ready** state. To establish this site as the new standby site, click **Rejoin** in the **Action** area of the **Monitoring** tab.

Initiate a manual failover

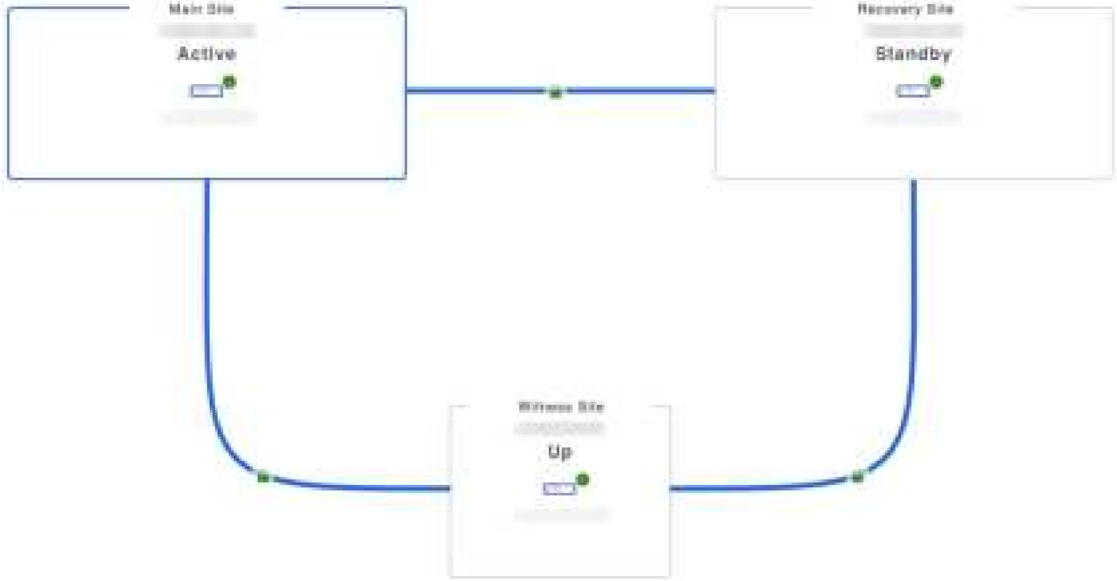
When you manually initiate a failover, you instruct Catalyst Center to swap the roles that are currently assigned to your disaster recovery system's main and recovery site. Manual failover is useful if you know that the current active site is experiencing issues and you want to proactively designate the standby site as the new active site. Complete this procedure to initiate a manual failover.

Note You cannot initiate a manual failover from your witness site. You can only do so from the current active site.

Procedure

Step 1 From the main menu, choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology. In this example, the user is logged in to the current active site.



Step 2 In the **Action** area, click **Manual Failover**.

The **Disaster Recovery Manual Failover** dialog opens, indicating that the standby site will assume the **Active** role.

Step 3 Click **Continue** to proceed.

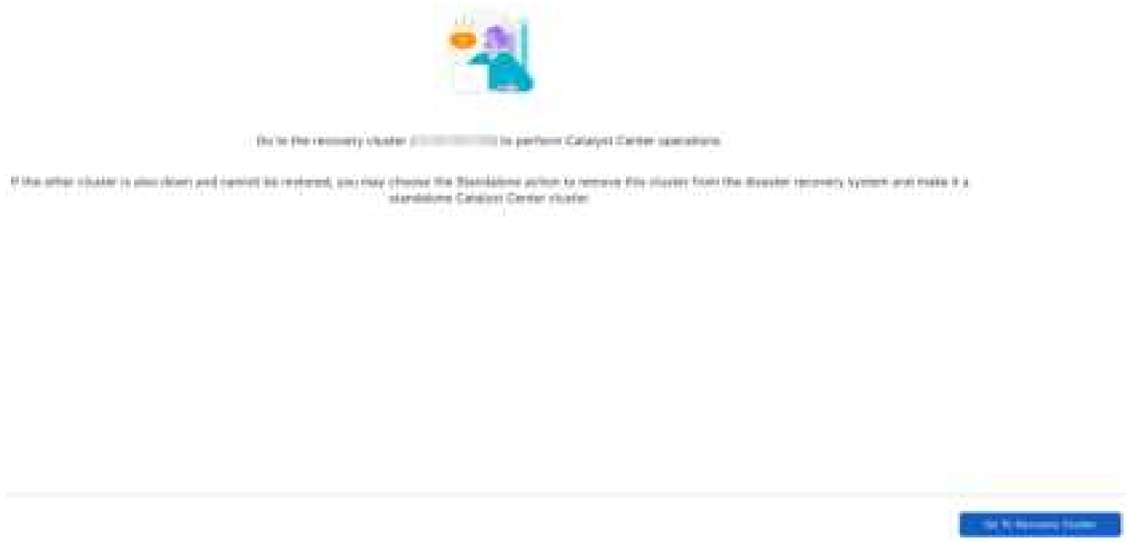
A message is displayed in the bottom-right corner of the page, indicating that the failover process has started. The site previously acting as the active site is isolated from the system.

At this point, the main and recovery sites are not connected and data replication is not taking place. If the former active site is experiencing issues, now is a good time to resolve those issues.

A subsequent failover (initiated by either the system or a user) cannot take place until you add the former active site back to your disaster recovery system.

Step 4 Reconnect the main and recovery sites and reconfigure your disaster recovery system:

a. After the Catalyst Center window updates, click **Go To Recovery Cluster**.

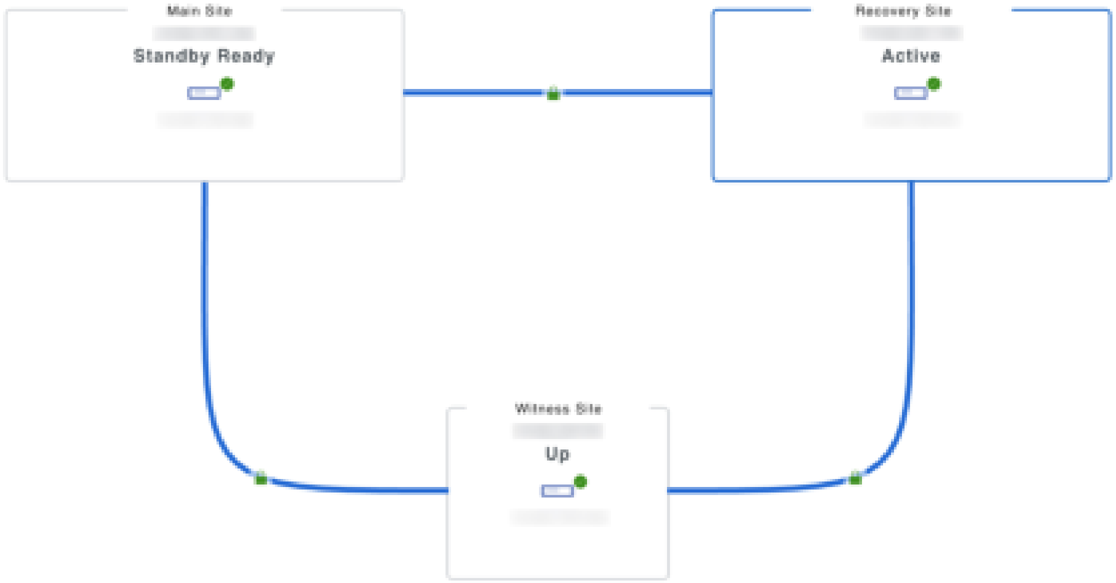


Go to the recovery cluster [redacted] to perform Catalyst Center operations.

If the other cluster is also down and cannot be restored, you may choose the Standalone action to remove this cluster from the disaster recovery system and make it a standalone Catalyst Center cluster.

b. Log in to your recovery site.

The site previously acting as the active site is isolated from the system and enters the **Standby Ready** state.

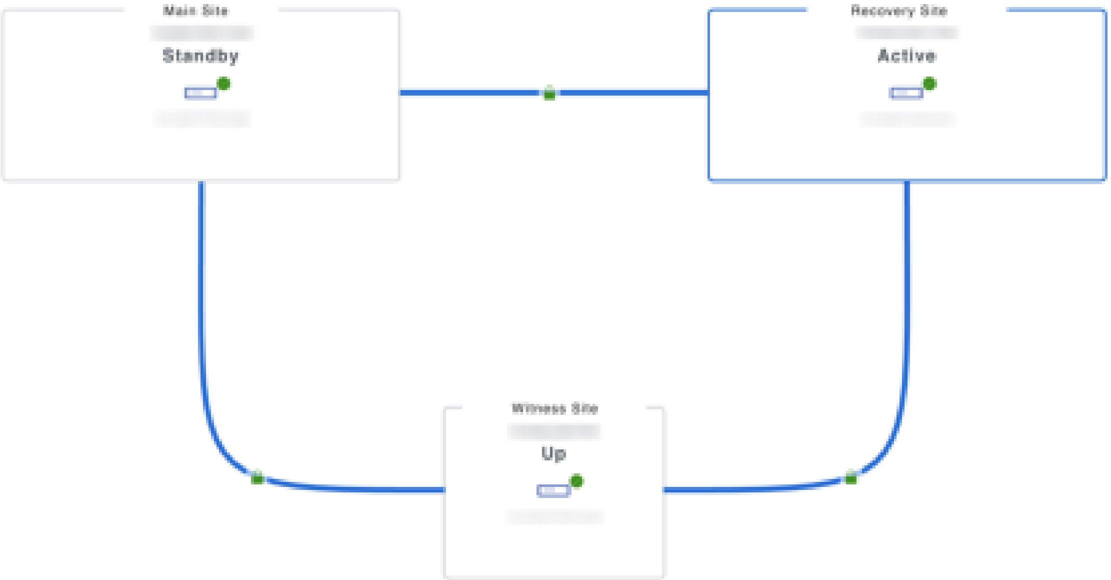


c. In the **Action** area, click **Rejoin**.

A dialog opens, indicating that data on the standby site will be erased.

Step 5 Click **Continue** to proceed and restart data replication.

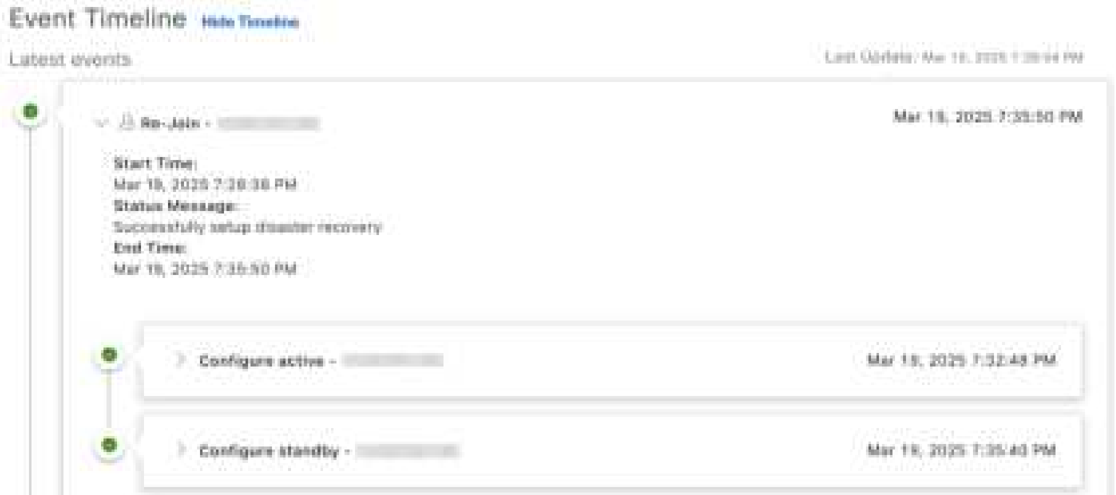
After Catalyst Center completes the relevant workflows, the manual failover completes. The main site, which was currently serving as the active site, is now the standby site.



Step 6 Confirm that your disaster recovery system is operational again:

a. In the top-right corner of the **Monitoring** tab, verify that its status is listed as **Up and Running**.

b. In the Event Timeline, verify that the **Rejoin** task completed successfully.



Event Timeline Hide Timeline

Latest events

Last Update: Mar 19, 2025 7:39:44 PM

Re-Join - Mar 19, 2025 7:35:50 PM

Start Time:
Mar 19, 2025 7:28:38 PM
Status Message:
Successfully setup disaster recovery
End Time:
Mar 19, 2025 7:35:50 PM

Configure active - Mar 19, 2025 7:32:48 PM

Configure standby - Mar 19, 2025 7:35:40 PM

Deregister your system

After your disaster recovery system is activated, you may need to update the settings that you entered for a particular site. If you find yourself in this situation, complete this procedure.

Note When you deregister your system, the settings that are currently set for all the sites in your system will be cleared.

Procedure

Step 1 From the **Action** area, click **Pause** to suspend the operation of your system.

For more information, see Place your system on pause, on page 225.

Step 2 From the **Action** area, click **Deregister**.

Catalyst Center deletes all the settings that you configured previously for your system's sites.

Step 3 Complete the tasks described in Set up disaster recovery, on page 212 to enter the appropriate settings for your sites, reregister them, and reactivate your system.

Disaster recovery system considerations

This section describes things to be aware of when managing your disaster recovery system.

Backup and restore considerations

- A backup can only be scheduled from your system's active site.
- You cannot restore a backup file when disaster recovery is enabled. You must first pause your system temporarily. For more information, see Place your system on pause, on page 225.
- You should only restore a backup file on the site that was the active site prior to pausing your system. After you restore the backup file, you then need to rejoin your system's sites. Doing so will reinstate disaster recovery and initiate the replication of the active site's data to the standby site. For more information, see Rejoin your system, on page 227.
- You can only restore a backup file on cluster nodes that have the same Catalyst Center version installed as the other nodes in your system.
- After a failover takes place, your deployment's backup and restore settings and schedule are not replicated to the new active site. You will need to configure them again.
- If applicable to your deployment, we recommend that you upgrade the TLS version for incoming TLS connections to Catalyst Center. In the Catalyst Center Security Best Practices Guide, see the "Change the Minimum TLS Version and Enable RC4-SHA (Not Secure)" topic. If you have already upgraded your main site, we recommend that you also upgrade your recovery site (ideally before you activate your disaster recovery system or after a failover occurs).

Node or cluster replacement considerations

You cannot do either of these replacements without breaking your disaster recovery system's configuration:

- Replace one of the nodes in a 1+1+1 setup.
- Replace all of one site's nodes in a 3+3+1 setup.

If you need to do so, ensure that you then complete the steps described in Deregister your system, on page 232 to get your system up and running again.

Reconfiguration considerations

- Any data present on the appliances that reside at the recovery site will be deleted in these scenarios:
  - When setting up your disaster recovery system for the first time and you activate the system.
  - When the recovery site is the current active site, you pause your system, deregister it, and then reregister it as the recovery site.
- When you reconfigure an existing disaster recovery system, make sure you know which site is the current active site and register it as your system's main site. Alternatively, you can make a backup of the recovery site's data (if it's currently active) and restore this data on your system's main site prior to the system's reconfiguration.
- These changes cannot be made without reconfiguring your system:
  - Changing the IP addresses and static/default routes configured for your disaster recovery system's Enterprise and Management interfaces.
  - Changing the witness site's IP address.
  - Updating a site's **cluster_hostname** setting.

  Complete the steps described in Deregister your system, on page 232 to configure new IP addresses and routes. If you updated the **cluster_hostname** value, complete these same steps after doing so.

HA considerations

You cannot convert the main and recovery sites from single-node clusters to HA clusters without breaking your disaster recovery system's configuration. If you need to do so:

1. Deregister your system, on page 232.
2. Convert both sites to HA clusters.
3. Reregister and reactivate disaster recovery (see Set up disaster recovery, on page 212).

Site failure considerations

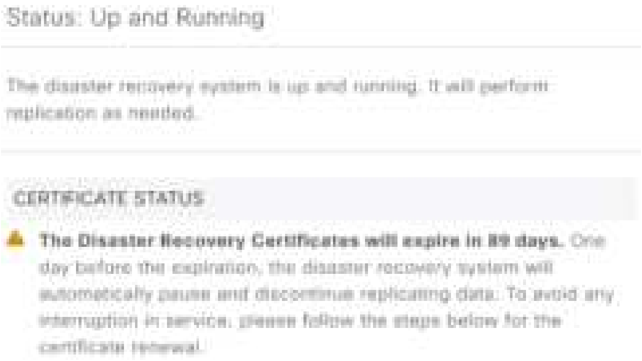
By default, the disaster recovery system waits seven minutes before recognizing that a site has failed and taking one of these actions:

- When the active site goes down, it starts the failover process.
- When either the standby or witness site goes down, the system marks that site as down and disables the ability to start any tasks from the **Action** area.

If you try to initiate a task before the seven minutes have passed, the **Details** area will display a message that indicates why it cannot be completed.

Certificate replacement considerations

The **Status** area indicates when the certificate configured for your disaster recovery system is set to expire. If the certificate will expire within 90 days, a warning message is displayed:



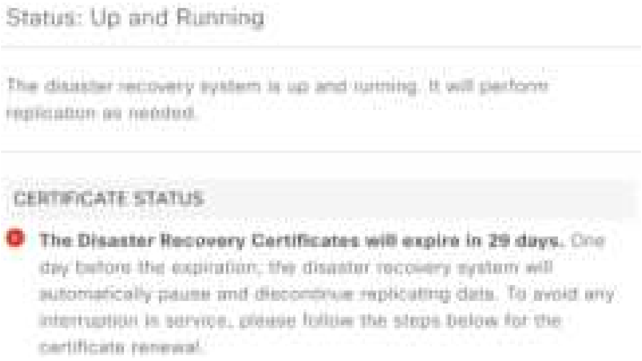
Status: Up and Running

The disaster recovery system is up and running. It will perform replication as needed.

CERTIFICATE STATUS

⚠ **The Disaster Recovery Certificates will expire in 89 days.** One day before the expiration, the disaster recovery system will automatically pause and discontinue replicating data. To avoid any interruption in service, please follow the steps below for the certificate renewal.

If the certificate will expire in 30 days or less, an error message is displayed instead:



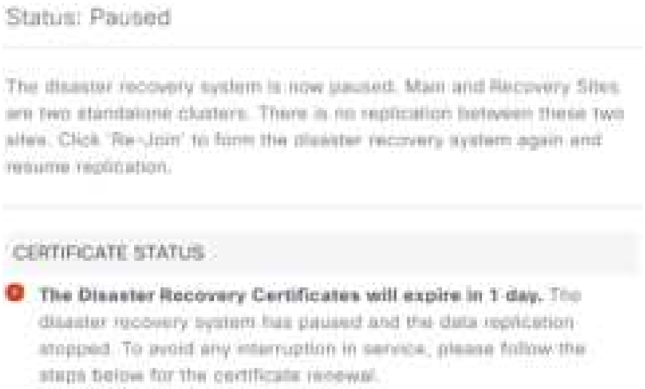
Status: Up and Running

The disaster recovery system is up and running. It will perform replication as needed.

CERTIFICATE STATUS

⛔ **The Disaster Recovery Certificates will expire in 29 days.** One day before the expiration, the disaster recovery system will automatically pause and discontinue replicating data. To avoid any interruption in service, please follow the steps below for the certificate renewal.

If the certificate is set to expire in a day, and the disaster recovery system is operational, Catalyst Center automatically pauses your system:



Status: Paused

The disaster recovery system is now paused. Main and Recovery Sites are two standalone clusters. There is no replication between these two sites. Click 'Re-Join' to form the disaster recovery system again and resume replication.

CERTIFICATE STATUS

The Disaster Recovery Certificates will expire in 1 day. The disaster recovery system has paused and the data replication stopped. To avoid any interruption in service, please follow the steps below for the certificate renewal.

To configure a new certificate and restore the operation of your system, you'll need to do these tasks:

1. Place your disaster recovery system on pause (unless Catalyst Center has already done so).
2. Replace your system's certificate by completing the steps described in the Add the disaster recovery certificate, on page 209 topic.
3. Rejoin your system to restart it.

VLAN mode considerations

- For a description of VLAN mode, see Steps 7 and 8 in the *Cisco Catalyst Center Installation Guide's* "Configure the Primary Node Using the Maglev Wizard" topic.
- VLAN mode:
  - Can only be enabled when you configure a Catalyst Center appliance using the Maglev Configuration wizard.
  - Can't be enabled using any of the browser-based configuration wizards.
  - Can't be disabled without reimaging the appliance.
- These items are not supported by Catalyst Center deployments that have VLAN mode enabled:
  - Catalyst Center in an ACI fabric
  - Disaster recovery

Administer your disaster recovery system

This section describes how to complete the various tasks you may need to carry out while managing your deployment's disaster recovery system.

Replace the current witness site

Complete this procedure to replace your disaster recovery system's current witness site with a new site.

Procedure

Step 1 Log in to the current witness site:

a) Open an SSH console to the witness site and run the **ssh -p 2222 maglev@***witness-site's-IP-address* command.

b) Enter the default (maglev) user's password.

Note
Before you proceed to the next step, note the witness site's IP address. You'll need to configure the same address after you replace the witness site. Otherwise, the witness site won't work as expected.

Step 2 Run the **witness reset** command.

Step 3 Delete the current witness site's virtual machine.

Step 4 Install the new witness site's virtual machine, as described in Install the witness site, on page 210.

Step 5 Log in to the new witness site:

a) Open an SSH console to the witness site and run the **ssh -p 2222 maglev@***witness-site's-IP-address* command.

b) Enter the default (maglev) user's password.

Step 6 Run the **witness reconnect -w *witness-site's-IP-address* -m *main-site's-Enterprise-virtual-IP-address* -u *admin-username*** command.

Note these points:

- Regardless of the main site's current disaster recovery status, use the main site's Enterprise VIP when reconnecting the witness site.
- To verify that the witness site is operational after running this command:

  a. From the Disaster Recovery Topology, click the **Show Detail Information** link to open the **Disaster Recovery System** slide-in pane.

  b. In the **Witness Site** section, confirm that the status for the witness site and configured IPSec links is `Up`.
- To view all of the available options for this command, run the **witness reconnect --help** command.

Monitor the event timeline

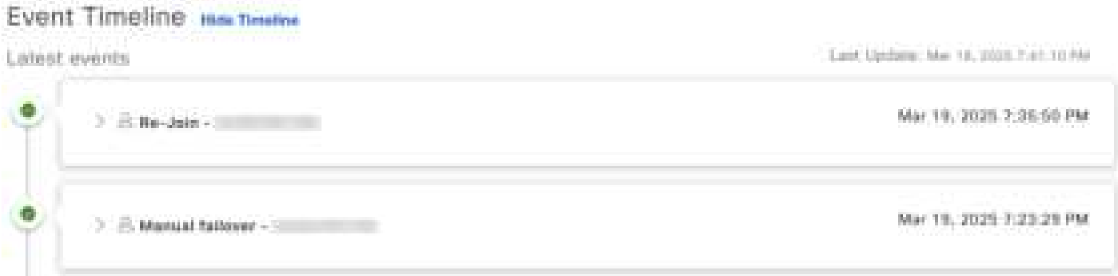
From the event timeline, you can track the progress of disaster recovery tasks that are currently running and confirm when these tasks have completed. To view the timeline:

1. From the main menu, choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

   The **Monitoring** tab is selected, by default.

2. Scroll to the bottom of the page.

Every task that is in progress or has completed for your system is listed here (in descending order based on their completion timestamp), starting with the most recent task. Catalyst Center indicates whether each task was initiated by the system (🖥) or a user (👤).



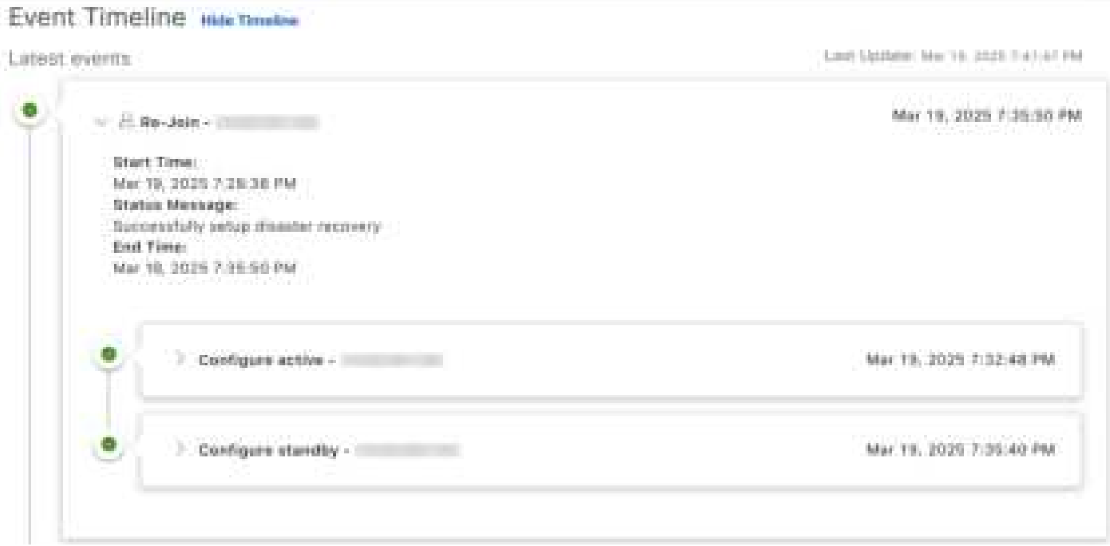
Event Timeline Hide Timeline

Latest events Last Update: Mar 19, 2025 7:41:10 PM

> Re-Join - [redacted] Mar 19, 2025 7:35:50 PM

> Manual failover - [redacted] Mar 19, 2025 7:23:29 PM

Say you want to monitor the restoration of your system after it was paused. Catalyst Center updates the Event Timeline as each task in the restoration process is started and then completed. To view a summary of what took place during a particular task, click **>**.



Event Timeline Hide Timeline

Latest events Last Update: Mar 19, 2025 7:41:47 PM

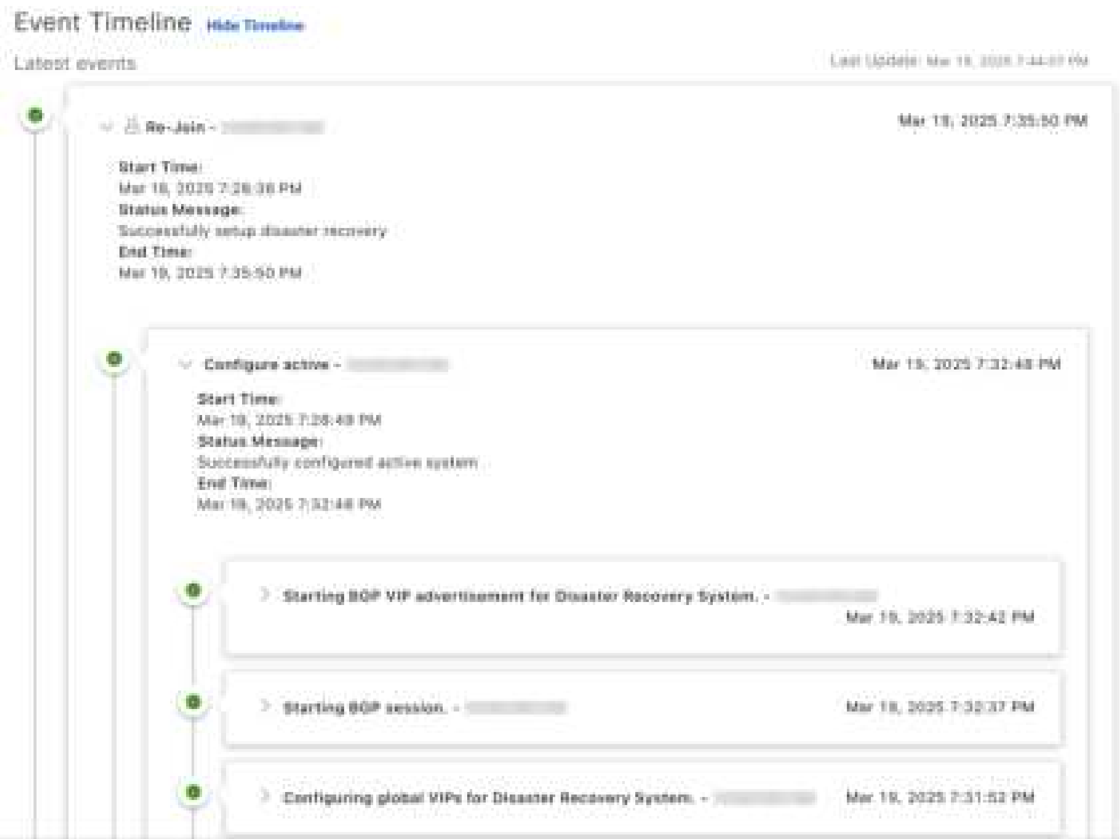
Re-Join - [redacted] Mar 19, 2025 7:35:50 PM

Start Time:
Mar 19, 2025 7:28:38 PM
Status Message:
Successfully setup disaster recovery
End Time:
Mar 19, 2025 7:35:50 PM

> Configure active - [redacted] Mar 19, 2025 7:32:48 PM

> Configure standby - [redacted] Mar 19, 2025 7:35:40 PM

Catalyst Center lists the relevant subtasks that were completed.



Event Timeline

Latest events

Last Update: Mar 19, 2025 7:44:07 PM

Re-Join - [redacted] Mar 19, 2025 7:35:50 PM

Start Time:
Mar 19, 2025 7:28:38 PM
Status Message:
Successfully setup disaster recovery
End Time:
Mar 19, 2025 7:35:50 PM

Configure active - [redacted] Mar 19, 2025 7:32:48 PM

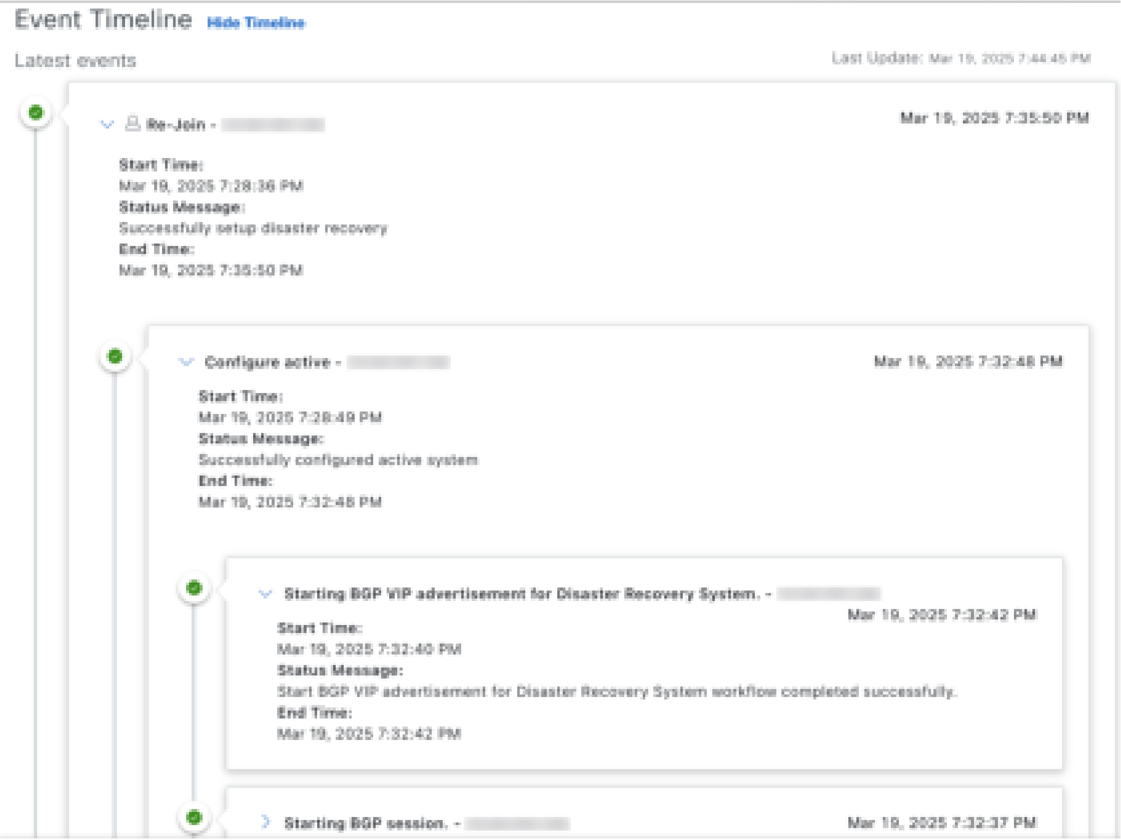
Start Time:
Mar 19, 2025 7:28:49 PM
Status Message:
Successfully configured active system
End Time:
Mar 19, 2025 7:32:48 PM

Starting BGP VIP advertisement for Disaster Recovery System. - [redacted] Mar 19, 2025 7:32:42 PM

Starting BGP session. - [redacted] Mar 19, 2025 7:32:37 PM

Configuring global VIPs for Disaster Recovery System. - [redacted] Mar 19, 2025 7:31:52 PM

As with tasks, you can click **>** to view summary information for a particular subtask.



Event Timeline Hide Timeline

Latest events Last Update: Mar 19, 2025 7:44:45 PM

Re-Join - [redacted] Mar 19, 2025 7:35:50 PM

Start Time:
Mar 19, 2025 7:28:36 PM
Status Message:
Successfully setup disaster recovery
End Time:
Mar 19, 2025 7:35:50 PM

Configure active - [redacted] Mar 19, 2025 7:32:48 PM

Start Time:
Mar 19, 2025 7:28:49 PM
Status Message:
Successfully configured active system
End Time:
Mar 19, 2025 7:32:48 PM

Starting BGP VIP advertisement for Disaster Recovery System. - [redacted] Mar 19, 2025 7:32:42 PM

Start Time:
Mar 19, 2025 7:32:40 PM
Status Message:
Start BGP VIP advertisement for Disaster Recovery System workflow completed successfully.
End Time:
Mar 19, 2025 7:32:42 PM

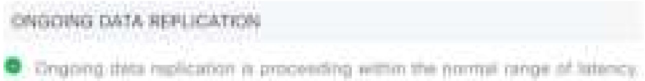
Starting BGP session. - [redacted] Mar 19, 2025 7:32:37 PM

See Troubleshoot your disaster recovery system, on page 246 for a description of the issues that you may encounter while monitoring the event timeline and how to remedy them.

Monitor managed services replication

After you activate your disaster recovery system, Catalyst Center begins monitoring the data replication status of the GlusterFS, MongoDB, and Postgres services. Whenever the replication of these services is taking place, the **Status** area displays one of these four messages:

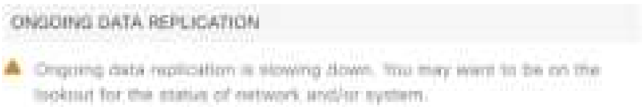
- Replication is completing as expected.

  ONGOING DATA REPLICATION

  ● Ongoing data replication is proceeding within the normal range of latency.

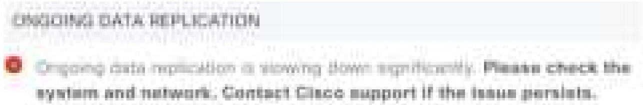
- Replication is completing, but the data sync lag between your system's main and recovery site is currently 20 minutes or more.

  ONGOING DATA REPLICATION

  ⚠ Ongoing data replication is slowing down. You may want to be on the lookout for the status of network and/or system.

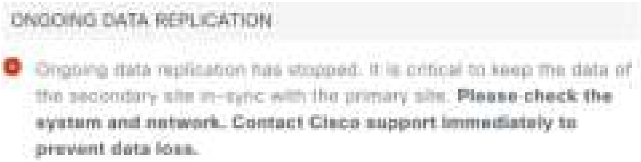
- Replication is completing, but the data sync lag between your system's main and recovery site is 30 minutes or more.



ONGOING DATA REPLICATION

Ongoing data replication is slowing down significantly. **Please check the system and network. Contact Cisco support if the issue persists.**

- Replication has stopped.



ONGOING DATA REPLICATION

Ongoing data replication has stopped. It is critical to keep the data of the secondary site in-sync with the primary site. **Please check the system and network. Contact Cisco support immediately to prevent data loss.**

These messages allow you to keep tabs on the replication of managed services, pointing out when network or system issues are impacting the sync of these services' data between your system's sites.

System and site states

In the disaster recovery GUI, the **Status** area indicates the current state of your system. This tables explain the various states that you may see for the individual sites in your system Topology.

Table 14: Active site states

State	Description
Unregistered	Newly installed site. Disaster recovery information is not available yet.
Initializing	The site is preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Initialized	The site has successfully prepared the data that it will transmit to the other sites in order to set up the disaster recovery cluster during the registration process.
Failed to Initialize	The site encountered an error while preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Connecting Recovery	The main site is contacting the recovery site to retrieve the initialized data required to set up secure communication with the main site.
Connecting Witness	The main site is contacting the witness site to retrieve the initialized data required to set up secure communication with the main site.
Recovery Site Connected	The main site successfully established secure communication with the recovery site.
Failed to Connect Recovery	The main site encountered an error while establishing a secure channel with the recovery site.
Failed to Connect Witness	The main site encountered an error while establishing a secure channel with the witness site.
Registered	The active site successfully established secure communication with the other two sites.
Deregistering	Removing the current disaster recovery configuration from the system.
Deregister Failed	An error occurred while removing the current disaster recovery configuration from the system.
Validating	Validating the state of the system before starting the disaster recovery configuration.

State	Description
Validated	Successfully validated the state of the system before starting the disaster recovery configuration.
Validation Failed	An error occurred while validating the state of the system before starting the disaster recovery configuration.
Configuring Active	Executing the workflows to establish this site as the active site.
Failed to Configure	An error occurred while running the workflows to enable disaster recovery on this site.
Syncing Config Data	Syncing the data required from the other sites to set up the disaster recovery system.
Config Data Synced	Successfully synced the data required from the other sites to set up the disaster recovery system.
Active Sync Failed	An error occurred while the pending active site was syncing the data required from the other sites to set up the disaster recovery system.
Waiting Standby Configuration	Successfully completed the workflows to establish this site as the active site; waiting for the standby site's workflows to complete.
Active	The site is successfully managing the network as the active site.
Failed to Configure	The site failed to execute some of the workflows that would enable itself as the active site in the disaster recovery cluster.
Isolating	The site is executing the workflows to isolate itself because it either lost connectivity with the other two sites or is preparing to become standby-ready (as part of a manual failover).
Isolated	The site has successfully executed the workflows to isolate itself because it either lost connectivity with the other two sites or is preparing to become standby-ready (as part of a manual failover).
Failed to Isolate	The site encountered an error while executing the workflows to isolate itself because it either lost connectivity with the other two sites or is preparing to become standby-ready (as part of a manual failover).
Configuring Active	Configuring a previous standby site as the active site (as part of a system-triggered or manual failover).
Failed during Failover	An error occurred while executing the workflows to establish this site as the active site (as part of a failover or recovery from a two-system failure).
Pausing Active	Executing the workflows that disable disaster recovery operations on the active site (in order to prepare for an administrative operation or a planned outage).
Active Paused	Successfully disabled disaster recovery operations on the active site.
Failed to Pause Active	An error occurred while disabling disaster recovery operations on the active site.
Active Stand Alone	Executing the workflows to establish a previous active site that lost connectivity with the other two sites as an independent system by removing all disaster recovery configurations.
Down	The active site has lost connectivity with the other two sites.

Table 15: Standby site states

State	Description
Unregistered	Newly installed site. Disaster recovery information is not available yet.
Initializing	The site is preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Initialized	The site has successfully prepared the data that it will transmit to the other sites in order to set up the disaster recovery cluster during the registration process.
Failed to Initialize	The site encountered an error while preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Connecting Main	The recovery site is contacting the main site to retrieve the initialized data required to set up secure communication with the main site.
Connecting Witness	The recovery site is contacting the witness site to retrieve the initialized data required to set up secure communication with the main site.
Main Site Connected	The recovery site successfully established secure communication with the main site.
Failed to Connect Main	The recovery site encountered an error while establishing a secure channel with the main site.
Failed to Connect Witness	The recovery site encountered an error while establishing a secure channel with the witness site.
Registered	The standby site successfully established secure communication with the other two sites.
Deregistering	Removing the current disaster recovery configuration from the system.
Deregister Failed	An error occurred while removing the current disaster recovery configuration from the system.
Validating	Validating the state of the system before starting the disaster recovery configuration.
Validated	Successfully validated the state of the system before starting the disaster recovery configuration.
Validation Failed	An error occurred while validating the state of the system before starting the disaster recovery configuration.
Configuring Standby	Executing the workflows to establish this site as the standby site.
Failed to Configure	An error occurred while running the workflows to enable disaster recovery on this site.
Syncing Config Data	Syncing the data required from the other sites to set up the disaster recovery system.
Config Data Synced	Successfully synced the data required from the other sites to set up the disaster recovery system.
Standby Sync Failed	An error occurred while the pending standby site was syncing the data required from the other sites to set up the disaster recovery system.
Waiting Active Configuration	Successfully completed the workflows to establish this site as the standby site; waiting for the active site's workflows to complete.
Standby	The site is successfully configured as the standby site in the disaster recovery cluster.

State	Description
Failed to Configure	The site failed to execute some of the workflows that would enable itself as the standby site in the disaster recovery cluster.
Isolating	The site is executing the workflows to isolate itself because it lost connectivity with the other two sites.
Isolated	The site has successfully executed the workflows to isolate itself because it lost connectivity with the other two sites.
Failed to Isolate	The site encountered an error while executing the workflows to isolate itself because it lost connectivity with the other two sites.
Configuring Standby	Configuring a previous active site as the standby-ready site (as part of a manual failover).
Standby Ready	A previous active system is ready to be configured as a standby system (as a result of a failover).
Pausing Standby	Executing the workflows that disable disaster recovery operations on the standby site (in order to prepare for an administrative operation or a planned outage).
Standby Paused	Successfully disabled disaster recovery operations on the standby site.
Failed to Pause Standby	An error occurred while disabling disaster recovery operations on the standby site.
Standby Stand Alone	Executing the workflows to establish a previous standby site that lost connectivity with the other two sites as an independent system by removing all disaster recovery configurations.
Down	The site has lost connectivity with the other two sites.

Table 16: Witness site states

State	Description
Unregistered	Newly installed site. Disaster recovery information is not available yet.
Registered	This site has been designated as the witness site and the validation checks have completed successfully.
Up	Configuration of the witness site has completed successfully.
Down	The site has lost connectivity with the other two sites.

Disaster recovery event notifications

You can configure Catalyst Center to send a notification whenever a disaster recovery event takes place. See the "Work with Event Notifications" topic in the *Cisco Catalyst Center Platform User Guide* for a description of how to configure and subscribe to these notifications. When completing this procedure, ensure that you select and subscribe to the SYSTEM-DISASTER-RECOVERY-v2 event in the **Platform** > **Developer Toolkit** > **Events** table.

Important Disaster recovery supports IPsec up/down notifications on a best-effort basis. When network disruptions prevent writing to the distributed store, some up/down notifications may be dropped. Event notifications resume after network communication is restored.

After you subscribe, Catalyst Center sends a notification indicating that the IPsec session is down because the system's certificate has expired. To update this certificate:

1. Place your system on pause, on page 225.
2. On both your main and recovery site, replace the current system certificate. From the main menu, choose **System** > **Settings** > **Certificates** > **System Certificates**.
3. Rejoin your system, on page 227.

Supported events

This table lists the disaster recovery events that Catalyst Center generates notifications for when they take place.

System health status	Event	Notification
OK	The disaster recovery system is operational.	`Activate DR (Disaster Recovery Setup Successful)`
OK	Failover to either the main or recovery site has completed successfully.	`Failover Successful`
OK	Registration of the main site has completed successfully.	`Successfully Registered Main Site`
OK	Registration of the recovery site has completed successfully.	`Successfully Registered Recovery Site`
OK	Registration of the witness site has completed successfully.	`Successfully Registered Witness Site`
OK	The disaster recovery system has been paused successfully.	`DR Pause Success`
OK	The standby site is operational.	`Standby Site Up`
OK	The witness site is operational.	`Witness Site Up`
OK	The disaster recovery system has been unregistered successfully.	`Unregister Success`
Degraded	Failover to either the main or recovery site has failed.	`Failover Failed`
Degraded	Automated failover is not available because the standby site is currently down.	`Standby Cluster Down`
Degraded	Automated failover is not available because the witness site is currently down.	`Witness Cluster Down`
Degraded	Unable to place the disaster recovery system on pause.	`Pause Failure`

System health status	Event	Notification
Degraded	BGP route advertisement failed.	`BGP Failure`
Degraded	The IPsec tunnel connecting your system's sites is operational.	`IPsec Up`
Degraded	The IPsec tunnel connecting your system's sites is currently down.	`IPsec Down`
NotOk	Disaster recovery system configuration failed.	`Activate DR Failure`
NotOk	The site that is currently in the **Standby Ready** state is unable to rejoin the disaster recovery system.	`Activate DR Failure`
NotOk	Unregistration of the disaster recovery system failed.	`Unregistration Failed`
NotOk	Registration of the main site failed.	`Main Registration Failed`
NotOk	Registration of the recovery site failed.	`Recovery Registration Failed`
NotOk	Registration of the witness site failed.	`Witness Registration Failed`

Troubleshoot your disaster recovery system

The following table describes the issues that your disaster recovery system may present and how to deal with them.

Note If a disaster recovery operation fails or times out, click **Retry** to do the operation again. If the problem persists and its solution is not provided in this table, contact Cisco TAC for assistance.

Table 17: Disaster recovery system issues

Error Code	Message	Solution
SODR10007	`Token does not match.`	The token provided during recovery site registration does not match the token generated during main site registration. From the main site's **Disaster Recovery** > **Configuration** tab, click **Copy Token** to ensure that you copy the correct token.
SODR10048	`Packages (`*`package names`*`) are mandatory and not installed on the main site.`	Install the listed packages before registering the system.
SODR10056	`Invalid credentials.`	Confirm that you entered the correct credentials for the main site during recovery and witness site registration.
SODR10062	`() site is trying to () with invalid IP address. Expected is (); actual is ().`	The main site IP address provided during recovery and witness site registration is different from the IP address that was provided during main site registration.

Error Code	Message	Solution
SODR10067	`Unable to connect to (`*recovery or witness site*`).`	Verify that the main site is up.
SODR10072	`All the nodes are not up for (`*main or recovery site*`).`	Check whether all three of the site's nodes are up.
SODR10076	`High availability should be enabled on (`*main or recovery*`) site cluster.`	Enable high availability (HA): **1.** Log in to the site you need to enable HA on. **2.** From the main menu, choose **System** > **Settings** > **System Configuration** > **High Availability**. **3.** Click **Activate High Availability**.
SODR10100	`(`*Main or recovery*`) site has no third party certificate.`	Replace the default certificate that Catalyst Center is currently using with a third-party certificate. See Update the Catalyst Center server certificate, on page 93 for more information.
SODR10113	`Save cluster metadata failed.`	Contact Cisco TAC for help with completing the appropriate recovery procedure.
SODR10118	`Appliance mismatch between main () and recovery ().`	Different appliances are used by the main and recovery sites. To successfully register disaster recovery, both sites must use the same 56 or 112 core appliance.
SODR10121	`Failed to advertise BGP. Reason: ().`	See Troubleshoot BGP route advertisement issues, on page 253 for more information.
SODR10122	`Failed to stop BGP advertisement. Reason: ().`	See Troubleshoot BGP route advertisement issues, on page 253 for more information.
SODR10123	`Failed to establish secure connection between main () and ()().`	No solution is available for this issue. Contact Cisco TAC for assistance.
SODR10124	`Cannot ping VIP: (`*main, recovery, or witness site's VIP or IP address*`).`	Do the following: • Verify that the address specified is correct. • Check whether the address is reachable from the other addresses.
SODR10129	`Unable to reach main site. ()`	Check whether the Enterprise virtual IP address configured for the main site is reachable from the recovery and witness sites.
SODR10132	`Unable to check IP addresses are on the same interface. Retry the operation. ()`	Retry the operation you just attempted.

Error Code	Message	Solution
SODR10133	`The disaster recovery enterprise VIP () and the IP addresses () are not configured or reachable via the same interface. Check the gateway or static routes configuration.`	Communication between a disaster recovery system's sites relies on the Enterprise network. The main and recovery site's Enterprise virtual IP address, and the witness site's IP address, need to be reachable via the Enterprise interface. This error indicates that the IP address/virtual IP address configured for one or multiple sites uses an interface other than the Enterprise interface for communication.
SODR10134	`The disaster recovery management VIP (`*`VIP address`*`) and the IPs (`*`IP addresses`*`) are configured/reachable via same interface. It should be configured/reachable via management interface. Check the gateway or static routes' configuration.`	The disaster recovery system's Management virtual IP address needs to be configured on the Management interface. This error indicates that the virtual IP address is currently configured on an interface where the Management cluster's virtual IP address has not been configured. Add a /32 static route to the Management virtual IP address that's configured on the Management interface.
SODR10136	`Certificates required to establish IPsec session not found.`	From the **System Certificate** page (**System** > **Settings** > **Certificates** > **System Certificates**), try uploading the third-party certificate again and then retry registration. If the problem persists, contact Cisco TAC for assistance.
SODR10138	`Self-signed certificate is not allowed. Upload a third-party certificate and retry.`	—
SODR10139	`Disaster recovery requires first non-wildcard DNS name to be same in main and recovery. {} in {} site certificate is not same as {} in {} site certificate.`	The third-party certificate installed on your main and recovery sites has different DNS names specified for your disaster recovery system. Generate a third-party certificate that specifies a DNS name for your system and upload this certificate to both sites. **Note** Ensure that the DNS name does *not* use a wildcard.
SODR10140	`Disaster recovery requires at least one non-wildcard DNS name. No DNS name found in certificate.`	The third-party certificate installed on your main and recovery sites does not specify a DNS name for your disaster recovery system. Catalyst Center uses this name to configure the IPsec tunnel that connects your system's sites. Generate a third-party certificate that specifies a DNS name for your system and upload this certificate to both sites. **Note** Ensure that the DNS name does *not* use a wildcard.
—	—	When all three of your system's sites are not connected due to network partitioning or another condition, Catalyst Center sets the status of the sites to **Isolated**. Contact Cisco TAC for help with completing the appropriate recovery procedure.

Error Code	Message	Solution
—	`External postgres services does not exists to check service endpoints.`	Do the following: 1. Log in to the site that the error occurred on. 2. Run the following commands: • **Kubectl get sep -A** • **kubectl get svc -A | grep external** 3. In the resulting output, search for `external-postgres`. 4. If present, run the following command: **kubectl delete sep external-postgres -n fusion** 5. Retry the operation that failed previously.
—	`Success with errors.`	If you see this message after initiating a failover or pausing your disaster recovery system, it indicates that the operation completed successfully even though one or multiple services encountered minor errors. You can go ahead and click **Rejoin** to restart your system. These errors will be resolved after you do so.
—	`Failed.`	This message indicates that a disaster recovery operation failed because one or multiple services encountered a critical error. To troubleshoot the failure, we recommend that you view the Event Timeline and drill down to the relevant error. When you see this message, click **Retry** to perform the operation again.
—	`Cannot ping VIP: (`*`VIP address`*`).`	Verify that the Enterprise VIP address configured for your system is reachable.
—	`VIP drop-down list is empty.`	Confirm that your system's VIP addresses and intracluster link are configured properly.
—	`Cannot perform (`*`disaster recovery operation`*`) due to ongoing workflow: BACKUP. Please try again at a later time.`	A disaster recovery operation was triggered while a scheduled backup was running. Retry the operation after the backup finishes.

Error Code	Message	Solution
—	`The GUI indicates that the standby site is still down after it has come back online.`	If the standby site goes down and Catalyst Center's first attempt to isolate it from your disaster recovery system fails, it may not automatically initiate a second attempt. When this happens, the GUI will indicate that the site is down, even if it is operational again. In addition, you will not be able to restart your system as the standby site is stuck in maintenance mode. To restore the standby site, do the following: **1.** In an SSH client, log in to the standby site. **2.** Run the **maglev maintenance disable** command to take the site out of maintenance mode. **3.** Log in to Catalyst Center. **4.** From the main menu, choose **System** > **Disaster Recovery**. The **Monitoring** tab is selected by default. **5.** In the **Action** area, click **Rejoin** in order to restart your disaster recovery system.
—	`Multiple services exists for MongoDB to check node-port label.`	For debugging, the MongoDB node port is exposed as a service. Run the following commands to identify this port and hide it: • **kubectl get svc --all-namespaces | grep mongodb** • **magctl service unexpose mongodb** *<port-number>*
—	`Multiple services exist for Postgres to check node-port label.`	For debugging, the Postgres node port is exposed as a service. Run the following commands to identify this port and hide it: • **kubectl get svc --all-namespaces | grep postgres** • **magctl service unexpose postgres** *<port-number>*

Two-site failure scenarios

A two-site failure occurs when at least two of your disaster recovery system's three sites go down at the same time or the sites have been partitioned. Refer to this table for a description of how Catalyst Center responds to the various failure scenarios and any user actions that need to be taken.

Failure scenario	System and user response
Scenario 1: Two of your system's sites go down.	1. The system isolates the site that's still online. **Important** Even if this operation fails, complete the first task described in Step 3 if you plan to operate this site as a standalone site. 2. Log in to this site. 3. If you want the site to operate as a standalone site, click **Standalone** and then click **Continue** in the resulting dialog box. **Note** If you choose this option and want to reestablish your disaster recovery system later: a. Reset the witness site by running the **witness reset** command. b. Log in to the other site that failed and click **Standalone** so that it also operates as a standalone site for the time being. c. Log in to the site that's still online and reconfigure your disaster recovery system. When you set this site to operate in standalone mode, the VIP configured for your system is deleted from the sites that went down. This step is key since it will reconfigure your system's VIP on these sites. If you don't want the site to operate as a standalone site, first bring the two sites that went down back up. Then do one of these tasks: • If the witness site remains offline, refer to the Scenario 3 system and user response. • If the standby site remains offline, refer to the Scenario 4 system and user response. • If the active site remains offline, refer to the Scenario 5 system and user response. When a site enters standalone mode, the system automatically configures its virtual IP address for that site. It also advertises its virtual IP address routes to prevent network reprovisioning.
Scenario 2: The active, standby, and witness sites go down and come back online about the same time.	1. The system isolates the active and standby sites. 2. The system restores the active site and the standby site enters the **Standby Ready** state. 3. You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Event Timeline. 4. Set up disaster recovery, on page 212.

Failure scenario	System and user response
Scenario 3: The active, standby, and witness sites go down. The active and standby sites come back online while the witness site remains offline.	**1.** The system isolates the active and standby sites. **2.** The system restores the active site and the standby site enters the **Standby Ready** state. **3.** You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Event Timeline. **4.** Do one of these tasks: • After the witness site comes back online, Set up disaster recovery, on page 212. • Place your system on pause, on page 225.
Scenario 4: The active, standby, and witness sites go down. The active and witness sites come back online while the standby site remains offline.	**1.** The system isolates and then restores the active site. **2.** You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Event Timeline. **3.** After the former active site comes back online and enters the **Standby Ready** state, Set up disaster recovery, on page 212. If you've determined that you need to replace the nodes at the standby site, instead: **a.** Log in to the witness site and run the **witness reset** command. **b.** Log in to the active site, click **Standalone**, and then click **Continue**. **c.** Replace the nodes at the standby site. **d.** If the witness site will use a virtual machine that's newer than the one that was used previously, complete the steps described in Install the witness site, on page 210. Otherwise, proceed to the next step. **e.** Set up disaster recovery, on page 212.

Failure scenario	System and user response
Scenario 5: The active, standby, and witness sites go down. The standby and witness sites come back online while the active site remains offline.	1. The system isolates the standby site and then establishes it as the new active site. 2. You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Event Timeline. 3. After the former active site comes back online and enters the **Standby Ready** state, Set up disaster recovery, on page 212. If you've determined that you need to replace the nodes at the standby site, instead: a. Log in to the witness site and run the **witness reset** command. b. Log in to the active site, click **Standalone**, and then click **Continue**. c. Replace the nodes at the standby site. d. If the witness site will use a virtual machine that's newer than the one that was used previously, complete the steps described in Install the witness site, on page 210. Otherwise, proceed to the next step. e. Set up disaster recovery, on page 212.

Troubleshoot BGP route advertisement issues

Complete this procedure to troubleshoot the cause of a BGP route advertisement error.

Procedure

Step 1 Validate the BGP session's status on the Catalyst Center cluster:

a) In the Event Timeline, confirm that the **Starting BGP VIP advertisement** task completed successfully (**Activate Disaster Recovery System** > **View Details** > **Configure active** > **View Details**).

   If the task failed, do the these task before going to Step 1b:

   1. Check whether the neighbor router that the error message indicates is up.
   2. Confirm that the neighbor router has connectivity with Catalyst Center. If it doesn't, restore connectivity. Then retry activating the new disaster recovery system or restarting a paused existing system.

b) In the Catalyst Center GUI, view the disaster recovery system's Logical Topology and determine whether the neighbor router is currently active.

   If it's down, check whether the Catalyst Center cluster is configured as a BGP neighbor from the router's perspective. If it's not, configure the cluster as a neighbor. Then retry activating the new disaster recovery system or restarting a paused existing system.

c) View the bgpd and bgpmanager log files by running these commands:

   - **sudo vim /var/log/quagga/bgpd.log**
   - **magctl service logs -rf bgpmanager | lql**

When viewing the log files, look for error messages. If you can't find any, this indicates that the BGP session is functioning properly.

d) Check the status of the BGP session between Catalyst Center and its neighbor router by running the **echo** *admin-password*| **sudo VTYSH_PAGER=more -S -i vtysh -c 'show ip bgp summary'** command.

In the command output, look for the neighbor router's IP address. At the end of the same line, confirm that the output lists the router's connection state as **0**. If so, this indicates that the BGP session is active and functioning properly.

Step 2 Validate the BGP session's status on the neighbor router indicated in the error message:

a) Run the **show ip bgp summary** command.
b) In the command output, look for the Catalyst Center cluster's virtual IP address. At the end of the same line, confirm that the output lists the cluster's connection state as **0**. If so, this indicates that the BGP session is active and functioning properly.
c) Run the **show ip route** command.
d) View the command's output and confirm whether Catalyst Center is advertising the disaster recovery system’s Enterprise virtual IP address.

For example, say your system's Enterprise virtual IP address is 10.30.50.101. If this is the first IP address that you see in the output, this confirms that Catalyst Center is advertising it.

CHAPTER 8

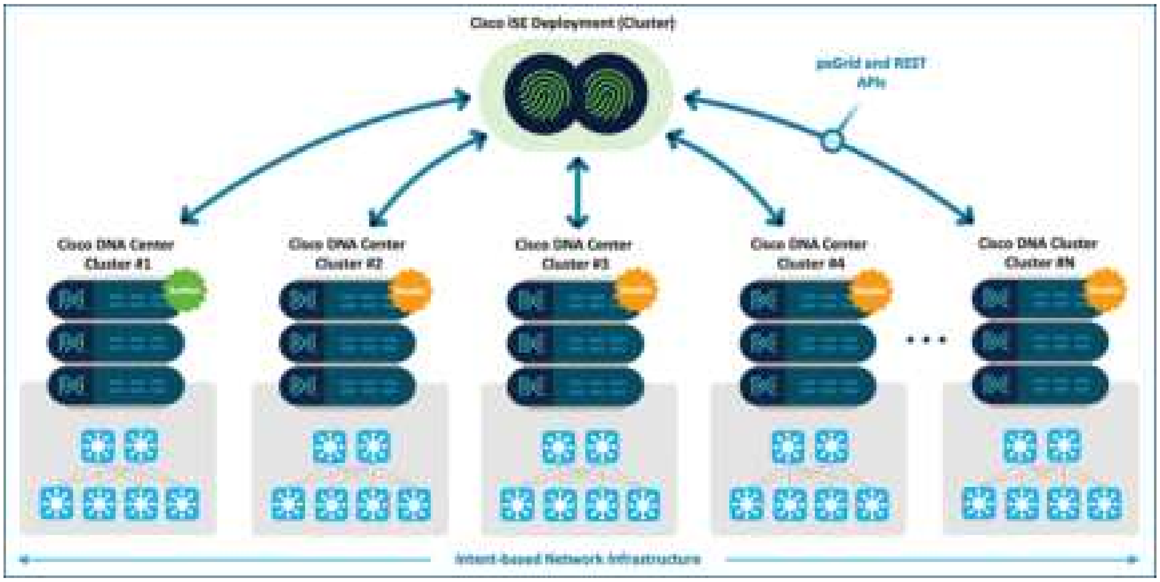
Integrate Multiple Catalyst Center Clusters with a Single Cisco ISE System

Overview of a Multiple Catalyst Center deployment

When you integrate more than one Catalyst Center cluster with a single Cisco ISE system, each Catalyst Center cluster is independent. No information is shared from any one cluster to any other. In this scenario, when Cisco Software-Defined Access (SD-Access) is deployed on Catalyst Center, the set of virtual networks (VNs) and all other SD-Access is local to each cluster.

Catalyst Center provides a mechanism to coordinate SD-Access and Group-Based Policy (GBP) elements across multiple Catalyst Center clusters integrated with a single Cisco ISE system. In order to allow global administration of SD-Access across multiple Catalyst Center clusters with a consistent set of VNs, the Multiple Catalyst Center feature leverages the existing secure connection with Cisco ISE to propagate VNs, security group tags (SGTs), Access Contracts, and Group-Based Access Control (GBAC) Policy from one cluster to another cluster. Cisco ISE takes the information learned from one cluster (known as the Author Node) and propagates it to the other clusters (known as the Reader Nodes).

The Multiple Catalyst Center feature is available when integrated with Cisco ISE Release 3.2 or later.


Cisco ISE Deployment (Cluster)
pxGrid and REST APIs
Cisco DNA Center Cluster #1
Cisco DNA Center Cluster #2
Cisco DNA Center Cluster #3
Cisco DNA Center Cluster #4
Cisco DNA Cluster Cluster #N
Intent-based Network Infrastructure

Note

- The Multiple Catalyst Center operation is disabled by default. To use this feature, select the **Enable Multiple Catalyst Center operation** (under **Advanced Settings**) when integrating Catalyst Center with Cisco ISE. You can enable this feature at the initial configuration or at a later time (after Cisco ISE is already integrated). After this functionality is enabled, only deleting the Cisco ISE integration can disable the functionality.

- If you are using earlier releases of Cisco ISE, you must contact your account team to submit a request to the Cisco SDA Design Council for inclusion in the Limited Availability program. A Multiple Catalyst Center Limited Availability package will be made available to provided to allow access to the limited availability (LA) version of this functionality. See the Multiple Cisco DNA Center to Single Cisco ISE Prescriptive Deployment Guide for more information.

The Multiple Catalyst Center feature has specific role designations for the clusters:

- Author Node cluster
- Reader Node cluster

Author Node cluster

The Author Node role is assigned to the first cluster (with the **Multiple Catalyst Center** option enabled) that integrates with the Cisco ISE deployment, or the first cluster which enables the **Multiple Catalyst Center** option. The Author Node cluster is the administration point for Group-Based Policy (GBP) and for Cisco SD-Access global data. The Author Node cluster manages VNs, SGTs, Access Contracts, and GBAC Policy. Creation, modification, or deletion of VNs and GBP components can only be done on the Author Node cluster.

The Author Node cluster pushes VN and GBP information to Cisco ISE via ERS (REST) APIs for Cisco ISE to use this information and publish to all other Cisco Catalyst Center Clusters in the Reader Node role through Cisco ISE pxGrid.

Only one cluster can be designated as the Author Node. It's the only node where GBP and user-defined global SDA data (such as VNs or extranet policy) can be managed.

If SGTs or VNs are operational on the Author Node, the SGTs or VNs can't be deleted.

Reader Node cluster

All other Catalyst Center clusters which have the Multiple Catalyst Center feature enabled are assigned the role of Reader Node cluster. Reader Node clusters have a read-only view of VNs and SGTs.

Even though Reader Node clusters consume and persist the same VNs, SGTs, Access Contracts, and GBAC Policies that are defined on the Author Node cluster, a Reader Node cluster doesn't display Access Contracts or policies.

VNs can only be created on the Author Node cluster. After created they are propagated to the Reader Node clusters, where they may be used in fabric provisioning operations. The Reader Node clusters configure the associated network attributes such as Virtual Network Identifies (VNID), Route Targets (RT), and Route Distinguishers (RD) which are local to that cluster.

Except for the VN and GBP features, each Reader Node cluster is an independent cluster that manages its own network infrastructure.

The Multiple Catalyst Center feature enables global policy administration across multiple Cisco Catalyst Center clusters integrated to a single Cisco ISE. This capability doesn't change the underlying limitations of managing virtual networks and fabrics on multiple Cisco Catalyst Center clusters. A VN may have the same name across multiple Cisco Catalyst Center clusters, which allows it to support consistent security group-VN associations across multiple clusters. But at the individual cluster level, the actual network attributes to associate with a VN (VRF, route target, route distinguisher, and so on) aren't identical across clusters. This is the same as when operating independent Catalyst Center clusters.

Up to four Catalyst Center clusters can be added as Reader Node clusters. Before adding a Catalyst Center node as a Reader, you must remove all admin-created Cisco SD-Access global data on the Reader Node cluster for Catalyst Center to integrate with Cisco ISE. This includes nondefault VNs (any VNs other than "DEFAULT_VN" and "INFRA_VN", Extranet Policy, and so on). In the event there's any nondefault GBP data (SGTs, Access Contracts, GBP), the user has the option to automatically clean up (delete) all nondefault GBP data, or to merge any GBP data not already present in Cisco ISE.

Note

- Only five Catalyst Center clusters can be integrated with a single Cisco ISE deployment. This means one Author Node cluster and up to four Reader Node clusters.
- It's possible to delete SGTs or VNs on the Author Node even when they are in use on Reader Nodes. In that event, the stale SGTs or VNs must be deleted manually on the Reader Nodes (after removing any references).

Multiple Catalyst Center policy management

After integrating Catalyst Center with Cisco ISE and doing GBP synchronization, policy information is synchronized between Catalyst Center and Cisco ISE. The policy authoring privileges are within Catalyst

Center. The Cisco ISE windows for management of SGTs, Security Group ACLs (SGACLs), and Egress Policy become read only.

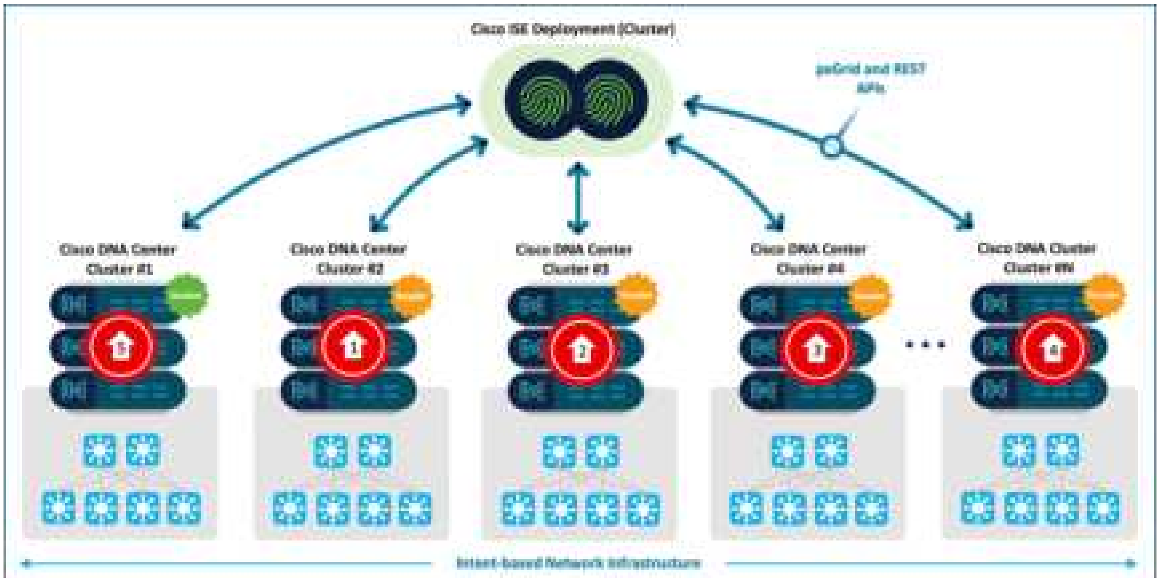
You can manage group-based policy (Security Groups, Access Contracts, and GBAC Policy) in Cisco ISE instead of in Catalyst Center.

In the Catalyst Center GUI, click the menu icon and choose **Policy** > **Group-Based Access Control** > **Policies** > **GBAC Configuration** > **Manage Group-Based Access Control in Cisco ISE**.

Upgrade recommendations for Multiple Catalyst Center

In a Multiple Catalyst Center environment, it's recommended to run the **same Catalyst Center software version across all Author and Reader Node clusters**, except during the process of cluster upgrades. You can upgrade all Reader Node clusters first, and then upgrade the Author Node cluster to avoid feature disparity and feature incompatibility across software versions. Avoid the promotion of a Reader Node cluster to the Author Node role in the middle of an upgrade cycle. All Catalyst Center clusters should be upgraded and running the same software version before promoting a Reader Node cluster.

Figure 1: Upgrade recommendations for Multiple Catalyst Center


Cisco ISE Deployment (Cluster)
pxGrid and REST APIs
Cisco DNA Center Cluster #1
Cisco DNA Center Cluster #2
Cisco DNA Center Cluster #3
Cisco DNA Center Cluster #4
Cisco DNA Cluster Cluster #N
Intent-based Network Infrastructure

Note The basic functionality of the Multiple Catalyst Center feature doesn't require the same software version in all the participating Author and Reader Node clusters. However, using mismatched code versions may result in a difference in fixes, capabilities, and features between the clusters. The same Catalyst Center software version is recommended across all Author and Reader Node clusters.

Multiple Catalyst Center deployments

There are two Multiple Catalyst Center deployment options.

- A new deployment of multiple Catalyst Center clusters that aren't currently integrated with Cisco ISE.
- An existing Catalyst Center cluster that is integrated with Cisco ISE and new additional Catalyst Center clusters without Cisco ISE Integration.

Enabling Multiple Catalyst Center

The Multiple Catalyst Center cluster functionality is disabled by default. It can be enabled during or after integration with Cisco ISE. After the Multiple Catalyst Center functionality is enabled, you can disable it only by removing the Cisco ISE integration completely.

Note The Multiple Catalyst Center operation requires pxGrid functionality. You can't disable pxGrid after enabling Multiple Catalyst Center.

Procedure

Step 1 In the Catalyst Center GUI, click the menu icon and choose **System** > **Settings** > **Authentication and Policy Servers**.

Step 2 Add **Cisco ISE**.

Step 3 Enter the required Cisco ISE information. For information, see Catalyst Center and Cisco ISE integration, on page 36.

Step 4 Choose **System** > **Settings** > **Authentication and Policy Servers** > **Add** > **ISE** > **Advanced Settings**.

The **Advanced Settings** switch exposes various advanced options, including the switch to enable the **Multiple Catalyst Center** operation.

Step 5 Enable the **Multiple Catalyst Center Operation** option.

Step 6 (Optional) If you are editing an existing Cisco ISE integration, re-enter the Cisco ISE admin password.

Step 7 Click **Add**.

Integrating Multiple Catalyst Center with a single Cisco ISE

There are prerequisites for integrating Catalyst Center and Cisco ISE for the first time. For information, see Catalyst Center and Cisco ISE integration, on page 36.

Before you begin

When Catalyst Center is already integrated with Cisco ISE, complete the following steps to reintegrate Catalyst Center and Cisco ISE after enabling the **Multiple Catalyst Center** operation. This allows Catalyst Center to negotiate the Author or Reader Node cluster role based on whether it's a first node or subsequent node joining Cisco ISE with the Multiple Catalyst Center feature enabled.

Procedure

Step 1 In the Catalyst Center GUI, click the menu icon and choose **System** > **Settings** > **Authentication and Policy Servers**.

Step 2 In the **Actions** column, hover your cursor over the ellipsis icon (•••) and choose **Edit**.

Step 3 Choose **System** > **Settings** > **Authentication and Policy Servers** > **Add** > **ISE** > **Advanced Settings**.

Step 4 Enable the **Multiple Catalyst Center Operation** option.

Step 5 Enter the Cisco ISE Admin password again.

Step 6 Click **Add**. Catalyst Center negotiates the Author Node role with Cisco ISE.

- If the status of the configured Cisco ISE server displays "FAILED" because of a password change, click **Retry**, and update the password to resynchronize the Cisco ISE connectivity.
- The status of the integration can be seen in the slide-in pane. Ensure that the integration **Status** displays as **Active** in the **Authentication and Policy Server** window.

Step 7 To verify the negotiated role of the cluster as the Author Node, choose **System** > **Settings** > **System Configuration** > **Multiple Catalyst Center Settings**.

Integrating other Catalyst Center clusters with Cisco ISE as Reader Nodes

To integrate the subsequent Catalyst Center clusters with the same Cisco ISE that has Multiple Catalyst Center enabled, the Catalyst Center cluster must not contain any nondefault VNs (any VNs other than "DEFAULT_VN" and "INFRA_VN").

Before you begin

Verify that the cluster that you want to integrate includes only the default VNs under **Policy** > **Virtual Network**.

Procedure

Step 1 In the Catalyst Center GUI, click the menu icon and choose **System** > **Settings** > **Authentication and Policy Servers**.

Step 2 Click **Add** and choose **ISE**.

Step 3 Enter the required Cisco ISE information. See Catalyst Center and Cisco ISE integration, on page 36.

Step 4 Choose **System** > **Settings** > **Authentication and Policy Servers** > **Add** > **ISE** > **Advanced Settings**.

Step 5 Enable the **Multiple Catalyst Center Operation** option.

Step 6 Click **Add**.

Step 7 (Optional) When integrating the cluster with Cisco ISE for the first time, click **Accept** in the slide-in pane for Catalyst Center to accept the certificate pushed by Cisco ISE. Close the slide-in pane.

Step 8 In the **Authentication and Policy Server** window, verify that the status of the integration displays as **Active**.

Step 9 To verify the Author and Reader Nodes, choose **System** > **Settings** > **System Configuration** > **Multiple CiscoCatalyst CenterSettings**.

Deleting a virtual network

The Author Node cluster does not know of Virtual Network (VN) usage on the Reader Node cluster. You must remove all references to a VN on all the Reader Node clusters before attempting to delete that VN on the Author Node cluster. If you delete a VN on the Author Node cluster, the VN is deleted on the Author node and on the Reader Node clusters which do not have references to it. But if one of the Reader Nodes is using that VN, the status of such a VN then displays as **Out of sync with Author**. You must remove all the references (for example, VN Addition in Host Onboarding Section or static port assignment) of the VN on the Reader Node cluster and then proceed to delete that VN on the Reader Node cluster.

Deleting a security group

The Author Node cluster is not aware of security group usage on a Reader Node cluster. You must remove all references to the security group on all the Reader Node clusters before attempting to delete that security group on the Author Node cluster. If you delete a security group on the Author Node cluster, that security group is deleted on the Author Node cluster, Cisco ISE, and on the Reader Node cluster if there are no references to it. If one of the Reader Node clusters is using that security group, the status of such a security group then displays as **Out of sync with Author**. You must remove all the references of the security group on the Reader Node cluster and then proceed to delete that security group on the Reader Node cluster.

Promotion of Reader Nodes to the Author Role

The Multiple Catalyst Center solution architecture has multiple Catalyst Center clusters and only one cluster can be the policy Author. There may be instances where the Administrator needs to promote a Reader Node cluster to take over the role of the Author Node cluster. This promotion should only be done when:

- You are taking the Author Node cluster out of service or making it unavailable for an extended period of time.
- The Author Node cluster is permanently unavailable or unresponsive for an extended period of time and policy changes are required during that time.

This promotion of a Reader Node to an Author Node can be done in two ways:

1. Graceful Promotion of a Reader Node to the Author role.
2. Force Promotion of a Reader Node to the Author role.

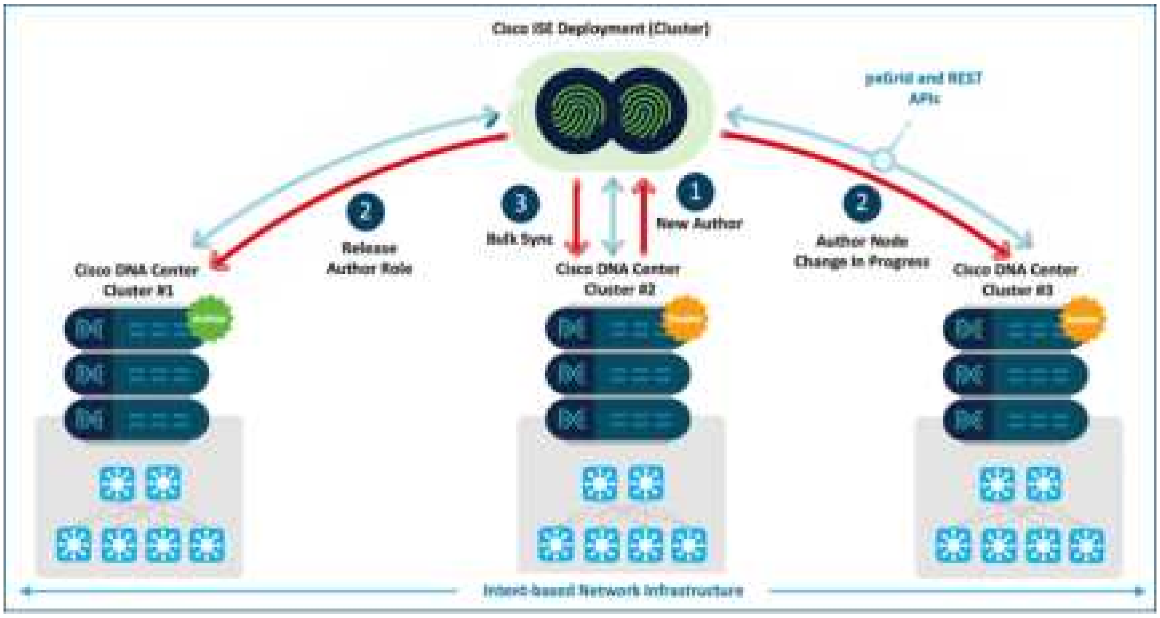
Graceful promotion of a Reader Node to the Author Role

You can manually promote a Reader Catalyst Center cluster to the Author Role if necessary in the Multiple Catalyst Center deployment. All the Reader Node clusters have a **Promote to Author** button. You can promote a Reader Node cluster to an Author Node while your current Author Node cluster is still in operation. However, do not start the promotion operation while the existing Author Node cluster is in the middle of a group-based policy authoring activity (for example, while synchronizing policies with Cisco ISE). If the Author Node cluster is busy, the promotion operation is staggered until the Author Node completes its current processing.

Note

- Upon graceful promotion of a Reader Node cluster to the Author Role, the Reader Node cluster initiates a request to Cisco ISE for a role change (Reader to Author).
- When Cisco ISE receives the role change request, it requests the current Author Node to release the role of policy Author. The current Author node then releases the role of policy Author (if no sync in progress) and takes over the role of the Reader Node cluster.
- The current Reader Node that selected for promotion assumes the role of the Author Node. Upon the Author and Reader Role change, Cisco ISE updates the other Reader Node clusters about the new Author Node through a configuration update.

Figure 2: Graceful promotion of a Reader Node to the Author Role


Cisco ISE Deployment (Cluster)
pxGrid and REST APIs
2
Release Author Role
3
Bulk Sync
1
New Author
2
Author Node Change in Progress
Cisco DNA Center Cluster #1
Cisco DNA Center Cluster #2
Cisco DNA Center Cluster #3
Intent-based Network Infrastructure

Procedure

Step 1 On the Reader Node cluster, choose **System** > **Settings** > > **System Configuration** > **Multiple Cisco Catalyst Center Settings** and verify the Author and Reader Nodes.

Step 2 Click the **Promote to Author** button.

Step 3 Click **Continue** to promote the node to the Author Role.

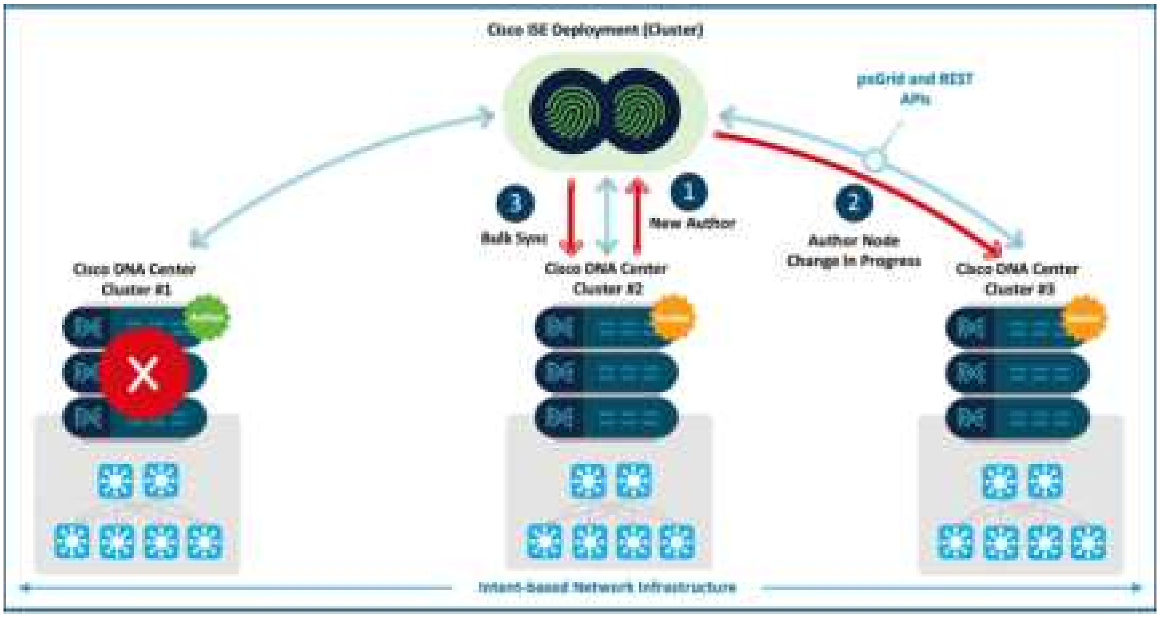
The transition process may take a few minutes.

Force promotion of a Reader Node to the Author Role

Force promotion is a form of manual promotion, that is intended strictly to promote the current Reader Node cluster to Author Node role in these situations:

- The current Author Node cluster is out of service.
- The current Author Node cluster is nonresponsive.
- The graceful promotion of a Reader Node to the Author Role is taking more than 5 minutes.

Figure 3: Force promotion of a Reader Node to the Author Role


Cisco ISE Deployment (Cluster)
pxGrid and REST APIs
3
Bulk Sync
1
New Author
2
Author Node Change In Progress
Cisco DNA Center Cluster #1
Author
Cisco DNA Center Cluster #2
Cisco DNA Center Cluster #3
Intent-based Network Infrastructure

Do not use the force promotion option while the existing Author Node cluster is in service with a GBP authoring activity, as this may result in data loss and the Author Node cluster going out of sync with Cisco ISE. Therefore, force promotion is only recommended if you must restore service immediately and you are willing to risk losing data. After the forced promotion, the promoted Reader Node cluster will become the new Author Node cluster for the deployment. When the former Author Node cluster becomes available, it will transition to a reader role and download the latest configuration data from Cisco ISE.

Upon initiating the promotion of a Reader Node cluster, the Reader Node cluster initiates a request to Cisco ISE for a Role change (in other words, Reader to Author). When Cisco ISE receives the role change request, it requests the current Author Node to release the role of policy Author. If the current Author Node is unresponsive and if the administrator selects **Force Promotion**, the Reader Node cluster ACA initiates a request to force the change of the Reader Node cluster to the Author Role and vice versa immediately in Cisco ISE. This configuration update message is sent to all the nodes.

The steps to force promote a Reader Node cluster to Author Node cluster are exactly the same as exlained in the graceful promotion of a Reader Node to the Author Role section. There is an additional step at the end to initiate the **Force Promotion** function.