



Configure System Settings

- [About System Settings, on page 2](#)
- [User Profile Roles and Permissions, on page 2](#)
- [Use System 360 , on page 3](#)
- [Catalyst Center and Cisco ISE Integration, on page 4](#)
- [Anonymize Data, on page 4](#)
- [Configure Authentication and Policy Servers, on page 5](#)
- [Configure Cisco AI Network Analytics, on page 8](#)
- [Update the Machine Reasoning Knowledge Base, on page 10](#)
- [Configure Cisco Credentials, on page 11](#)
- [Configure Connection Mode, on page 12](#)
- [Register Plug and Play, on page 13](#)
- [Configure Smart Account, on page 15](#)
- [Smart Licensing, on page 15](#)
- [Device Controllability, on page 16](#)
- [Configure SNMP Properties, on page 19](#)
- [Enable ICMP Ping, on page 19](#)
- [Configure AP Location for PnP Onboarding, on page 20](#)
- [Configure an Image Distribution Server, on page 20](#)
- [Enable PnP Device Authorization, on page 21](#)
- [Configure Device Prompts, on page 21](#)
- [Configure Device Configuration Backup Settings, on page 22](#)
- [Configure an External Server for Archiving Device Configuration, on page 23](#)
- [Integrity Verification, on page 24](#)
- [Configure an IP Address Manager, on page 26](#)
- [Configure Webex Integration, on page 27](#)
- [Configure an AppX MS-Teams Integration, on page 28](#)
- [Configure an AppX MS-Teams Integration Through Cisco Cloud Services, on page 29](#)
- [Configure ThousandEyes Integration, on page 30](#)
- [Configure Debugging Logs, on page 30](#)
- [Configure the Network Resync Interval, on page 32](#)
- [View Audit Logs, on page 32](#)
- [Enable Visibility and Control of Configurations, on page 34](#)
- [View, Edit, and Delete Tasks, on page 34](#)

- [High Availability](#), on page 36
- [Configure Integration Settings](#), on page 39
- [Set Up a Login Message](#), on page 39
- [Configure the Proxy](#), on page 40
- [Security Recommendations](#), on page 41
- [About Product Telemetry](#), on page 57
- [Account Lockout](#), on page 57
- [Password Expiry](#), on page 58
- [IP Access Control](#), on page 58

About System Settings

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



Note

- Any changes that you make to the Catalyst Center configuration—including changes to the proxy server settings—must be done from the Catalyst Center GUI.
- Any changes to the IP address, static route, DNS server, or **maglev** user password must be done from the CLI with the `sudo maglev-config update` command.
- By default, the Catalyst Center system time zone is set to UTC. Do not change this time zone in settings because the Catalyst Center GUI works with your browser time zone.
- 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). The roles assigned to a user profile define the capabilities that a user has permission to perform. Catalyst Center has three main default user roles:

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- OBSERVER-ROLE

The SUPER-ADMIN-ROLE gives users broad capabilities and permits them to perform all actions in the Catalyst Center GUI, including creating custom roles and assigning them to user profiles. The NETWORK-ADMIN-ROLE and the OBSERVER-ROLE have more limited and restricted capabilities in the Catalyst Center GUI.

If you're unable to perform an action in Catalyst Center, the reason might be that your user profile is assigned a role that doesn't permit it. For more information, check with your system administrator or see the [Cisco Catalyst Center Administrator Guide](#).

Use System 360

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

Step 1 From the top-left corner, click the menu icon and choose **System > System 360**.

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

Cluster

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

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

The side panel displays the following information:

- **Node Status:** Displays the health status of the node.
If the node health is **Unhealthy**, hover your cursor over the status to view additional troubleshooting information.
- **Services Status:** Displays the health status of the services. Even if one service is down, the status is **Unhealthy**.
- **Name:** Service name.
- **Appstack:** App stack name.
An app stack is a loosely coupled collection of services. A service in this environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.
- **Health:** Status of the service.
- **Version:** Version of the service.
- **Tools:** Displays metrics and logs for the service. Click the **Metrics** link to view service monitoring data in Grafana. Grafana is an open-source metric analytics and visualization suite. You can troubleshoot issues by reviewing the service monitoring data. For information about Grafana, see <https://grafana.com/>. Click the **Logs** link to view service logs in Kibana. Kibana is an open-source analytics and visualization platform. You can troubleshoot issues by reviewing the service logs. For information about Kibana, see <https://www.elastic.co/products/kibana>.
- **Actions:** Option available to restart the service. For some of the internal and system specific services, the **Actions** option is disabled.
- **High Availability:** Status of HA is not available through Catalyst Center on ESXi because HA is provided by VMware vSphere. For more information, see [High Availability, on page 36](#).
- **Cluster Tools:** Lets you access the following tools:
 - **Monitoring:** Access multiple dashboards of Catalyst Center components using Grafana, which is an open-source metric analytics and visualization suite. Use the **Monitoring** tool to review and analyze key Catalyst Center metrics, such as memory and CPU usage. For information about Grafana, see <https://grafana.com/>.

- **Log Explorer:** Access Catalyst Center activity and system logs using Kibana. Kibana is an open-source analytics and visualization platform designed to work with Elasticsearch. Use the **Log Explorer** tool to review detailed activity and system logs. In the Kibana left navigation pane, click **Dashboard**. Then, click **System Overview** and view all of the system logs. For information about Kibana, see <https://www.elastic.co/guide/en/kibana/current/index.html>. For information about Elasticsearch, see <https://www.elastic.co/guide/index.html>.

Note All logging in Catalyst Center is enabled by default.

System Management

- **Software Management:** Displays information about the installed version status and system updates. Click the **View** link to view the update details. The dashlet notifies when the airgap mode is enabled.

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

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

Additionally, it displays the status of the next scheduled backup (or indicates that no backup is scheduled). When airgap mode is enabled, the backup configuration is not found.

Note A backup has a color badge next to it. A green badge indicates a successful backup with a timestamp. An orange badge indicates that the next backup is not yet scheduled.

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](#).

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.

-
- Step 1** From the top-left corner, click the menu icon and 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 the following:

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

Before you configure Cisco ISE, confirm that:

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

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



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

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

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

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



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

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

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

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

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

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

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 the following details:

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

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

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

Note

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

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

hostname.domainname.com

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

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

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

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

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

When you enable this option, ensure that:

- The Catalyst Center certificate is generated by the same CA as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).
 - The Certificate Extended Key Use (EKU) field includes "Client Authentication."
- **Protocol:** **TACACS** and **RADIUS** (the default). You can select both protocols.
- Attention** If you do not enable TACACS for a Cisco ISE server here, you cannot configure the Cisco ISE server as a TACACS server under **Design > Network Settings > Servers** when configuring a AAA server for network device authentication.
- **Authentication Port:** UDP port used to relay authentication messages to the AAA server. The default UDP port used for authentication is 1812.
 - **Accounting Port:** UDP port used to relay important events to the AAA server. The default is UDP port 1812.
 - **Port:** TCP port used to communicate with the TACACS server. The default TCP port used for TACACS is 49.
 - **Retries:** Number of times that Catalyst Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
 - **Timeout:** The time period for which the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

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

Cisco ISE server registration phase:

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

pxGrid subscriptions registration phase:

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

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

Step 6 Click **Add**.

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

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

- a. From the top-left corner, click the menu icon and choose **Provision > Inventory**.
The **Inventory** window displays the device information.
- b. From the **Focus** drop-down menu, choose **Provision**.
- c. In the **Devices** table, the **Provisioning Status** column displays information about the provisioning status of your device (**Success**, **Failed**, or **Not Provisioned**).
Click **See Details** to open a slide-in pane with additional information.
- d. In the slide-in pane that is displayed, click **See Details**.
- e. Scroll down to the **ISE Device Integration** tile to view detailed information about the integration status of the device.

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 Catalyst Advantage software license for Catalyst Center. The **AI Network Analytics** application is part of the Catalyst Advantage software license.
- Make sure that the latest version of the AI Network Analytics application is installed.
- Make sure that your network or HTTP proxy is configured to allow outbound HTTPS (TCP 443) access to the following cloud hosts:

- **api.use1.prd.kairos.ciscolabs.com** (US East Region)
- **api.euc1.prd.kairos.ciscolabs.com** (EU Central Region)

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

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

Step 3 Do one of the following:

- If you have an earlier version of Cisco AI Network Analytics installed in your appliance, do the following:
 - 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 choose 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 the following:
 - a. Click **Configure**.
 - b. In the **Where should we securely store your data?** area, choose 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.

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, as follows:

-
- Step 1** From the top-left corner, click the menu icon and 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 perform a manual update.

-
- Step 1** From the top-left corner, click the menu icon and choose **System > Settings**.
- Step 2** Scroll down to **External Services** and choose **Machine Reasoning Knowledge Base**. The **Machine Reasoning Knowledge Base** window shows the following 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 the following:
- Under **AVAILABLE UPDATES**, click **Update**. A **Success** pop-up window appears with the status of the update.
 - Manually download the Machine Reasoning Knowledge Base to your local machine and import it to Catalyst Center. Do the following:
 - 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

You can configure Cisco credentials for Catalyst Center. Cisco credentials are the username and password that you use to log in to the Cisco website to access software and services.



Note The Cisco credentials configured for Catalyst Center using this procedure are used for software image and update downloads. The Cisco credentials are also encrypted by this process for security purposes.

Before you begin

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

- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > Cisco Accounts > Cisco.com Credentials**.
- Step 2** Enter your Cisco username and password.
- Step 3** Click **Save**.
Your cisco.com credentials are configured for the software and services.
-

Clear Cisco Credentials

To delete the cisco.com credentials that are currently configured for Catalyst Center, complete the following 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 19](#) for a description of how to reenter EULA acceptance.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles](#).

-
- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > Cisco Accounts > Cisco.com Credentials**.
- Step 2** Click **Clear**.
- Step 3** In the resulting dialog box, click **Continue** 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.

-
- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > Cisco Accounts > SSM Connection Mode**.

The following connection modes are available:

- **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, do the following:
- 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.

-
- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > Cisco Accounts > PnP Connect**. A table of PnP connected profiles is displayed.
- Step 2** Click **Register** to register a virtual account.
- Step 3** 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 4** Click the required **IP** or **FQDN** radio button.
- Step 5** Enter the IP address or FQDN (Fully Qualified Domain Name) of the controller.
- Step 6** Enter the profile name. A profile is created for the selected virtual account with the configuration that you provided.
- Step 7** 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 8** 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 the following 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.
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.

Before you begin

Ensure that you have SUPER-ADMIN-ROLE permissions.

-
- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > Cisco Accounts > Smart Account**.
- Step 2** Click the **Add** button. You are prompted to provide Smart Account credentials.
- Enter your Smart Account username and password.
 - Click **Save**.
Your Smart Account is configured.
- 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.
- Choose the **Smart Account** from the drop-down list.
 - 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.

Before you begin

- To enable Smart Licensing, you must configure Cisco Credentials (see [Configure Cisco Credentials, on page 11](#)) and upload Catalyst Center license conventions in Cisco SSM.
- To enable Smart Licensing, you must add Smart Account in **System > Settings > Cisco Accounts > Smart Account**. For more information, see [Configure Smart Account, on page 15](#).

-
- Step 1** From the top-left corner, click the menu icon and 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.

The following device settings are enabled as part of device controllability:

- **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 18](#).

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.

The following circumstances dictate whether or not device controllability configures network settings on devices:

- **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 aids deployment of the required network settings that Catalyst Center needs to manage devices.



Note If you disable device controllability, none of the credentials or features described in the **Device Controllability** page will be configured on the devices during discovery or at runtime.

Device controllability is enabled by default. To manually disable device controllability, do the following:

-
- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > Device Settings > Device Controllability**.
 - Step 2** Uncheck the **Enable Device Controllability** check box.
 - Step 3** Click **Save**.
-

Accept the License Agreement

You must accept the end-user license agreement (EULA) before downloading software or provisioning a device.



Note If you have not yet configured cisco.com credentials, you are prompted to configure them in the **Device EULA Acceptance** window before proceeding.

-
- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > Device Settings > Device EULA Acceptance**.
- Step 2** Click the **Cisco End User License Agreement** link and read the EULA.
- Step 3** Check the **I have read and accept the Device EULA** check box.
- Step 4** 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.

- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > Device Settings > SNMP**.
- Step 2** Configure the following 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.

The following procedure describes how to enable an ICMP ping.

-
- Step 1** From the top-left corner, click the menu icon and 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.

-
- Step 1** From the top-left corner, click the menu icon and 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.

-
- Step 1** From the top-left corner, click the menu icon and 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 the following 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

The following procedure describes how to enable authorization on a device.

Step 1 From the top-left corner, click the menu icon and 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

Step 1 From the top-left corner, click the menu icon and 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, do the following:

- From the **Prompt Type** drop-down list, choose **username**.
- In the **Prompt Text** field, enter the text in Regular Expression (Regex).
- Click **Save**.

Step 4 To create custom prompts for the password, do the following:

- From the **Prompt Type** drop-down list, choose **password**.
- In the **Prompt Text** field, enter the text in Regular Expression (Regex).
- 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).

-
- Step 1** From the top-left corner, click the menu icon and 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 23](#).
-

Configure an External Server for Archiving Device Configuration

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

Before you begin

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

-
- Step 1** From the top-left corner, click the menu icon and 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.

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/cscrdtr/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.

Step 1 From the top-left corner, click the menu icon and 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, perform one of the following 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 Perform one of the following 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 following KGV auto download information is displayed:

- **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 is displayed. 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.

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

Confirm that your external IP address manager is set up and functional.

Step 1 From the top-left corner, click the menu icon and 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, follow these steps:

- 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 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.

Step 1 From the top-left corner, click the menu icon and 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's 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

Once 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.

- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > External Services > Cisco Catalyst - Cloud**.
- Step 2** From the **Region** drop-down list, choose the desired region.
- Step 3** Click the **Q** 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, do the following:
- Log in to **Cisco Catalyst - Cloud** with your cisco.com credentials.
 - If you do not have cisco.com credentials, [you can create them](#).
 - In the **Activate application on your product** window, click the consent flow link and do the following:
 - In the **Sign in to your account** window, enter the Microsoft admin username and password, and click **Sign In**.
 - Click **Accept**.
 - In the **Activate application on your product** window, choose the product that you want to activate and click **Next**. To register a new product, click the **here** link and do the following:
 - In the **Host Name/IP** field, enter IP address of the product.
 - In the **Product Name** field, enter the name of the product.
 - In the **Type** field, enter the type of the product.
 - Click **Register**.
 - Cisco Catalyst - Cloud** synchronizes with Catalyst Center automatically; you are redirected to the **Choose the Scope for your Cisco Catalyst Center** window. Click **Next**.
 - In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
 - 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 29](#).

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.

-
- 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 top-left corner, click the menu icon and choose **Applications and Products**.
- Step 3** From the **Region** drop-down list, choose the desired region.
- 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 28](#).
- 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, do the following:
- In the **Product Activations** table, click **Add**.
 - Choose the product that you want to activate and click **Next**.
- Note** You cannot select more than one product at a time.
- In the **Summary** window, review the configuration settings. To make any changes, click **Edit**. Otherwise, click **Activate**.
- Step 10** (Optional) To deactivate the product, do the following:
- Click the **AppX MS-Teams** tile.
 - In the **Product Activations** table, check the check box next to the product that you want to deactivate.
 - From the **More Action** drop-down list, choose **Deactivate**.
 - In the confirmation window, click **Deactivate**.
- Step 11** (Optional) To disconnect the product from AppX MS-Teams application, do the following:
- Click the **AppX MS-Teams** tile to view the details in the **App 360** window.
 - 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.

For ThousandEyes integration to work, after deploying the ThousandEyes agent on the device, you must set the agent hostname to match the **Device Name** in the **Provision > Network Devices > Inventory** table.

Before you begin

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

- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > External Services > ThousandEyes Integration**.
- Step 2** In the **Insert new token here** field, enter the authentication token.
- Note** To receive the OAuth Bearer Token, go to the [ThousandEyes](#) page.
- Step 3** Click **Save**.
ThousandEyes is enabled.
- Step 4** (Optional) Click **Delete** to delete the OAuth Bearer Token.
-

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.

-
- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > System Configuration > Debugging Logs**.
- The **Debugging Logs** window is displayed.
- Step 2** From the **Service** drop-down list, choose a service to adjust its logging level.
- The **Service** drop-down list displays the services that are currently configured and running on Catalyst Center.
- Step 3** Enter the **Logger Name**.
- This is an advanced feature that has been added to control which software components emit messages into the logging framework. Use this feature with care. Misuse of this feature can result in loss of information needed for technical support purposes. Log messages will be written only for the loggers (packages) specified here. By default, the Logger Name includes packages that start with *com.cisco*. You can enter additional package names as comma-separated values. Do not remove the default values unless you are explicitly directed to do so. Use * to log all packages.
- Step 4** From the **Logging Level** drop-down list, choose the new logging level for the service.
- Catalyst Center supports the following logging levels in descending order of detail:
- **Trace**: Trace messages
 - **Debug**: Debugging messages
 - **Info**: Normal, but significant condition messages
 - **Warn**: Warning condition messages
 - **Error**: Error condition messages
- Step 5** From the **Time Out** field, choose the time period for the logging level.
- Configure logging-level time periods in increments of 15 minutes up to an unlimited time period. If you specify an unlimited time period, the default level of logging should be reset each time a troubleshooting activity is completed.
- Step 6** Review your selection and click **Save**.
-

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.
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

-
- Step 1** From the top-left corner, click the menu icon and 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.

-
- Step 1** From the top-left corner, click the menu icon and choose **Activities > Audit Logs**.
- The **Audit Logs** window opens, where you can view logs about the current policies in your network. These policies are applied to network devices by the applications installed on Catalyst Center.
- Step 2** Click the timeline slider to specify the time range of data you want displayed on the window:
- a. In the **Time Range** area, choose a time range—**Last 2 Weeks**, **Last 7 Days**, **Last 24 Hours**, or **Last 3 Hours**.
 - b. To specify a custom range, click **By Date** and specify the start and end date and time.
 - c. Click **Apply**.
- Step 3** Click the arrow next to an audit log to view the corresponding child audit logs.
- Each audit log can be a parent to several child audit logs. By clicking the arrow, you can view a series of additional child audit logs.

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

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

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

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

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

Step 6 Click **Subscribe** to subscribe to the audit log events.

A list of syslog servers is displayed.

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

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

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

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

Export Audit Logs to Syslog Servers

Security Recommendation: We strongly encourage you to export audit logs from Catalyst Center to a remote syslog server in your network, for more secure and easier log monitoring.

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

Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **Activities > Audit Logs**.

Step 2 Click **Subscribe**.

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

Step 4 (Optional) To unsubscribe, deselect the syslog servers and click **Save**.

Use APIs to View Audit Logs in Syslog Servers

With the Catalyst Center platform, you can use APIs to view audit logs in syslog servers. Using the **Create Syslog Event Subscription** API from the **Developer Toolkit**, create a syslog subscription for audit log events.

Whenever an audit log event occurs, the syslog server lists the audit log events.

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, the following banner message is displayed 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*.

Step 1 From the top-left corner, click the menu icon and 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, Edit, 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.

Step 1 From the top-left corner, click the menu icon and 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, 2023, at 12 PM. One device is in San Jose, CA, and the other device is in Bengaluru, India. The **Starts** field displays May 8, 2023, 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, 2023, 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 the following table to view, edit, or delete a task on the **Tasks** window.

Action	Steps
View a task.	<p>a. Click the task name to open a slide-in pane with more information.</p> <p>The task details depend on what type of task you're viewing.</p> <p>b. In the slide-in pane, depending on the details displayed, you can do the following:</p> <ul style="list-style-type: none"> • 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. <p>A tar file is created and saved to your local machine.</p> <p>Tip While creating a support case, you can attach the downloaded error report in addition to other details you may want to include.</p>

Action	Steps
Edit the schedule of a recurring task.	<ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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.
Delete a task.	<ol style="list-style-type: none"> a. Locate the task and click Delete.

High Availability

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

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

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

Configure VMware vSphere HA for Host-Level Failures

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

Before you begin

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



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

- Step 1** Log in to the vSphere Client.
- Step 2** Choose the appropriate Catalyst Center cluster in the device menu.
- Step 3** To configure the cluster, choose **Configure > Services > vSphere Availability**.
- Step 4** From the top-right corner, click **Edit**.
- Step 5** Click the toggle button to enable **vSphere HA**.
- Step 6** Choose **Failures and responses** and configure the following settings:
- Click the toggle button to enable **Host Monitoring**.
 - Go to the **Host Failure Response** drop-down list and choose **Restart VMs**.

Edit Cluster Settings | danc-cluster
×

vSphere HA

Failures and responses
Admission Control
Heartbeat Datastores
Advanced Options

You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring ?

> Host Failure Response	Restart VMs ▾
> Response for Host Isolation	Disabled ▾
> Datastore with PDL	Power off and restart VMs ▾
> Datastore with APD	Power off and restart VMs - Conservative restart policy ▾
> VM Monitoring	Disabled ▾

CANCEL
OK

Step 7 Click **OK**.

Configure Catalyst Center on ESXi Virtual Machine for Priority Restart

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

Step 1 Log in to the vSphere Client.

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

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

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

Step 5 Click **OK**.

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

- a) Check the **Override** check box.
- b) From the drop-down list, choose **Highest**.

The screenshot shows the 'Add VM Override' dialog box for the cluster 'danc-cluster'. The dialog is divided into sections for different vSphere features. The 'vSphere HA' section is currently active, showing the 'VM Restart Priority' setting. The 'Override' checkbox is checked, and the dropdown menu is set to 'Highest'. Other settings in the 'vSphere HA' section include 'Start next priority VMs when:', 'Additional delay:', 'VM restart priority condition timeout:', and 'Host isolation response'. The 'vSphere HA - PDL Protection Settings' section shows the 'Failure Response' set to 'Power off and restart VMs'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'FINISH'.

Step 7 Click **FINISH**.

VMware vSphere Product Documentation

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

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

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.

Step 1 From the top-left corner, click the menu icon and 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.

Step 1 From the top-left corner, click the menu icon and 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 on ESXi has a proxy server configured as an intermediary between itself and the network devices that it manages, you must configure access to the proxy server.



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

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles](#).

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

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

Step 3 Enter the proxy server's URL address.

Step 4 Enter the proxy server's port number.

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

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

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

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

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

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

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

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. We strongly recommend that you 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.

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, we recommend that the proxy and the Catalyst Center server certificate 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, perform the following procedure to import a proxy gateway certificate in to Catalyst Center.

Before you begin

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

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

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

See [About Restricted Shell](#), on page 55.

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 the following command, where *<directory>* is the location of the certificate file on the Catalyst Center server and *<proxy.pem>* is your proxy server's TLS/SSL certificate file:

```
$ sudo /usr/local/bin/update_cacerts.sh -v -a /<directory>/<proxy.pem>
```

The command returns an output that is similar to the following:

```
Reading CA cert from file /tmp/sdn.pem
Adding certificate import_1E:94:6D:2C:81:22:BB:B2:2E:24:BD:72:57:AE:35:AD:EC:5E:71:44.crt
Updating /etc/ca-certificates.conf
Updating certificates in /etc/ssl/certs...
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Deleting tempfiles /tmp/file0PpQxV /tmp/filePtmQ8U /tmp/filercR3cV
```

Step 3 In the command output, look for the line “1 added” and confirm that the number added is not zero. The number can be 1 or more than 1, based on the certificates in the chain.

Step 4 Enter the following commands to restart docker and the catalog server:

```
sudo systemctl restart docker
magctl service restart -d catalogserver
```

Step 5 Log in to Catalyst Center GUI and do the following:

- Navigate to **System > Settings > Certificates > Trusted Certificates** and upload the same certificate. For more information, see [Configure Trusted Certificates](#), on page 54.
- Check cloud connectivity and CMX/Spaces connectivity.

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 the following 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.

With Catalyst Center 2.3.4.x and earlier, do not import Digital Signature Algorithm (DSA), Diffie-Hellman (DH), Elliptic-curve Diffie-Hellman (ECDH), and Elliptic Curve Digital Signature Algorithm (ECDSA) key types, because they are not supported. Catalyst Center 2.3.4.x and earlier does not support any form of ECDH and ECDSA, which includes any leaf certificate tied to the certificate chain.

Catalyst Center 2.3.5 and later supports Edwards-curve Digital Signature Algorithm (EdDSA), ECDSA, and RSA 2048-4096 key types.

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 supports the import and storage of an X.509 certificate and private key into Catalyst Center. After import, the certificate and private key 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 using the **Certificates** window in the GUI.

Before you begin

Obtain a valid X.509 certificate that is issued by your internal Certificate Authority. The certificate must correspond to a private key in your possession.

Step 1 From the top-left corner, click the menu icon and choose > **System** > **Settings** > **Trust & Privacy** > **System Certificates**.

Step 2 In the **System** tab, view the current certificate data.

When you first view this window, the current certificate data that is displayed in the Catalyst Center self-signed certificate. The self-signed certificate's expiry is set for several years in the future.

Note The expiration date and time is displayed as a Greenwich Mean Time (GMT) value. A system notification is displayed in the Catalyst Center GUI two months before the certificate expires.

The **System** tab displays the following fields:

- **Current Certificate Name:** Name of the current certificate.
- **Issuer:** Name of the entity that has signed and issued the certificate.
- **Expires:** Expiry date of the certificate.

Step 3 In the **System Certificates** window, click **Replace Certificate**.

If you are generating the CSR for the first time, the **Generate New CSR** link is displayed.

Otherwise, the **Download existing CSR** link is displayed. You can download the existing CSR and submit it to your provider to generate your certificate. If you don't want to use the existing CSR, click **Delete existing CSR**, and then click **Accept** in the subsequent **Confirmation** window. You can now see the **Generate New CSR** link.

Step 4 Click the **Generate New CSR** link.

Step 5 In the **Certificate Signing Request Generator** window, provide information in the required fields.

Step 6 Click **Generate New CSR**.

The generated new CSR is downloaded automatically.

The **Certificate Signing** window shows the CSR properties and allows you to do the following:

- Copy the CSR properties in plain text.
- Copy Base64 and paste to any Certificate Authority. For example, you can paste Base64 to Microsoft Certificate Authority.
- Download Base64.

Step 7 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.

Note **PKCS** file type is disabled if you choose the **Generate New CSR** option to request a certificate.

Step 8 Confirm that the certificate issuer provides the certificate full chain (server and CA) in p7b. When in doubt, do the following to examine and assemble the chain:

- a) Download the p7b bundle in DER format and save it as server-cert-chain.p7b.
- b) Copy the server-cert-chain.p7b certificate to the Catalyst Center cluster through SSH.
- c) Enter the following command:

```
openssl pkcs7 -in server-cert-chain.p7b -inform DER -out server-cert-chain.pem -print_certs
```

For using the `openssl` command, you must have access to the restricted or secure root shell. If you want to access the root shell, you must contact Cisco TAC for assistance.

- d) Confirm that all certificates are accounted for in the output, with the issuer and Catalyst Center certificates included. Continue to upload as PEM. If the certificates are in loose files, complete the next step to download and assemble the individual files.

Step 9 If the certificate issuer provides the certificate and its issuer CA chain in loose files, do the following:

- a) Gather the PEM (base64) files or use `openssl` to convert DER to PEM.
- b) 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. For example:

```
cat certificate.pem subCA.pem rootCA.pem > server-cert-chain.pem
```

- c) Continue to upload as PEM.

Step 10 For a **PEM** file, perform the following tasks:

- Import the **PEM** file by dragging and dropping the file into the Drag and Drop 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.

- Import the **Private Key** by dragging and dropping the file into the Drag and Drop 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.

- Choose the encryption option from the **Encrypted** area for the private key.
- If you choose encryption, enter the password for the private key in the **Password** field.

Step 11 For a **PKCS** file, perform the following tasks:

- Import the **PKCS** file by dragging and dropping the file into the Drag and Drop 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.

- Enter the passphrase for the certificate in the **Password** field.

Note For PKCS, the imported certificate also requires a passphrase.

- For the **Private Key** field, choose the encryption option for the private key.
- For the **Private Key** field, if encryption is chosen, enter the password for the private key in the **Password** field.

Step 12 Click **Save**.

Note After the Catalyst Center server's SSL certificate is replaced, you are automatically logged out, and must log in again.

Step 13 Return to the **Certificates** window to view the updated certificate data.

The information displayed in the **System** tab should have changed to reflect the new certificate name, issuer, and the certificate authority.

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 the following procedure:



Note For more information regarding SCEP, see [Simple Certificate Enrollment Protocol Overview](#).

Step 1 From the top-left corner, click the menu icon and 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 the following 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 the following 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, if you want to switch back to the internal certificate, do the following:

Step 1 From the top-left corner, click the menu icon and 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 50](#).

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.

Step 1 From the top-left corner, click the menu icon and 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.

Certificate Management

Manage Device Certificates

You can view and manage certificates that are issued by Catalyst Center for managed devices to authenticate and identify the devices.

Step 1 From the top-left corner, click the menu icon and 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 If you want to revoke a valid certificate, do the following:

- 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 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.

Step 1 From the top-left corner, click the menu icon and 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**.

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 the following 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, do the following:

- 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 the following 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 the following procedure).

After the import, Catalyst Center initializes itself as the subordinate CA and provides all the existing functionalities of a subordinate CA.

- If device controllability is enabled (which is the default) before the switchover from the internal root CA to the subordinate CA, the new device certificate is updated automatically.
- 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.
- Note 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.

-
- Step 1** From the top-left corner, click the menu icon and 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 are displayed:

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 perform one of the following 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 is displayed.

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 50](#).
- 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.

Step 1 From the top-left corner, click the menu icon and 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 perform one of the following 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 is displayed.

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.

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.

The following manual configuration is required to enroll from an external CA via SCEP.

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
  rsa-keypair 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>
```

Renew 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 certificates for another year before they are set to expire.

- We recommend that you renew certificates before they expire, not after.
- You can only renew 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.

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 the following command:

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

Step 3 Renew the certificates that are set to expire soon by entering the following 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
```

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.

Step 1 From the top-left corner, click the menu icon and 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 1: Restricted Shell Commands

Command	Description
<code>cat</code>	Concatenate and print files in restricted mode.
<code>clear</code>	Clear the terminal screen.
<code>date</code>	Display the current time in the given FORMAT or set the system date.
<code>debug</code>	Enable console debug logs.

Command	Description
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.
ps	Check status of active processes in the system.
rca	Root cause analysis collection utilities.
reboot	Reboot the machine.
rm	Delete files in restricted mode.
route	Print the IP routing table.
runonce	Execute runonce scripts.
scp	Restricted secure copy.
sftp	Secure file transfer.
shutdown	Shutdown the machine.
ssh	OpenSSH SSH client.
tail	Print the last 10 lines of each FILE to standard output.
top	Display sorted list of system processes.
traceroute	Print the route packets trace to network host.

Command	Description
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 top-left corner, click the menu icon and 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.

Configure Telemetry Collection

-
- Step 1** From the top-left corner, click the menu icon and choose **System Settings > Settings > Telemetry Collection**.
- Step 2** To review the agreement for Telemetry Collection, click **End User License Agreement**.
- Step 3** (Optional) To disable Telemetry Collection, uncheck the **Telemetry Collection** check box and click **Update**.
-

Account Lockout

You can configure the account lockout policy to manage user login attempts, account lockout period, and number of login retries.

-
- Step 1** From the top-left corner, click the menu icon and 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 the following **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 Choose the **Idle Session Timeout** value from the drop-down list.

Step 5 Click **Save**.

If you leave the session idle, a **Session Timeout** dialog box appears five minutes before the session timeout. Click **Stay signed in** if you want to continue the session. You can click **Sign out** to end the session immediately.

Password Expiry

You can configure the password expiration policy to manage the following:

- Password expiration frequency.
- Number of days that users are notified before their password expires.
- Grace period.

Step 1 From the top-left corner, click the menu icon and 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 the following options for IP access control:

- 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, perform the following steps:

1. [Enable IP Access Control, on page 59](#)
2. [Add an IP Address to the IP Access List, on page 59](#)
3. (Optional) [Delete an IP Address from the IP Access List, on page 60](#)

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.

Step 1 From the top-left corner, click the menu icon and 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, perform the following steps.

Before you begin

Ensure that you enable IP access control. For more information, see [Enable IP Access Control, on page 59](#).

Step 1 From the top-left corner, click the menu icon and 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.

The screenshot shows the 'IP Access Control' settings page. The main page has a title 'IP Access Control' and a sub-header 'Settings / Trust & Privacy'. Below the title, it states 'Cisco DNA Center is accessible from all IP addresses by default.' There are two radio buttons: 'Allow all IP addresses to connect' (unselected) and 'Allow only listed IP addresses to connect' (selected). Below this is a table with two columns: 'IP Address' and 'Subnet Mask'. The table contains one row with the IP address '209.165.200.230' and subnet mask '32'. At the bottom of the table, it says '1 Records'. An 'Add IP' dialog box is open on the right side of the page. The dialog box has a title 'Add IP' and a close button 'X'. It contains two input fields: 'IP Address*' with the value '209.165.210.0' and a placeholder 'Enter an IPv4 address', and 'Subnet Mask*' with the value '27' and a placeholder 'Valid range: 0-32'. At the bottom of the dialog box, there are 'Cancel' and 'Save' buttons.

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, perform the following steps.

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 59](#) and [Add an IP Address to the IP Access List, on page 59](#).

Step 1 From the top-left corner, click the menu icon and 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, perform the following steps.

Before you begin

Ensure that you have SUPER-ADMIN-ROLE permissions.

-
- Step 1** From the top-left corner, click the menu icon and choose **System > Settings > Trust & Privacy > IP Access Control**.
- Step 2** Click the **Allow all IP addresses to connect** radio button.
-

