Cisco Catalyst Center 2.3.7.x on ESXi Administrator Guide

First Published: 2023-12-20

Last Modified: 2024-04-08

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

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

© 2023–2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

Configure System Settings 1

About System Settings 2

User Profile Roles and Permissions 2

Use System 360 3

Catalyst Center and Cisco ISE Integration 4

Anonymize Data 4

Configure Authentication and Policy Servers 5

Configure Cisco AI Network Analytics 8

Client Certificate Renewal 9

Disable Cisco AI Network Analytics 10

Update the Machine Reasoning Knowledge Base 10

Configure Cisco Credentials 11

Clear Cisco Credentials 12

Configure Connection Mode 12

Register Plug and Play 13

Create PnP Event Notifications 14

Configure Smart Account 15

Smart Licensing 15

Device Controllability 16

Configure Device Controllability 18

Accept the License Agreement 19

Configure SNMP Properties 19

Enable ICMP Ping 19

Configure AP Location for PnP Onboarding 20

Configure an Image Distribution Server 20

Enable PnP Device Authorization 21

Configure Device Prompts 21
Create Custom Prompts 22
Configure Device Configuration Backup Settings 22
Configure an External Server for Archiving Device Configuration 23
Integrity Verification 24
Upload the KGV File 24
Configure an IP Address Manager 26
Configure Webex Integration 27
Configure an AppX MS-Teams Integration 28
Configure an AppX MS-Teams Integration Through Cisco Cloud Services 29
Configure ThousandEyes Integration 30
Configure Debugging Logs 30
Configure the Network Resync Interval 32
View Audit Logs 32
Export Audit Logs to Syslog Servers 33
Use APIs to View Audit Logs in Syslog Servers 33
Enable Visibility and Control of Configurations 34
View, Edit, and Delete Tasks 34
High Availability 36
Configure VMware vSphere HA for Host-Level Failures 36
Configure Catalyst Center on ESXi Virtual Machine for Priority Restart 38
VMware vSphere Product Documentation 39
Configure Integration Settings 39
Set Up a Login Message 39
Configure the Proxy 40
Security Recommendations 41
Configure the Proxy Certificate 41
Upload an SSL Intercept Proxy Certificate 43
Certificate and Private Key Support 43
Certificate Chain Support 44
Update the Catalyst Center Server Certificate 45
Use an External SCEP Broker 47
Switch Back to an Internal Certificate Authority 48
Export the Catalyst Center Certificate Authority 48

Certificate Management 49
Manage Device Certificates 49
Configure the Device Certificate Lifetime 49
Change the Role of the Certificate Authority from Root to Subordinate 50
Provision a Rollover Subordinate CA Certificate 52
Configure the Device Certificate Trustpoint 53
Renew Certificates 54
Configure Trusted Certificates 54
About Restricted Shell 55
About Product Telemetry 57
Configure Telemetry Collection 57
Account Lockout 57
Password Expiry 58
IP Access Control 58
Configure IP Access Control 58
Enable IP Access Control 59
Add an IP Address to the IP Access List 59
Delete an IP Address from the IP Access List 60
Disable IP Access Control 60

CHAPTER 2 **Manage Applications** 63
Application Management 63
Download and Install the Latest System Version 63
Download and Install the Latest System Version in Air Gap Mode 70
Download and Install Application Updates 71
Uninstall an Application 72

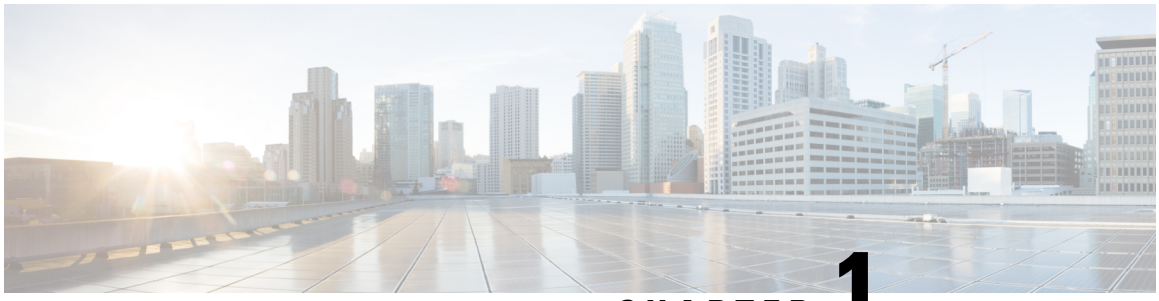
CHAPTER 3 **Manage Users** 73
About User Profiles 73
About User Roles 73
Create an Internal User 74
Edit a User 74
Delete a User 75
Reset a User Password 75

Change Your Own User Password 76
Change Your Own User Password Without Admin Permission 76
Reset a Forgotten Password 76
Configure Role-Based Access Control 76
Catalyst Center User Role Permissions 78
Display Role-Based Access Control Statistics 82
Configure External Authentication 82
Two-Factor Authentication 84
Prerequisites for Two-Factor Authentication 85
Two-Factor Authentication Workflow 85
Configure Two-Factor Authentication 85
Enable Two-Factor Authentication Using RADIUS 87
Enable Two-Factor Authentication Using TACACS+ 87
Log In Using Two-Factor Authentication 88
Display External Users 88

CHAPTER 4 **Manage Licenses** 89
License Manager Overview 89
Integration with Cisco Smart Accounts 92
Set Up License Manager 93
Visualize License Usage and Expiration 94
View Historical Trends for License Consumption 95
View License Details 96
Change License Level 97
Auto Registration of Smart License-Enabled Devices 98
Day 0 Configuration for Smart License-Enabled Devices 98
Apply Specific License Reservation or Permanent License Reservation to Devices 99
Enable SLR/PLR When the Devices and Catalyst Center Are Connected to CSSM 99
Enable SLR/PLR When the Devices and Catalyst Center Are Not Connected to CSSM 100
Generate the Authorization Code from CSSM 100
Cancel SLR or PLR Applied to Devices 101
Install the Authorization Code and Enable the High Security License 101
Disable the High Security License 102
Upload Resource Utilization Details to CSSM 102

Change Device Throughput 103
Transfer Licenses Between Virtual Accounts 103
Manage Customer Tags on Smart License-Enabled Devices 104
Modify License Policy 104

CHAPTER 5 **Backup and Restore** 107
About Backup and Restore 107
Backup and Restore Event Notifications 109
NFS Backup Server Requirements 109
Backup Physical Disk Nomenclature 110
Backup Storage Requirements 110
Add a Physical Disk for Backup and Restore 111
Add the NFS Server 114
Configure the Location to Store Backup Files 115
Create a Backup 117
Restore Data from Backups 119
Restore Data from a Physical Disk for a Faulty Virtual Appliance 121
Restore Data from an NFS Server for a Faulty Virtual Appliance 127
Schedule Data Backup 130



CHAPTER 1

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 Reason 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, on page 73.

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.

a) Enter your Smart Account username and password.
b) 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.

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

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

Note Cisco Accounts supports multiple smart and virtual accounts.

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

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

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

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

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

Step 9 Click **Delete**.

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

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

Smart Licensing

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

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

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

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:

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

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

c. Click **Save**.

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

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

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

c. Click **Save**.

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

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

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

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

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

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

Configure Device Configuration Backup Settings

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

Note

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

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

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

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/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar

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

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

Before you begin

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

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 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:

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

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

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

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

c) In the **Activate application on your product** window, 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**.

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

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

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

Note If you want to deactivate the product or disconnect from AppX MS-Teams application, see Configure an AppX MS-Teams Integration Through Cisco Cloud Services, on page 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:

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

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

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

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

Step 10 (Optional) To deactivate the product, do the following:

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

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

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

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

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

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

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

c) Click **Disconnect now**.

Configure ThousandEyes Integration

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

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.	**a.** Click the task name to open a slide-in pane with more information. The task details depend on what type of task you're viewing. **b.** In the slide-in pane, depending on the details displayed, you can do the following: • View device and provisioning details by clicking **Device Details** or **Provision Details**. • View more information about in-progress, completed, and failed tasks by clicking **View Details** or **See Details**. • Search for a task using **Search Table**. • Filter for a task using the filter icon in the top-right corner of the table. • Download an error report of a failed task by clicking **Download Error Report**. A tar file is created and saved to your local machine. **Tip** While creating a support case, you can attach the downloaded error report in addition to other details you may want to include.

Action	Steps
Edit the schedule of a recurring task.	**a.** Locate the task and click **Edit**. **b.** In the **Edit Schedule** slide-in pane, define the **Start Date** and **Start Time**. **c.** Using the **Recurrence** toggle button, click a recurrence interval. **d.** In the **Run at Interval** field, enter a value. **e.** (Optional) To schedule an end date and time for this task, do the following: **1.** Check the **Set Schedule End** check box. **2.** To end the task on a specific date, click **End Date** and choose the date. **3.** To end the task after a number of occurrences, click **End After** and in the **Occurrences** field, enter a numerical value. **f.** Click **Preview** to review the changes in the table. **g.** Ensure the table's listed **Site Time** (the device's time zone) and **Local Time** (your time zone) for each device reflect the intended scheduled time **h.** When you're ready, click **Save**.
Delete a task.	**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**.

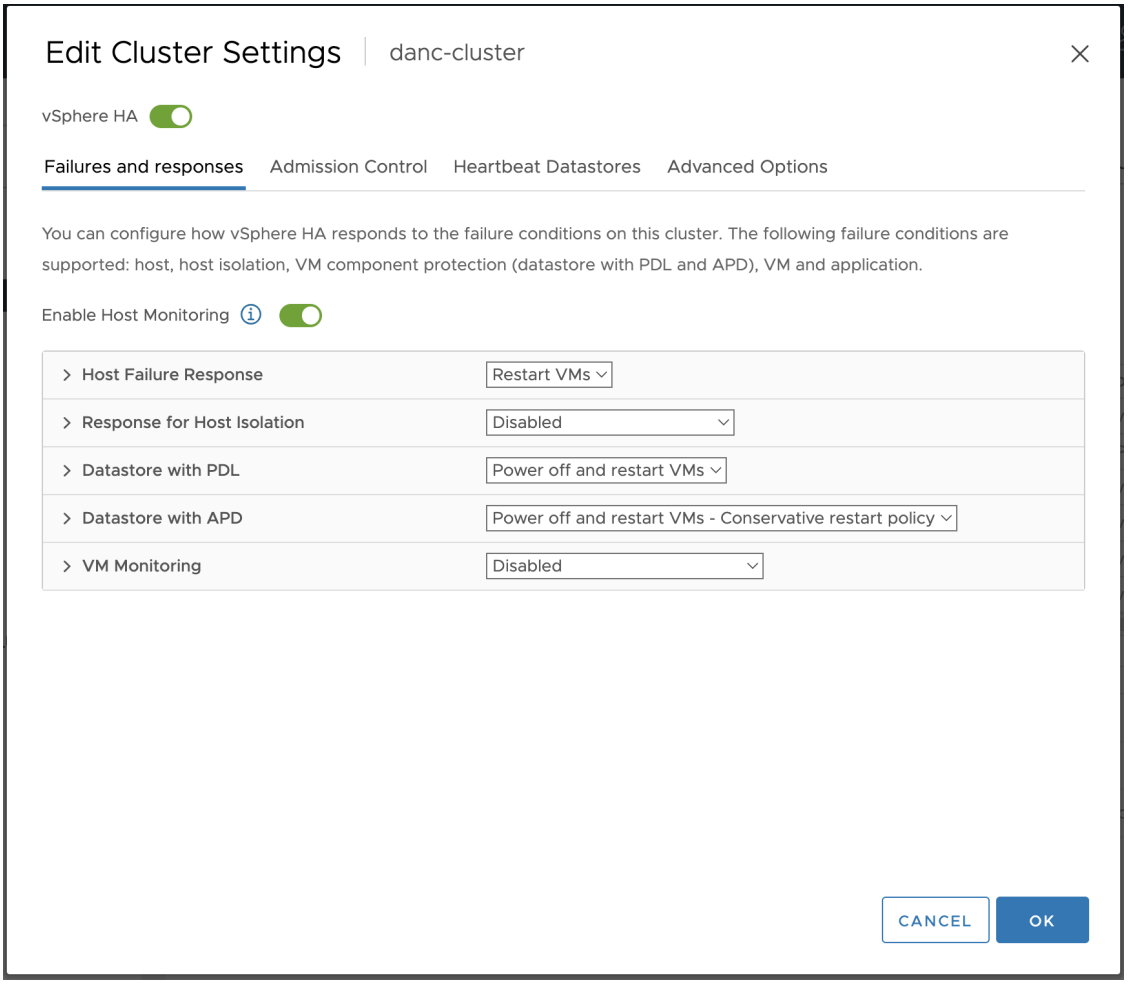
Step 4 From the top-right corner, click **Edit**.

Step 5 Click the toggle button to enable **vSphere HA**.

Step 6 Choose **Failures and responses** and configure the following settings:

a) Click the toggle button to enable **Host Monitoring**.

b) Go to the **Host Failure Response** drop-down list and choose **Restart VMs**.



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**.

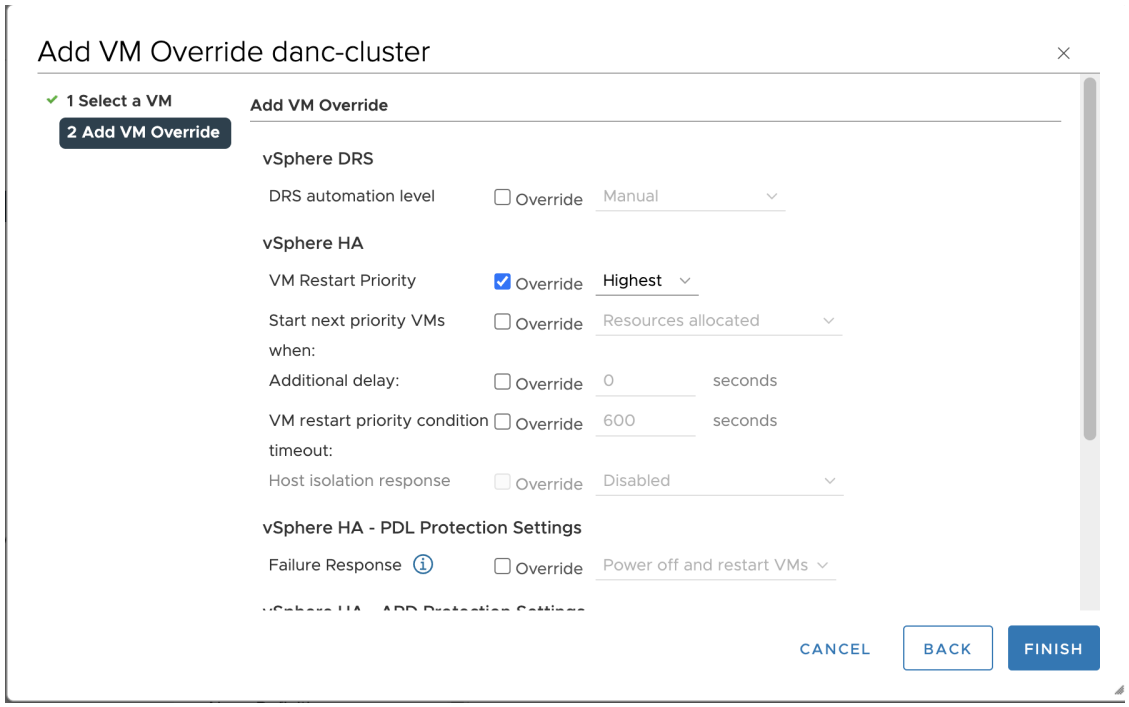
Step 4 In the **Select a VM** window, choose the deployed Catalyst Center on ESXi virtual machine.

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**.



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, on page 73.

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 /temp/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:

a) Navigate to **System** > **Settings** > **Certificates** > **Trusted Certificates** and upload the same certificate. For more information, see Configure Trusted Certificates, on page 54.

b) 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
  rsakeypair sdn-network-infra-iwan
  fingerprint <CA_fingerprint> # to verify that the CA at the url connection matches the fingerprint
 given
```

Step 2 (Optional, but recommended) Automatically renew the certificate and avoid certificate expiry:

```
auto-enroll 80 regenerate
```

Step 3 (Optional) Specify the interface that is reachable to the enrollment URL. Otherwise, the default is the source interface of the http service.

```
source interface <interface>
```

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

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.

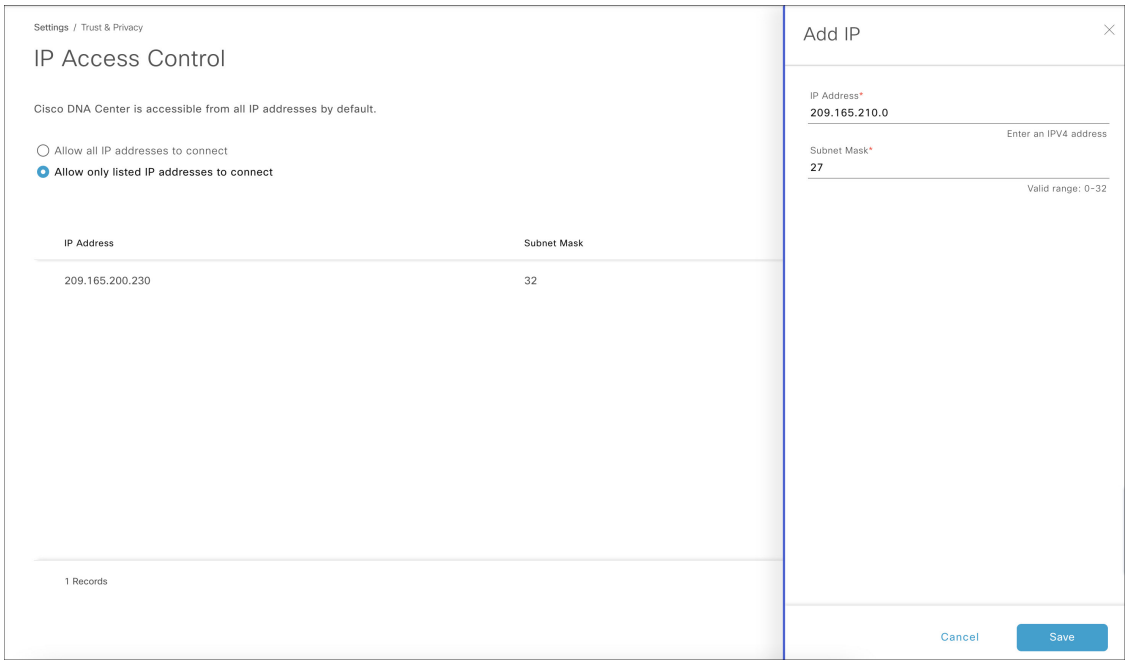
Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

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.



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

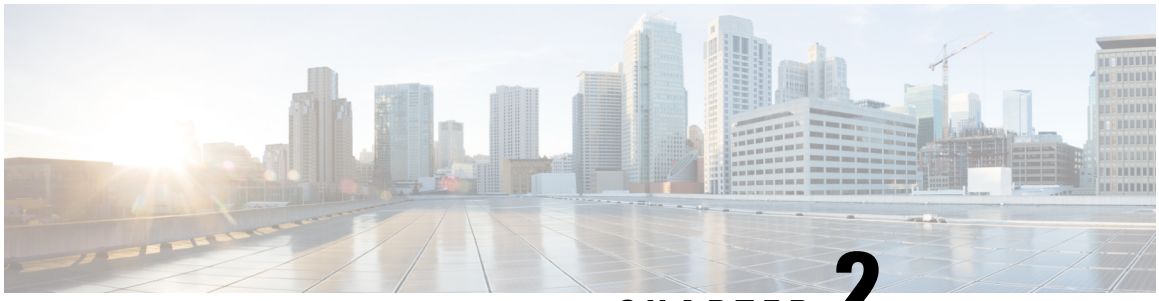
To disable IP access control and allow all IP addresses to access Catalyst Center, perform the following steps.

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.



CHAPTER 2

Manage Applications

- Application Management, on page 63
- Download and Install the Latest System Version, on page 63
- Download and Install the Latest System Version in Air Gap Mode, on page 70
- Download and Install Application Updates, on page 71
- Uninstall an Application, on page 72

Application Management

Catalyst Center provides many of its functions as individual applications, packaged separately from the core infrastructure. This enables you to install and run the applications that you want and uninstall those you are not using, depending on your preferences.

The number and type of application packages shown in the **Software Management** window vary depending on your Catalyst Center version and your Catalyst Center licensing level. All the application packages that are available to you are shown, whether or not they are currently installed.

Some applications are so basic that they are required on nearly every Catalyst Center deployment. For a description of a package, click the **Currently Installed Applications** link and place your cursor over its name.

Each Catalyst Center application package consists of service bundles, metadata files, and scripts.

Note We do not recommend to use CLI command for any package management activities, if package install or upgrade is not working from the Catalyst Center GUI, do not use any CLI command, instead contact Cisco TAC for assistance.

Download and Install the Latest System Version

The **Software Management** window indicates the latest Catalyst Center version available.

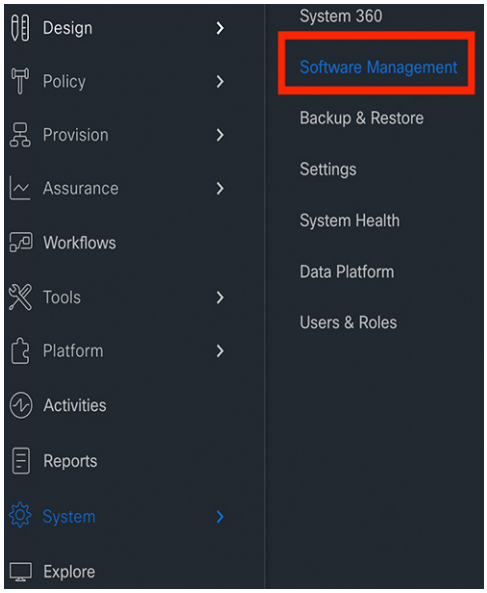
Complete the following procedure to download and install the latest version.

Before you begin

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

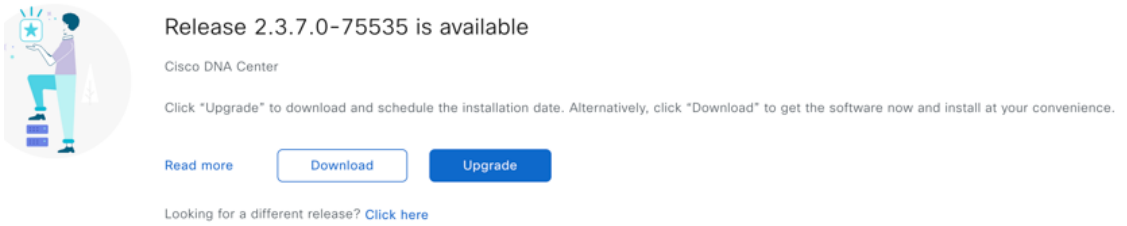
Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Note At this point, Catalyst Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window doesn't display a system update that's currently available.



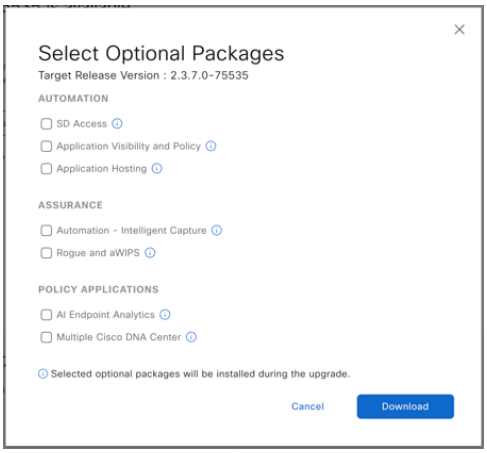
Step 2 If the window indicates that a system update is available, click one of the following options:

a. Click **Download** to download the system update.

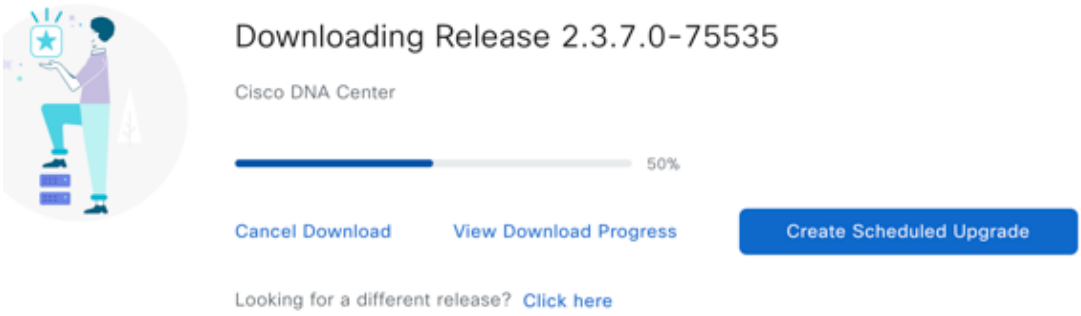


Do the following in the **Download** dialog box, which lists the applications that are currently available:

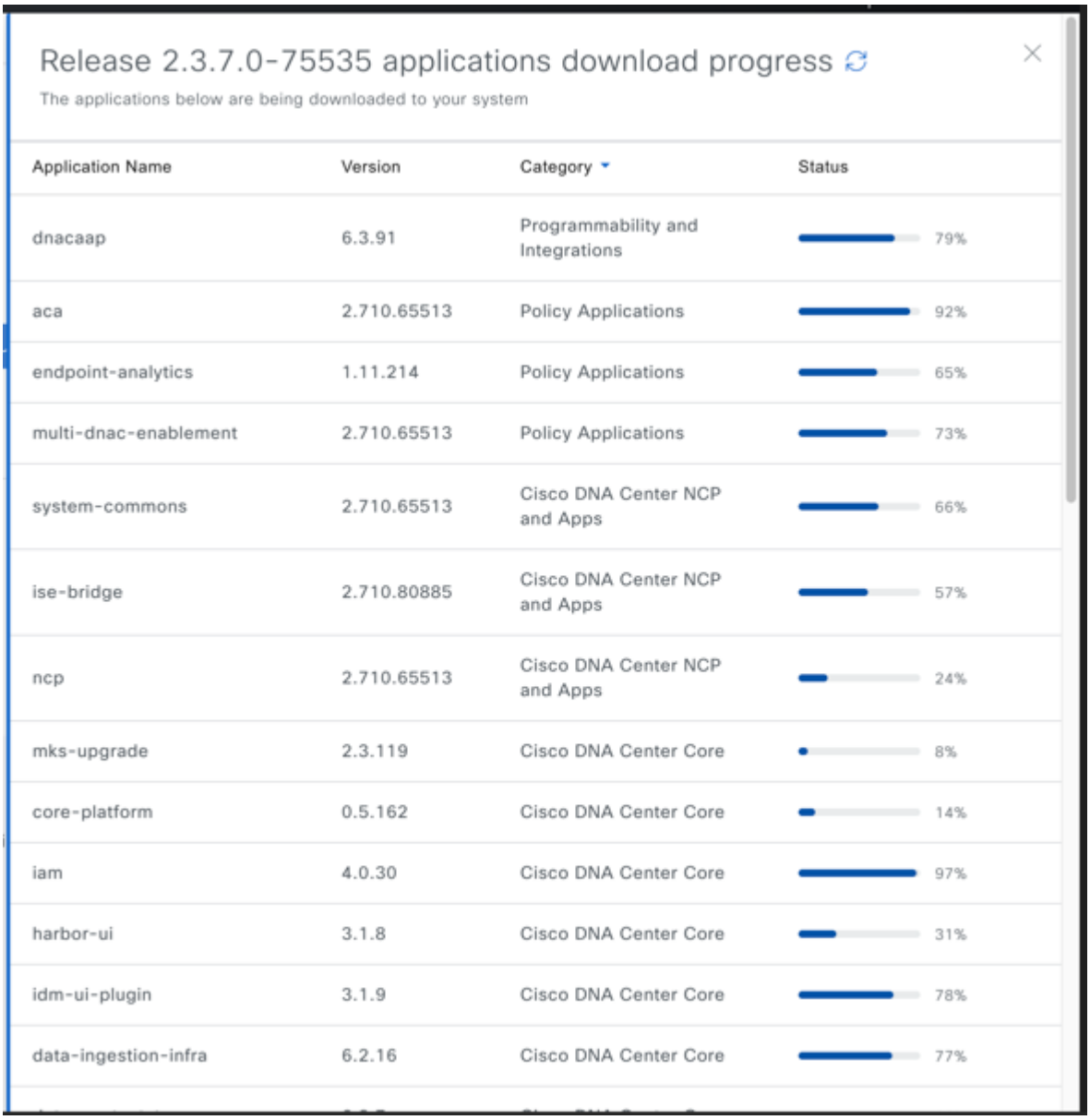
1. Check the check box for the application that you want to install.
2. Click **Download**.



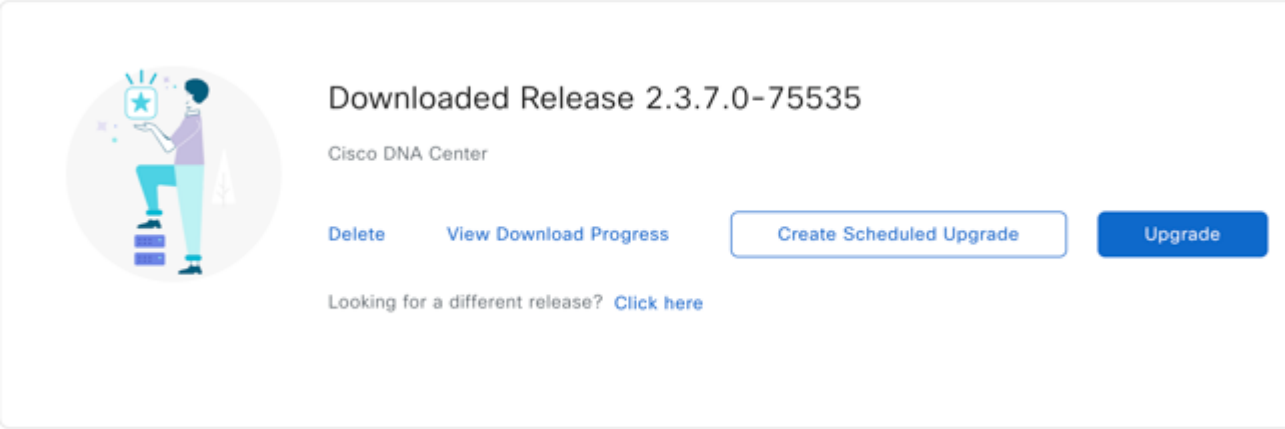
A download progress bar is displayed on the **Software Management** window.



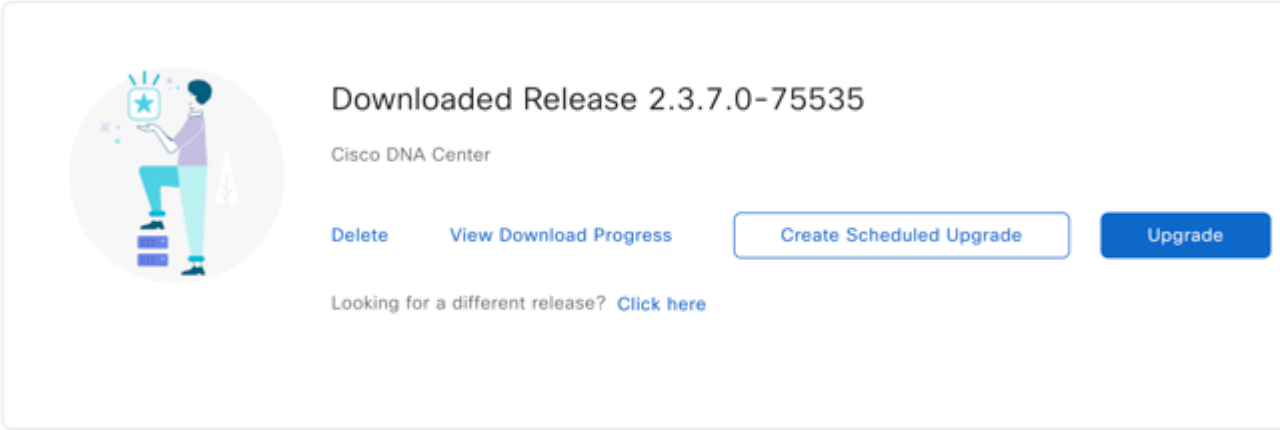
3. Click **View Download Progress** to view the progress of the packages that are being downloaded. The slide-in pane displays the progress of the individual applications.



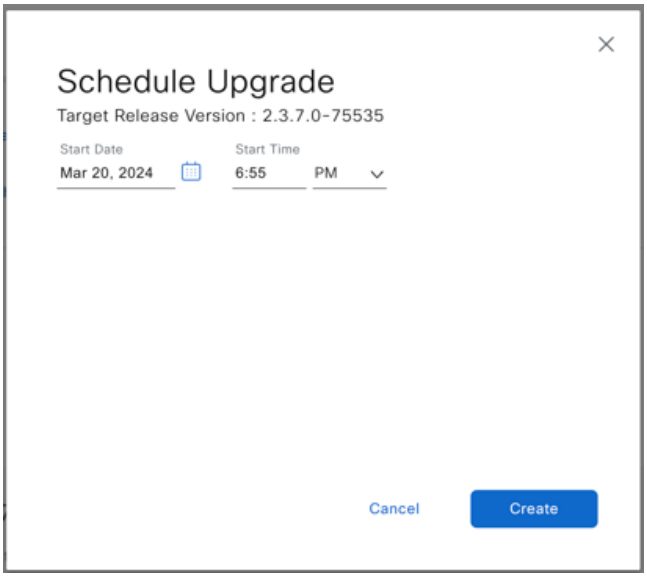
4. Click the **Delete** button if you want to delete the downloaded files.



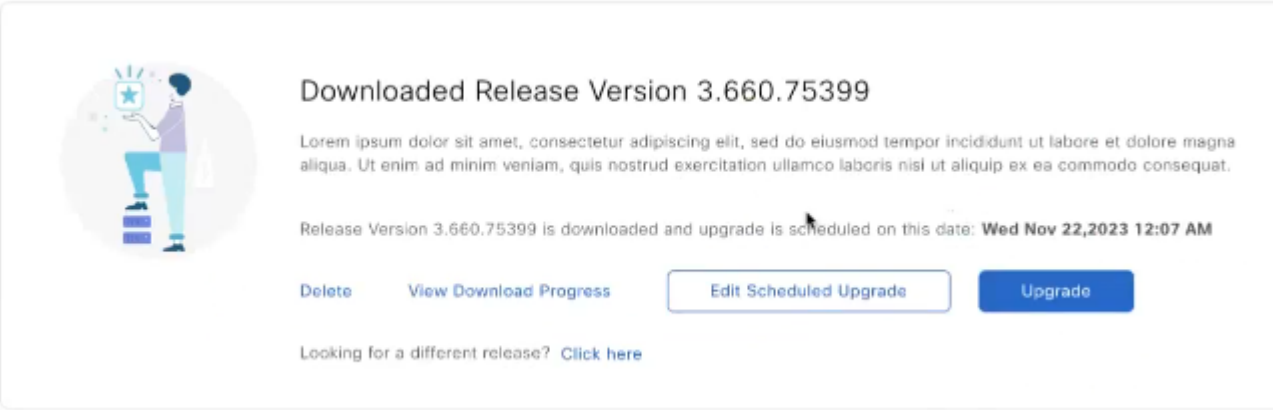
5. Click **Create Scheduled Upgrade** to schedule the date and time for the upgrade to take place.



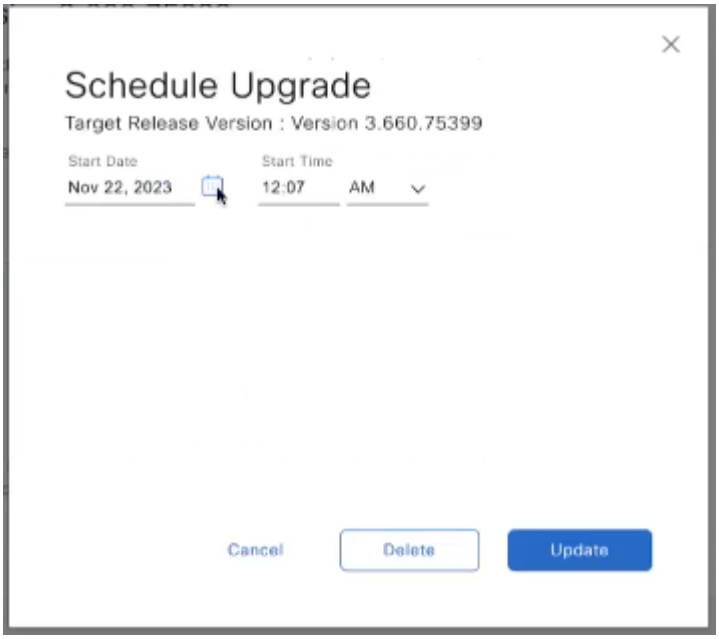
Schedule the upgrade, then click **Create**.



6. Do the following to edit or delete the scheduled upgrade:
   a. Click **Edit Scheduled Upgrade** to edit or delete the scheduled upgrade.

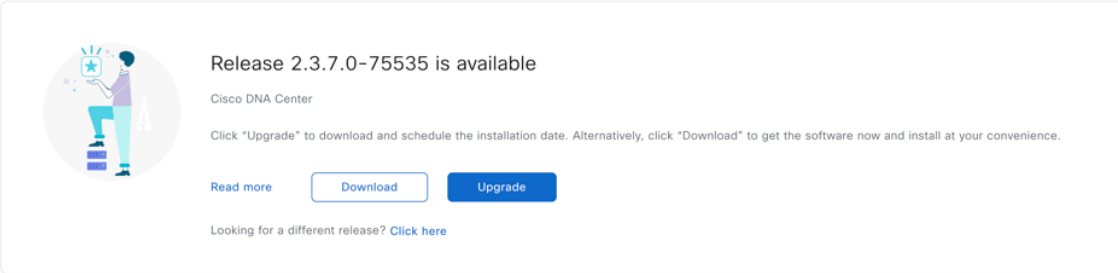


   b. To edit the scheduled upgrade, change the date and time of the schedule and click **Update**.



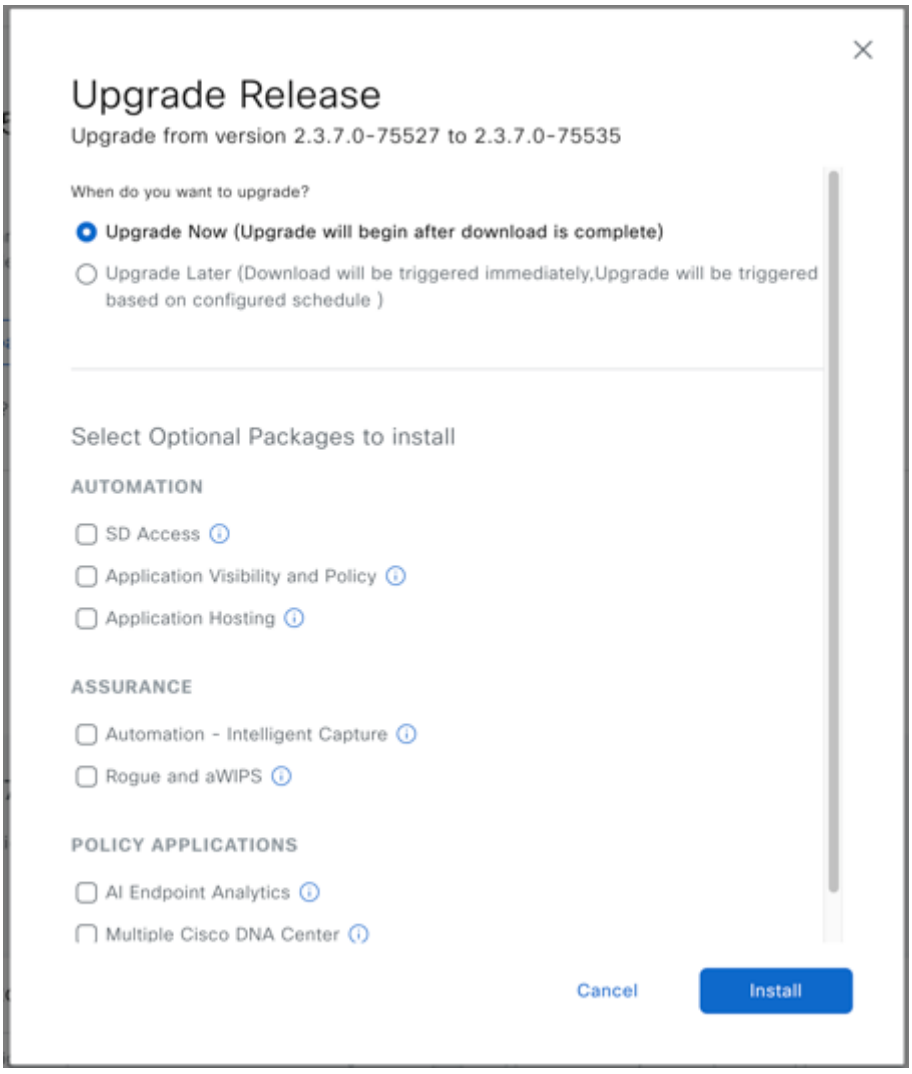
   c. To delete the scheduled upgrade, click **Delete**.

b. Click **Upgrade** to download the latest system version and perform the upgrade.



Choose one of the following options in the **Upgrade Release** dialog box:

- **Upgrade Now**: After choosing this option, click **Install**. All of the packages for the latest release are downloaded. After the download completes, the upgrade is triggered automatically.



- **Upgrade Later**: Choose this option to begin the download of packages for the latest release immediately. You'll then be able to configure when the upgrade will take place.

Do the following in the **Upgrade Release** dialog box:

1. The dialog box lists the available application packages. To install an application, check the check box next to the application.
2. Click **Install**.

Note Catalyst Center enters Maintenance mode during the upgrade and remains unavailable while the system update takes place. After the update completes, log back in to Catalyst Center.

After the system upgrade is complete, a message at the top of the window indicates that your system is up to date.

Step 3 In the **Software Management** window, click **View Installed Applications** to view the applications that are currently installed. You can do the following on this window:

- Check the check box next to the optional application that you want to uninstall and click **Uninstall**.
- Click **Activities** on the top-right corner to view the changes that are made to the system. You can view the system upgrade or download details, the applications installed or uninstalled, and a timestamp of the activity.

  Click the **Execution ID** to view details of an activity.

Download and Install the Latest System Version in Air Gap Mode

The system upgrade is completed by connecting to the internet and using the online update process. However, in some cases, the upgrade is maintained strictly within internal networks (that is, within an air-gapped environment). This upgrade may be necessary to support additional security or regulatory requirements.

Note With the Air Gap mode enabled, you can do the following:

- Communicate with only private IP subnets.
- Add IP address ranges to pass through the air-gapped environment by using the provided API.
- Switch between Air Gap mode and Cloud mode.

Before you begin

Air Gap mode must be enabled on the cluster. For information about how to enable Air Gap mode, see the *Cisco Catalyst Center Air Gap Deployment Guide*.

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

Step 2 Access the air gap directory on the restricted shell and copy the air gap tarball from the predetermined location using the following SCP command:

```
scp -P 2222 <airgap tar file> maglev@<cluster_ip>:airgap/
```

If it is a three-node cluster, you can copy the file to any node.

Step 3 In the top-right corner of the **Software Management** window, click **Scan** to view the latest available software release.

Step 4 To download the files and schedule the upgrade for a later time, do the following:

a) Click **PreLoad**.

b) In the **Schedule Upgrade** dialog box, schedule the system upgrade and click **PreLoad**.

On the successful submission, a banner message at the top of the window displays the scheduled date and time of the system upgrade.

c) Click the ellipsis at the end of the banner message to edit or delete the scheduled system upgrade. You can also choose to upgrade the schedule immediately.

Step 5 To download the latest version and upgrade the system immediately, do the following:

a) Click **Upgrade**.

b) In the dialog box, from the listed available package applications, check the check box next to application to install the application.

c) Click **Install**.

Note Catalyst Center enters maintenance mode during the upgrade and remains unavailable while the system update takes place.

After the system upgrade is complete, a message at the top of the window indicates that your system is up to date.

Note

- If the system can connect to the external cloud when the air gap mode is enabled, use the following command to verify the network policy:

```
sudo calicoctl get gnp allow-outbound-external -o yaml
```

- Use the following command to verify if ALM has network mode as air gap:

```
kubectl get pods -n maglev-control-plane alm-agent-8469679dfb-nvkxk -o yaml | grep -A1
 NETWORK_MODE
```

Note The above command can only be run from a full shell (_shell and consent token).

- Use the following command to get the scan status and logs:

```
kubectl get pods -n maglev-control-plane | grep ef-airgap-seed
```

- Use the following command to get the preload status and logs:

```
kubectl get pods -n maglev-control-plane | grep ef-airgap-scan
```

Download and Install Application Updates

Catalyst Center treats individual applications as separate from the core infrastructure. Specifically, individual packages for applications can be installed to run on Catalyst Center.

Packages for applications may take time to install and deploy. Therefore, install the packages during a maintenance period for your network.

Before you begin

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

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

Note At this point, Catalyst Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window doesn't display the application updates that are currently available.

Step 2 If any application updates are available, they are displayed at the bottom of the window. Do one of the following:

a. To install all the available application updates, click the **Select All** link.

b. To install individual application updates, check the appropriate check boxes.

Step 3 Click **Install**.

Note During installation, dependencies are checked and installed automatically.

The window displays a progress bar for each application that's being updated.

Step 4 Click the **Currently Installed Applications** link and confirm that the applications you selected have been updated.

Step 5 In the **Software Management** window, click **Activities** to view a list of changes made to the system. You can view the system upgrade or download details, the applications installed or uninstalled, and a timestamp of the activity.

Step 6 Under the **Actions** column, click the ellipsis to view the tasks that occurred during the execution of the activity.

Uninstall an Application

Catalyst Center treats individual applications as separate from the core infrastructure. Specifically, individual packages for applications can be uninstalled from Catalyst Center.

You can uninstall only packages for applications that are not system critical.

Before you begin

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

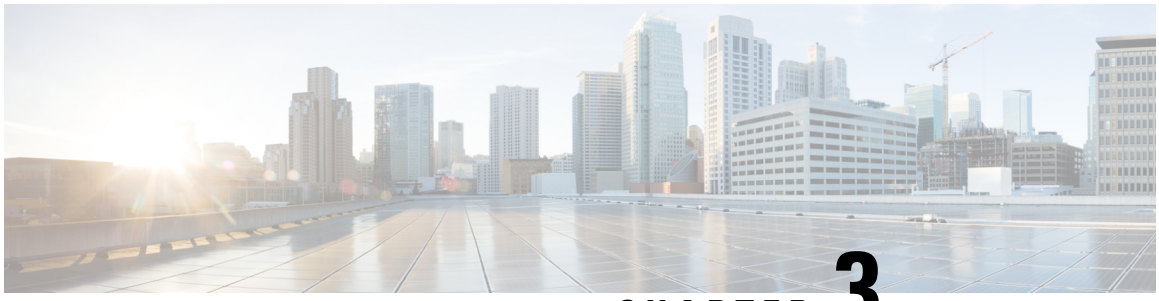
Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Step 2 Click the **Currently Installed Applications** link to view all the applications that are installed on your Catalyst Center appliance.

Step 3 Check the package you want to remove and click **Uninstall**.

Note
- You can uninstall multiple packages simultaneously.
- You can uninstall only the optional packages.

Catalyst Center displays a message after the application has been removed.



CHAPTER 3

Manage Users

- About User Profiles, on page 73
- About User Roles, on page 73
- Create an Internal User, on page 74
- Edit a User, on page 74
- Delete a User, on page 75
- Reset a User Password, on page 75
- Change Your Own User Password, on page 76
- Change Your Own User Password Without Admin Permission, on page 76
- Reset a Forgotten Password, on page 76
- Configure Role-Based Access Control, on page 76
- Display Role-Based Access Control Statistics, on page 82
- Configure External Authentication, on page 82
- Two-Factor Authentication, on page 84
- Display External Users, on page 88

About User Profiles

A user profile defines the login, password, and role (permissions) of a user.

You can configure both internal and external profiles for users. Internal user profiles reside in Catalyst Center, and external user profiles reside on an external AAA server.

A default user profile with SUPER-ADMIN-ROLE permissions is created when you install Catalyst Center.

About User Roles

Users are assigned user roles that specify the functions that they are permitted to perform:

- **Administrator (SUPER-ADMIN-ROLE)**: Users with this role have full access to all of the Catalyst Center functions. They can create other user profiles with various roles, including those with the SUPER-ADMIN-ROLE.
- **Network Administrator (NETWORK-ADMIN-ROLE)**: Users with this role have full access to all of the network-related Catalyst Center functions. However, they do not have access to system-related functions, such as backup and restore.

- **Observer (OBSERVER-ROLE)**: Users with this role have view-only access to the Catalyst Center functions. Users with an observer role cannot access any functions that configure or control Catalyst Center or the devices it manages.

Create an Internal User

You can create a user and assign this user a role.

Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **User Management**.

Step 2 Click **Add**.

Step 3 Enter a first name, last name, email address, and username for the new user.

The email address must meet the requirements for the standard Apache EmailValidator class.

Step 4 Under **Role List**, choose one of the following roles: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.

Step 5 Enter a password and confirm it. The password must contain:

- At least eight characters
- A character from at least three of the following categories:
  - Lowercase letter
  - Uppercase letter
  - Number
  - Special character

Step 6 Click **Save**.

Edit a User

You can edit some user properties (but not the username).

Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to edit.

Step 3 Click **Edit**.

Step 4 Edit the first or last name or email address, if needed.

Step 5 Under **Role List**, choose a new role, if needed: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.

Step 6 Click **Save**.

Delete a User

Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to delete.

Step 3 Click **Delete**.

Step 4 At the confirmation prompt, click **Continue**.

Reset a User Password

You can reset another user's password.

For security reasons, passwords are not displayed to any user, not even to the users with administrator privileges.

Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user whose password you want to reset.

Step 3 From the **More Actions** drop-down list, click **Reset Password**.

Step 4 Enter a new password and confirm it. The new password must contain:

- At least eight characters
- A character from at least three of the following categories:
  - Lowercase letter
  - Uppercase letter
  - Number

- Special character

Step 5 Click **Save**.

Change Your Own User Password

Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **Change Password**.

Step 2 Enter information in the required fields.

Step 3 Click **Update**.

Change Your Own User Password Without Admin Permission

The following procedure describes how to change your password without admin permission.

Step 1 From the top-right corner, click your displayed username and choose **My Profile and Settings** > **My Account**.

Step 2 In the **Password** field, click **Update Password**.

Step 3 In the **Update Password** dialog box, enter the new password and confirm the new password.

Step 4 Click **Update**.

Reset a Forgotten Password

If you forgot your password, contact the Cisco Technical Assistance Center (TAC) to reset it.

Configure Role-Based Access Control

Catalyst Center supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict user access to certain Catalyst Center functions.

Use this procedure to define a custom role and then assign a user to that role.

Before you begin

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

Step 1 Define a custom role.

a) From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **Role Based Access Control**.
b) Click **Create a New Role**.
The **Create a Role** window appears. If this is your first iteration of RBAC, after you have created the new role, you will be asked to assign users to the new role.
c) If a task overview window opens, click **Let's do it** to go directly to the workflow.
The **Create a New Role** window opens.
d) Enter a name for the role and then click **Next**.
The **Define the Access** window opens with a list of options. By default, the observer role is set for all Catalyst Center functions.
e) Click the > icon corresponding to the desired function to view the associated features.
f) Set the permission level to **Deny**, **Read**, or **Write** for the desired features.

If you set the permission level of a feature to **Deny**, the user to whom you assign this role cannot view this feature in the GUI.

g) Click **Next**.
The **Summary** window opens.
h) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
If you click **Edit**, the **Role-Name** window opens.

Step 2 To assign a user to the custom role you just created, click **Add Users**.

The **User Management** window opens, which allows you to assign the custom role to an existing user or to a new user.

- To assign the custom role to an existing user, do the following:
  a. In the **Internal Users** window, click the radio button next to the user to whom you want to assign the custom role, and then click **Edit**.

  The **Update Internal User** slide-in pane opens.

  b. From the **Roles** drop-down list, choose the custom role, and then click **Save**.

- To assign the custom role to a new user, do the following:
  a. Click **Add**.

  The **Create Internal User** slide-in pane opens.

  b. Enter the first name, last name, and username in the fields provided.

  c. From the **Roles** drop-down list, choose the custom role to assign to the new user.

  d. Enter the password and then confirm it.

  e. Click **Save**.

Step 3 If you are an existing user who was logged in when the administrator was updating your access permissions, you must log out of Catalyst Center and then log back in for the new permission settings to take effect.

Catalyst Center User Role Permissions

Table 2: Catalyst Center User Role Permissions

Capability	Description
Assurance	Assure consistent service levels with complete visibility across all aspects of your network.
Monitoring and Troubleshooting	Monitor and manage the health of your network with issue troubleshooting and remediation, proactive network monitoring, and insights driven by AI Network Analytics. This role lets you: • Resolve, close, and ignore issues. • Run Machine Reasoning Engine (MRE) workflows. • Analyze trends and insights. • Troubleshoot issues, including path trace, sensor dashboards, and rogue management. • Run workflows for rogue and Cisco Advanced Wireless Intrusion Prevention System (aWIPS). These workflows include AP-allowed list, vendor-allowed list, aWIPS profile creation, assigning an aWIPS profile, and so on.
Monitoring Settings	Configure and manage issues. Update network, client, and application health thresholds. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.
Troubleshooting Tools	Create and manage sensor tests. Schedule on-demand forensic packet captures (Intelligent Capture) for troubleshooting clients. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.
Network Analytics	Manage network analytics-related components.
Data Access	Enable access to query engine APIs. Control functions such as global search, rogue management, and aWIPS. Note: Setting the permission to Deny affects Search and Assurance functionality.
Network Design	Set up the network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
Advanced Network Settings	• Update network settings, such as global device credentials, authentication and policy servers, certificates, trusted certificates, cloud access keys, Stealthwatch, Umbrella, and data anonymization. • Export the device inventory and its credentials. Note: To complete this task, you must have Write permission on **Network Settings**.
Image Repository	Manage software images and facilitate upgrades and updates on physical and virtual network entities.
Network Hierarchy	Define and create a network hierarchy of sites, buildings, floors, and areas based on geographic location. Users with this role can also add CMX servers in **System** > **Settings**.

Capability	Description
Network Profiles	Create network profiles for routing, switching, and wireless. Assign profiles to sites. This role includes CLI Templates, Tagging, Feature Templates, and Authentication Template. Note: To create SSIDs, you must have Write permission on **Network Settings**.
Network Settings	Common site-wide network settings such as AAA, NTP, DHCP, DNS, Syslog, SNMP, and Telemetry. Users with this role can add an SFTP server and modify the Network Resync Interval in **System** > **Settings**. Note: To create wireless profiles, you must have Write permission on **Network Profiles**. To assign a CMX server to a site, building, or floor, you must have Write permission on **Network Hierarchy**.
Virtual Network	Manage virtual networks (VNs). Segment physical networks into multiple logical networks for traffic isolation and controlled inter-VN communication.
Network Provision	Configure, upgrade, provision, and manage your network devices.
Compliance	Manage compliance provisioning.
EoX	Scan the network for details on publicly announced information pertaining to the **End of Life**, **End of Sales**, or **End of Support** of the hardware and software in your network. Note: To view EoX scans, you must have Read permission on **Compliance**. To run EoX scans, you must have Write permission on **Compliance**.
Image Update	Upgrade software images on devices that don't match the Golden Image settings after a complete upgrade lifecycle.
Inventory Management	Discover, add, replace, or delete devices on your network while managing device attributes and configuration properties. Note: To replace a device, you must have Write permission on **Network Provision** > **PnP**.
Inventory Management > Device Configuration	Device Configuration: Display the running configuration of a device.
Inventory Management > Discovery	Discovery: Discover new devices in your network.
Inventory Management > Network Device	Network Device: Add devices from Inventory, view device details, and perform device-level actions.
	Inventory Insights: Displays device issues, such as Speed/Duplex settings mismatch and VLAN mismatch, and the number of times each issue occurred. Provides detailed actions for users to perform to revolve the issues. Because this information requires action, including possible configuration changes, it is not displayed to users who have a read-only role.
Inventory Management > Port Management	Port Management: Allow port actions on a device.
Inventory Management > Topology	Topology: Display network device and link connectivity. Manage device roles, tag devices, customize the display, and save custom topology layouts. Note: To view the SD-Access Fabric window, you must have at least Read permission on **Network Provision** > **Inventory Management** > **Topology**.

Capability	Description
License	Unified view of your software and network assets relative to license usage and compliance. The role also controls permissions for cisco.com, Cisco credentials, device EULA, and Smart accounts.
Network Telemetry	Enable or disable the collection of application telemetry from devices. Deploy related settings, such as site telemetry receivers, wireless service assurance, and controller certificates, to devices. Note: To enable or disable the collection of application telemetry, you must have Write permission on **Provision**.
PnP	Automatically onboard new devices, assign them to sites, and configure them with site-specific contextual settings.
Provision	Provision devices with the site-specific settings and policies that are configured for the network. This role includes Fabric, Application Policy, Application Visibility, Cloud, Site-to-Site VPN, Network/Application Telemetry, Stealthwatch, Sync Start vs Run Configuration, and Umbrella provisioning. On the main dashboards for rogue and aWIPS, you can enable or disable certain actions, including rogue containment. To provision devices, you must have Write permission on **Network Design** and **Network Provision**.
Network Services	Configure additional capabilities on the network beyond basic network connectivity and access.
Application Hosting	Deploy, manage, and monitor virtualized and container-based applications running on network devices.
Bonjour	Enable the Wide Area Bonjour service across your network to enable policy-based service discovery.
Stealthwatch	Configure network elements to send data to Cisco Stealthwatch to detect and mitigate threats, even in encrypted traffic. To provision Stealthwatch, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Services** > **Stealthwatch** • **Network Design** > **Advanced Settings**

Capability	Description
Umbrella	Configure network elements to use Cisco Umbrella as the first line of defense against cybersecurity threats. To provision Umbrella, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Provision** > **Scheduler** • **Network Services** > **Umbrella** You must also have Read permission on **Advanced Network Settings**.
Platform	Open platform for accessible, intent-based workflows, data exchange, notifications, integration settings, and third-party app integrations.
APIs	Drive value by accessing Catalyst Center through REST APIs.
Bundles	Enhance productivity by configuring and activating preconfigured bundles for ITSM integration.
Events	Subscribe to get notified in near real time about network and system events of interest and initiate corrective actions. You can configure email and syslog logs in **System** > **Settings** > **Destinations**.
Reports	Generate reports using predefined reporting templates for all aspects of your network. Generate reports for rogue devices and for aWIPS. You can configure webhooks in **System** > **Settings** > **Destinations**.
Security	Manage and control secure access to the network.
Group-Based Policy	Manage group-based policies for networks that enforce segmentation and access control based on Cisco security group tags. This role includes Endpoint Analytics.
IP-Based Access Control	Manage IP-based access control lists that enforce network segmentation based on IP addresses.
Security Advisories	Scan the network for security advisories. Review and understand the impact of published Cisco security advisories that may affect your network.
System	Centralized administration of Catalyst Center, which includes configuration management, network connectivity, software upgrades, and more.
Machine Reasoning	Configure automatic updates to the machine reasoning knowledge base to rapidly identify security vulnerabilities and improve automated issue analysis.
System Management	Manage core system functionality and connectivity settings. Manage user roles and configure external authentication. This role includes Integrity Verification, HA, Disaster Recovery, Debugging Logs, Product Telemetry, System EULA, IPAM, Cisco AI Analytics, Backup & Restore, and Data Platform.

Capability	Description
Utilities	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.
Audit Log	Detailed log of changes made via UI or API interface to network devices or Catalyst Center.
Event Viewer	View network device and client events for troubleshooting.
Network Reasoner	Initiate logical and automated troubleshooting for network issues while drawing on the knowledge wealth of network domain experts.
Remote Device Support	Allow the Cisco support team to remotely troubleshoot the network devices managed by Catalyst Center. With this role enabled, an engineer from the Cisco Technical Assistance Center (TAC) can connect remotely to a customer's Catalyst Center setup for troubleshooting purposes.
Scheduler	Integrated with other back-end services, scheduler lets you run, schedule, and monitor network tasks and activities such as deploy policies, provision, or upgrade the network. You can also schedule rogue containment.
Search	Search for various objects in Catalyst Center, such as sites, network devices, clients, applications, policies, settings, tags, menu items, and more.

Display Role-Based Access Control Statistics

You can display statistics that show how many users belong to each user role. You can also drill down to view the list of users who have a selected role.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **Role Based Access Control**.

All default user roles and custom roles are displayed.

Step 2 Click the number corresponding to each user role to view the list of users who have that role.

Configure External Authentication

If you are using an external server for authentication and authorization of external users, you should enable external authentication in Catalyst Center.

Before you begin

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- You must configure at least one authentication server.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **External Authentication**.

Step 2 To enable external authentication in Catalyst Center, check the **Enable External User** check box.

Step 3 (Optional) Configure the AAA attribute.

For TACACS authentication, the following AAA attributes are supported:

Catalyst Center	TACACS
Empty	cisco-av-pair
cisco-av-pair	cisco-av-pair
Cisco-AVPair	Cisco-AVPair

For RADIUS authentication, the following AAA attributes are supported:

Catalyst Center	RADIUS
Empty	cisco-av-pair
Cisco-AVPair	cisco-av-pair

a) In the **AAA Attribute** field, enter the appropriate attribute for your use case, as described in the preceding tables. The default value of the **AAA Attribute** field is null.

b) Click **Update**.

Step 4 (Optional) Configure the AAA server or servers.

Configure these settings only if you want to swap the current primary or secondary AAA servers or define different AAA servers. From the top-left corner, click the menu icon and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers** to open the **Authentication and Policy Servers** window.

a) From the **Primary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.

b) From the **Secondary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.

c) (Optional) If you are using a Cisco ISE server, you can update the settings, if necessary.

For information about Cisco ISE policies, see "Configure and Manage Policies" in the *Cisco Identity Services Engine Administrator Guide*.

Table 3: Cisco ISE Server Settings

Name	Description
Shared Secret	Key for device authentications. The shared secret can contain up to 100 characters. The shared secret must be provided before the AAA address can be updated.
Username	Name that is used to log in to the Cisco ISE CLI.
Password	Password for the Cisco ISE CLI username.

Name	Description
FQDN	Fully qualified domain name (FQDN) of the Cisco ISE server. The FQDN consists of two parts, a hostname and the domain name, in the following format: *hostname.domainname.com* For example, the FQDN for a Cisco ISE server might be ise.cisco.com.
Subscriber Name	A unique text string—for example, `acme`—that is used during Catalyst Center-to-Cisco ISE integration to set up a new pxGrid client in Cisco ISE.
Virtual IP Address(es)	Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

d) (Optional) To update advanced settings, click **View Advanced Settings** and update the settings, if necessary.

Table 4: AAA Server Advanced Settings

Name	Description
Protocol	TACACS or RADIUS.
Authentication Port	Port used to relay authentication messages to the AAA server. • For RADIUS, the default is UDP port 1812. • For TACACS, the port is 49 and can't be changed.
Accounting Port	Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. • For RADIUS, the default UDP port is 1813. • For TACACS, the port is 49 and can't be changed.
Retries	Number of times that Catalyst Center can attempt to connect with Cisco ISE.
Timeout	Length of time that Catalyst Center waits for Cisco ISE to respond. The maximum timeout value is 60 seconds.

e) Click **Update**.

Two-Factor Authentication

Two-factor authentication, also known as 2FA, adds another layer of security to user verification by using an identifier method in addition to a user's name and password. The identifier method is generally something that only the actual intended user possesses (such as a phone app or keyfob) and is intentionally separated from the original login method.

The Catalyst Center implementation of two-factor authentication supports the use of a token client (that generates single-use token codes after the appropriate PIN is entered), a token server (that validates token codes), and an authentication server to manage user access. Authentication can be handled using either the RADIUS or TACACS+ protocol.

Prerequisites for Two-Factor Authentication

The following prerequisites must be in place to set up two-factor authentication for use with Catalyst Center:

- An authentication server that is able to return attribute-value pairs to convey RBAC role authorizations for authenticated Catalyst Center users. In our example, we use Cisco Identity Services Engine (Cisco ISE) 2.3 Patch 1.
- A two-factor token server that you will integrate with your authentication server. In our example, we use RSA Authentication Manager 7.2.
- A token card application on the client's machine that generates software tokens. In our example, we use RSA SecurID Software Token.

Two-Factor Authentication Workflow

Here is a summary of what happens when a user logs in to a Catalyst Center appliance on which two-factor authentication has been configured:

1. In an RSA SecurID token client, a user enters their PIN to get a token code.
2. In the Catalyst Center login page, they enter their username and token code.
3. Catalyst Center sends the login request to Cisco ISE using either the RADIUS or TACACS+ protocol.
4. Cisco ISE sends the request to the RSA Authentication Manager server.
5. RSA Authentication Manager validates the token code and informs Cisco ISE whether the user has been authenticated successfully.
6. If the user has been authenticated, Cisco ISE matches the authenticated user with their configured authorization profile and returns the **role=NETWORK-ADMIN-ROLE** attribute-value pair.
7. Catalyst Center grants access to the features and pages associated with the user's role-based access control (RBAC) role.

Configure Two-Factor Authentication

To configure two-factor authentication on your Catalyst Center appliance, complete the following procedure.

Step 1 Integrate RSA Authentication Manager with Cisco ISE:

a) In RSA Authentication Manager, create two users: **`example_admin`** (for the Admin user role) and **`example_observer`** (for the Observer role).

For more information, see the "Add a User to the Internal Database" topic in the RSA Self-Service Console Help. To access this topic, do the following:

1. Open the *RSA Self-Service Console Help*.
2. In the **Search help** field, enter **`Add a User to the Internal Database`** and then click **Search help**.

b) Create a new authentication agent.

For more information, see the "Add an Authentication Agent" topic in the *RSA Self-Service Console Help*.

c) Generate the Authentication Manager agent configuration file (sdconf.rec):

1. From the RSA Security Console, choose **Access** > **Authentication Agents** > **Generate Configuration File**.

   The **Configure Agent Timeout and Retries** tab opens.
2. For the **Maximum Retries** and **Maximum Time Between Each Retry** fields, use the default values.
3. Click **Generate Configuration File**.

   The **Download Configuration File** tab opens.
4. Click the **Download Now** link.
5. When prompted, click **Save to Disk** to save a local copy of the zip file.
6. Unzip the file and use this version of the sdconf.rec file to overwrite the version that is currently installed on the agent.

d) Generate a PIN for the **`example_admin`** and **`example_observer`** users that you created in Step 1a.

For more information, see the "Create My On-Demand Authentication PIN" topic in the *RSA Self-Service Console Help*.

e) Start Cisco ISE, choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**, and then click **Add**.

f) In the **RSA SecurID Identity Sources** page, click **Browse**, choose the sdconf.rec file you downloaded, and then click **Open**.

g) Check the **Reauthenticate on Change PIN** check box, then click **Submit**.

Step 2 Create two authorization profiles, one for the Admin user role and one for the Observer user role.

a) In Cisco ISE, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

b) For both profiles, enter the following information:

- **Name**: Enter the profile name.
- **Access Type**: Choose **ACCESS_ACCEPT**.
- **Advanced Attributes Settings** area: Choose **Cisco:cisco-av-pair** from the first drop-down list.

  If you are creating an authorization profile for the Admin user role, choose **Role=NETWORK-ADMIN-ROLE** from the second drop-down list.

  If you are creating an authorization profile for the Observer user role, choose **Role=OBSERVER-ROLE** from the second drop-down list.

Step 3 Create an authentication policy for your Catalyst Center appliance.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authentication Policies" topic.

Step 4 Create two authorization policies, one for the Admin user role and one for the Observer user role.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authorization Policies" topic.

Step 5 In the RSA Authentication Manager Security Console, verify that software tokens have been assigned to both users.

For more information, see the "View a Token" topic in the *RSA Self-Service Console Help*.

Note If you need to assign tokens, complete the steps described in the "Assign a Software Token to a User" topic.

Enable Two-Factor Authentication Using RADIUS

To enable two-factor authentication that uses a Cisco ISE server configured for RADIUS, complete the following procedure:

Step 1 Integrate Cisco ISE with Catalyst Center.

In the *Catalyst Center Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.

Step 2 Configure Catalyst Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important Ensure that you specify the same shared secret for both Cisco ISE and Catalyst Center.

Enable Two-Factor Authentication Using TACACS+

To enable two-factor authentication that uses a Cisco ISE server configured for TACACS+, complete the following procedure:

Step 1 In Cisco ISE, choose **Administration** > **Network Resources** > **Network Devices** to open the **Network Devices** window.

Step 2 Click **TACACS Authentication Settings** to view its contents. Ensure that a shared secret has already been configured for the Catalyst Center device that you added previously.

Step 3 Choose **Work Centers** > **Device Administration** > **Policy Elements** to open the **TACACS Profiles** window.

Step 4 Create TACACS+ profiles for the example_admin and example_observer user roles:

a) Click **Add**.

b) Complete the following tasks:

- Enter the profile name.
- After clicking the **Raw View** tab, enter the following text into the **Profile Attributes** text box:
  - For the example_admin user role, enter `Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE`
  - For the example_observer user role, enter `Cisco-AVPair=ROLE=OBSERVER-ROLE`

c) Click **Save**.

Step 5 Integrate Cisco ISE with Catalyst Center.

In the *Catalyst Center Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.

Step 6 Configure Catalyst Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important Ensure that you specify the same shared secret for both Cisco ISE and Catalyst Center.

Log In Using Two-Factor Authentication

To log in to Catalyst Center using two-factor authentication, complete the following procedure:

Step 1 From the Catalyst Center login page, enter the appropriate username.

Step 2 Open the RSA SecurID token client and enter the PIN you configured previously to generate a one-time token.

Step 3 Copy this token and paste it into the **Password** field of the Catalyst Center login page.

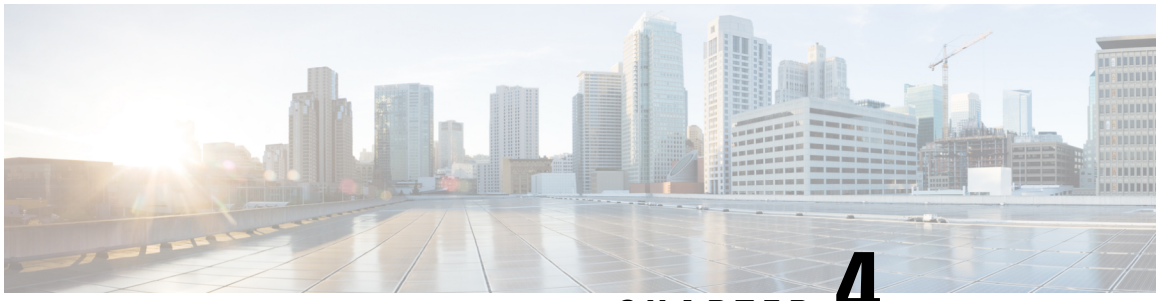
Step 4 Click **Log In**.

Display External Users

You can view the list of external users who have logged in through RADIUS or TACACS for the first time. The information that is displayed includes their usernames and roles.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **External Authentication**.

Step 2 Scroll to the bottom of the window, where the **External Users** area lists the external users.



CHAPTER 4

Manage Licenses

- License Manager Overview, on page 89
- Integration with Cisco Smart Accounts, on page 92
- Set Up License Manager, on page 93
- Visualize License Usage and Expiration, on page 94
- View Historical Trends for License Consumption, on page 95
- View License Details, on page 96
- Change License Level, on page 97
- Auto Registration of Smart License-Enabled Devices, on page 98
- Day 0 Configuration for Smart License-Enabled Devices, on page 98
- Apply Specific License Reservation or Permanent License Reservation to Devices, on page 99
- Cancel SLR or PLR Applied to Devices, on page 101
- Install the Authorization Code and Enable the High Security License, on page 101
- Disable the High Security License, on page 102
- Upload Resource Utilization Details to CSSM, on page 102
- Change Device Throughput, on page 103
- Transfer Licenses Between Virtual Accounts, on page 103
- Manage Customer Tags on Smart License-Enabled Devices, on page 104
- Modify License Policy, on page 104

License Manager Overview

The Catalyst Center License Manager feature helps you visualize and manage all of your Cisco product licenses, including Smart Account licenses. From the top-left corner, click the menu icon and choose **Tools** > **License Manager**. The **License Manager** window contains tabs with the following information:

- **Overview**:
  - Switch: Shows purchased and in-use license information for all switches.
  - Router: Shows purchased and in-use license information for all routers.
  - Wireless: Shows purchased and in-use license information for all wireless controllers and APs.
  - ISE: Shows purchased and in-use license information for devices managed by Cisco Identity Services Engine (ISE).

- **Licenses**: The **License Summary** shows the total licenses purchased from Cisco Smart Software Management (CSSM), the number of licenses that are about to expire, and out-of-compliance details for all types of licenses for all Cisco devices.
- **Devices**: The **Devices** table shows the license type, license expiry, license mode, virtual account, site, and registration status of each device managed by Catalyst Center.
- **Reporting**: The **Smart License Compliance** card allows you to launch the **Smart License Update** workflow.
- **Sync Status**: In a table, the Smart License Policy (SLP) compliance shows the devices and timeline graph of license usage reports sent from Catalyst Center to CSSM.

To manage licenses, you can use the controls shown above the table listings in each tab. The following table describes each of the controls.

Note Not all controls are available in every tab.

Table 5: License Management Controls

Control	Description
Filter	Click **Filter** to specify one or more filter values and then click **Apply**. You can apply multiple filters. To remove a filter, click the **x** icon next to the corresponding filter value.
Change Cisco DNA License	Select one or more licenses and choose **Actions** > **Change Cisco DNA License** to change the level of a selected Catalyst Center license to Essential or Advantage. You can also use this control to remove a Catalyst Center license. For more information, see Change License Level, on page 97.
Change Virtual Account	Select one or more licenses and choose **Actions** > **Change Virtual Account** to specify the Virtual Account used to manage these licenses.
Manage Smart License > Register	Select one or more Smart License-enabled devices and choose **Actions** > **Manage Smart License** > **Register** to register the Smart License-enabled devices.
Manage Smart License > Deregister	Select one or more Smart License-enabled devices and choose **Actions** > **Manage Smart License** > **Deregister** to unregister the Smart License-enabled devices.
Manage License Reservation > Enable License Reservation	Choose the device for which you want to apply Specific License Reservation (SLR) or Permanent License Reservation (PLR), then choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.
Manage License Reservation > Update License Reservation	The device must be in SLR registered state. You can update the SLR applied to a wireless device or switch with a wireless controller package. Choose the device for which you want to update SLR, then choose **Actions** > **Manage License Reservation** > **Update License Reservation**.
Manage License Reservation > Cancel/Return License Reservation	Choose the device and choose **Actions** > **Manage License Reservation** > **Cancel/Return License Reservation** to cancel or return the SLR or PLR applied to the device.

Control	Description
Manage License Reservation > Factory License Reservation	Choose the device and choose **Actions** > **Manage License Reservation** > **Factory License Reservation** to enable the factory-installed SLR on the device.
Recent Tasks	Click **Recent Tasks** to see a list of all 50 of the most recently performed Catalyst Center tasks. Use the drop-down to filter the list to show only those tasks with a status of **Success**, **Failure**, or **In Progress**.
License Usage	Click **License Usage** to see the license utilization percentage for all types of licenses.
Refresh	Click **Refresh** to reload the window with current data.
Find	Enter a search term in the **Find** field to find all licenses in the list that have that term in any column. Use the asterisk (*) character as a wildcard anywhere in the search string.
Show Records	Select the total number of records to display in each page of the table.

The Licenses table displays the information shown for each device. All of the columns support sorting. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

Note Not all columns are used in every tab. Also, some of the columns are hidden in the default column view setting. To view the hidden columns, click the gear icon and under **Edit Table Columns**, choose the columns you want displayed in the table.

Table 6: License Usage Information

Column	Description
Device Type: Device Series	Name of the device product series (for example, Catalyst 3850 Series Ethernet Stackable Switch). For more information, see View License Details, on page 96.
Device Type: Total Devices	The total number of devices in this product series that are under active management by Catalyst Center.
Purchased Licenses	The total number of purchased Catalyst Center subscription licenses for the devices in this product series.
Purchased Licenses: Network/Legacy	The total number of purchased Network (or Legacy) perpetual licenses for the devices in this product series.
Used Licenses	The total number of Catalyst Center subscription licenses applied to the devices in this product series.
Used Licenses: Network/Legacy	The total number of Network perpetual licenses for the devices in this product series.
Feature Licenses (applicable only for Routers)	The number of licenses purchased for specific features such as security, AVC, and so on.

Table 7: All License Information

Column	Description
Device Name	Name of the device. For more information, see View License Details, on page 96.
Device Family	The category of the device, such as Switches and Hubs, as defined by Catalyst Center.
IP Address	IP address of the device.
Device Series	The full name of the Cisco product series to which the listed device belongs (for example, Cisco Catalyst 3850 Series Ethernet Stackable Switch).
Catalyst Center License	The Catalyst Center license level.
Catalyst Center License Expiry	The expiration date of the Catalyst Center license.
License Mode	The Catalyst Center license mode.
Network License	The type of network license.
Virtual Account	The name of the Cisco Virtual Account managing the license for the device. The Virtual Account and the site hierarchy are distinct entities and are not interconnected.
Site	The Catalyst Center site where the device is located.
Registration Status	The registration status of the device.
Authorization Status	The authorization status of the device.
Reservation Status	The reservation status of the device.
Last Updated Time	The last time this entry in the table was updated.
MAC Address	The MAC address of the licensed device.
Term	The total term during which the Catalyst Center subscription license is in effect.
Days to Expiry	The number of days remaining until the Catalyst Center license term expires.
Software Version	The version of the network operating system currently running on the device.

Integration with Cisco Smart Accounts

Catalyst Center supports Cisco Smart Accounts, an online Cisco service that provides simplified, flexible, automated software- and device-license purchasing, deployment, and management across your organization. You can add multiple Cisco Smart Accounts.

When there are multiple Cisco Smart Accounts, one account is designated as the default, which the License Manager uses for visualization and licensing operations (such as registration, license level changes, and so on).

Virtual Accounts serve as subdivisions within a Cisco Smart Account, offering enhanced control over licenses and entitlements associated with the Smart Account. Virtual Accounts and the site hierarchy are distinct entities and are not interconnected.

After changing the default Cisco Smart Account, it takes several minutes to retrieve the data from CSSM and display it on the License Manager Overview and All License windows.

You can delete any Cisco Smart Accounts, except for the default account.

If you already have a Cisco Smart Account, you can use Catalyst Center to:

- Track your license consumption and expiration
- Apply and activate new licenses, without intervention
- Promote each device's license level from Essentials to Advantage (or vice versa) and reboot the device with the newly changed level of feature licensing
- Identify and reapply unused licenses

You can accomplish this automatically, without leaving Catalyst Center.

Set Up License Manager

You must set up access to your Cisco Smart Account before you can use the Catalyst Center License Manager tools.

Before you begin

- Ensure that you have SUPER-ADMIN-ROLE permissions and the appropriate RBAC scope to perform this procedure.
- Collect the Cisco user ID and password for your Smart Account.
- If you have multiple Smart Accounts, choose the Smart Account that you want to use with Catalyst Center, and collect that account's user ID and password.
- To enable a Smart Account, Catalyst Center must have reachability to tools.cisco.com.
- To apply licenses to a device in Catalyst Center, the device must be present in Inventory, must have a site assigned to it, and must have reachability to tools.cisco.com.
- Ensure that all allowed ports, FQDNs, and URLs listed in the *Cisco Catalyst Center Installation Guide* are allowed on any firewall or proxy.

Step 1 Log in using a Catalyst Center system administrator username and password.

Step 2 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Cisco.com Credentials**.

Step 3 Under **Cisco.com Credentials**, enter the username and password for your cisco.com account.

Step 4 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Smart Account**.

Step 5 Under **Smart Account**, click **Add** and enter the username and password for your Smart Account.

Step 6 Click **Save**.

Step 7 If you have multiple Smart Accounts, click **Add** and enter your additional accounts.

Step 8 If you have multiple Smart Accounts, choose one account to be the default. The License Manager uses the default account for visualization and licensing operations. To change the default Smart Account:

a) Click **Change** next to the selected Smart Account name.
b) Change the active Smart Account and choose a Smart Account to be the default.
c) Click **Apply**.
After changing the default account, it takes several minutes to retrieve the data from CSSM and display it on the License Manager Overview and All License windows.

Step 9 To edit a Smart Account, click the three dots in the Actions column and choose **Edit**.

Step 10 To delete a nondefault Smart Account, click the three dots in the Actions column and choose **Delete**.

Step 11 To access your Smart Account using a virtual or subordinate Smart Account name and password, under **Link Your Smart Account**, choose:

- **Use Cisco.com user ID** if your cisco.com and Smart Account credentials are the same.
- **Use different credentials** if your cisco.com and Smart Account credentials are different, and then enter your Smart Account credentials.

Step 12 Click **View all virtual accounts** to view all virtual Smart License Accounts.

What to do next

Register the Catalyst Center controller as a controller for Cisco Plug and Play Connect in a Cisco Smart Account, for redirection services. This also allows you to synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Catalyst Center Plug and Play. For more information, see in the *Cisco Catalyst Center User Guide*.

Visualize License Usage and Expiration

Catalyst Center can display graphical representations of your purchased licenses, how many of them are in use (that is, assigned to devices), and their duration.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager**.

Step 2 Select the type of device category for which you want to see the license usage: **Switches**, **Routers**, **Wireless**, **ISE**, **Licenses**, or **Reporting**.

The **License Usage** pie chart at the top of the window displays the aggregate number of purchased licenses and the number of licenses currently in use for the device category that you selected. The graphs also indicate the proportion of Essentials versus Advantage licenses within each total.

Under the graphs, the **License Usage** table shows subtotals for used and unused licenses, listed alphabetically by product family name.

Step 3 To see detailed comparisons for a particular product family, click the name of the product family in the **Device Series** column.

Catalyst Center displays details about the product family that you selected.

Step 4 To see a graphical representation of license duration, scroll down to the **License Timeline** section. The timeline graph for each product family is a visual representation of when the licenses in the configured Smart Account will expire for that product family.

View Historical Trends for License Consumption

Catalyst Center allows you to view historical trends for all purchased and consumed license consumptions in CSSM on a daily, weekly, and monthly basis. CSSM stores the historical information up to one year.

Before you begin

Catalyst Center must be registered to a particular smart account in CSSM. For more information, see Integration with Cisco Smart Accounts, on page 92.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Licenses**.

- The **License Summary** area shows the total number of purchased Catalyst Center subscription licenses from CSSM.
- The **Smart Account** area displays the details about the smart account.
- The **ESSENTIALS**, **ADVANTAGE**, and **PREMIER** area categorizes the number of **Total Licenses**, **About to Expire**, and **Out of Compliance** Catalyst Center subscription licenses.
- In the **License** window, a table filters your discovered devices and their licenses based on the following views from the **Focus** drop-down list:
  - Virtual Account View
  - Licenses View
  - Device Series View
  - Device Type View
  - License Type View

Step 2 To view the historical information of a chosen license, click the license link in the row for that device.

A license details slide-in pane shows the complete license details and license history of the chosen device.

Note The title of the license details slide-in pane matches the title of the chosen device.

Step 3 In the license details slide-in pane, choose the frequency of historical information from the **Frequency** drop-down list.

The available frequencies are:

- **Daily**: Displays the license data snapshot on the first day.
- **Weekly**: Displays the license data snapshot on Monday.
- **Monthly**: Displays the license data snapshot on the first day of the month.

Depending on the frequency selection a graph is displayed that shows the license data based on **Purchased**, **In Use**, and **Balance** licenses.

Depending on the frequency selection, the **License History** table filters the license historical information based on **Date**, **Purchased**, **In Use**, and **Balance**.

Note License historical information is always one day old, because CSSM provides this information from the previous data onwards. Catalyst Center periodically retrieves the license historical information from CSSM on a daily basis.

View License Details

There are many ways to find and view license details in Catalyst Center. For example, you can click the license usage and term graphs displayed in the **Switches**, **Routers**, **Wireless**, **ISE**, or **Devices** tabs in the **License Manager** window. Each graph displays pop-ups with aggregated facts about licenses for each of these product families.

The following method provides the comprehensive license details for a single device using the **Devices** table in the License Manager.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

The License Manager window displays a table listing all of your discovered devices and their licenses. Information in the table includes only basic device and license information, such as device type, license expiration dates, and so on.

Step 2 Scroll through the table to find the device whose license details you want to see. If you are having trouble finding the device you want, you can:

- Filter: Click ▽ and then enter your filter criteria in the appropriate field. (For example, enter all or part of the device name in the **Device Name** field.) You can enter filter criteria in multiple fields. When you click **Apply**, the table displays only the rows displaying information that matches your filter criteria.

  If you want to view the devices that belong to a particular site, navigate to the site in the left pane, and click the site. The devices are filtered accordingly. A site marker indicating the site hierarchy is displayed at the top of the page.

- Find: Click in the **Find** field and enter the text you want to find in any of the table columns. When you press **Enter**, the table scrolls to the first row with text that matches your entry in the **Find** field.

- Customize: Click the gear icon and under **Edit Table Columns**, choose the columns you want displayed in the table. For example, deselect **Device Series** or select **Days to Expiry**. When you click **Apply**, the table displays only the columns you selected.

Step 3 When you find the device that you want, click the **Device Name** link in the row for that device.

Catalyst Center displays the **License Details** slide-in pane with complete license details and license history for the device that you selected. **Actions** displays actions that can be performed on the device or its licenses.

When you are finished, click ✖ to close the **License Details** slide-in pane.

Change License Level

You can upgrade or downgrade the feature level of your device licenses. You can do this with Catalyst Center (subscription) licenses. Your feature level choices are either the basic Essentials level or the comprehensive Advantage level. (Note that network license conversion is available for products in the Cisco Catalyst 9000 device family only and network license conversion is handled implicitly when the Catalyst Center license level is changed.)

Whenever you change a device's license level, Catalyst Center automatically downloads and applies your licenses behind the scenes, using your Smart Account.

Because applying a license level change requires a device reboot, License Manager prompts you to confirm that you want to reboot the device when the license level change is complete. You can choose not to reboot with the license change, but you will need to schedule the reboot for later, or your license level change will not be applied.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

The License Manager window displays a table listing all of your discovered devices and their licenses.

Step 2 Use **Find** or scroll through the table to find the devices whose license level you want to change. If you are having trouble finding the device you want, or want to select multiple devices, follow the tips in View License Details, on page 96 to change the table to display only the devices you want.

Step 3 Check the check box next to each device for which you want to change the license level, then choose **Actions** > **Change License** > **Change Cisco DNA License**.

Catalyst Center displays a **Change Cisco DNA License Level** window for the license type that you want to change.

Step 4 Click the license level that you want for these devices: **Essentials** or **Advantage**. To remove the license from the device, click **Remove**.

Step 5 Click **Continue**. Catalyst Center asks if you want the change to be applied immediately or later. You must also choose whether you want to reboot the device when its license status is updated.

To continue:

- If you are not ready to make the change: Click **Back** to change your License Level selection, or click ✖ to close the window and cancel the change.
- If you are ready to make the change immediately: Click **Now**, then click **Confirm**. The device using this license will reboot when the change is applied.
- If you want the change to be applied later: Click **Later**, enter a name for the scheduled task, and specify the date and time when you want the change to be applied. If you want the change to take place as scheduled in the time zone of the site where the device is located, click **Site Settings**. When you are finished specifying the schedule parameters, click **Confirm**.

Auto Registration of Smart License-Enabled Devices

You can enable auto registration of Smart License (SL)-enabled devices. When auto registration is enabled, any SL-enabled devices added to Catalyst Center are automatically registered to the chosen virtual account.

Note This feature does not support Smart Licensing Using Policy (SLUP) enabled devices that runs on Cisco IOS-XE software version, 17.3.1.

Step 1 Log in using a Catalyst Center system administrator username and password.

Step 2 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Cisco Accounts** > **Smart Account**.

Step 3 Click **License**.

Step 4 Check the **Auto register smart license enabled devices** check box.

Step 5 Choose a virtual account.

Step 6 Click **Apply**.

Day 0 Configuration for Smart License-Enabled Devices

Devices that are already added to Catalyst Center before enabling auto registration aren't automatically registered. You can view the Smart License-enabled devices that aren't registered in the **All Licenses** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

The **License Manager** window displays a banner message with the number of SL-enabled devices that aren't auto registered and a table listing all of your discovered devices and their licenses with a link to set up auto registration.

Alternatively, you can filter the unregistered devices by using the **Registration Status** column.

Step 2 Choose the SL-enabled devices that you want to register and choose **Actions** > **Manage Smart License** > **Register**.

Step 3 Choose the virtual account and click **Continue**.

Step 4 To register the devices:

- If you want to register the devices immediately, choose **Now** and click **Confirm**.
- If you want to register the devices later, choose **Later** and specify a date and time. After specifying the schedule parameters, click **Confirm**.

Apply Specific License Reservation or Permanent License Reservation to Devices

Smart Licensing requires a smart device instance to regularly sync with Cisco Smart Software Management (CSSM) so that the latest license status is refreshed and compliance is reported. Some customers have devices that are within highly secured networks with limited internet access. In these types of networks, devices cannot regularly sync with CSSM and show out of compliance. To support these customer environments, Specific License Reservation (SLR) and Permanent License Reservation (PLR) have been introduced. The License Manager enables Catalyst Center customers to reserve licenses securely from CSSM using an API-based workflow. In Catalyst Center, it requires a one-time connectivity to CSSM in the staging environment, then the devices never need to connect to Cisco in SLR or PLR mode. If no connectivity to CSSM or staging is possible, you can resort to the manual SLR/PLR workflow available in CSSM.

SLR lets you install a node-locked license file (SLR authorization code) on a product instance. This license file enables individual (specific) licenses (entitlement tags).

PLR lets you install an authorization code that enables all licensed features on the product.

Both SLR and PLR require preapproval at the Smart Account level. Contact licensing@cisco.com for support.

To enable SLR or PLR when both the device and Catalyst Center are connected to CSSM, see Enable SLR/PLR When the Devices and Catalyst Center Are Connected to CSSM, on page 99.

To enable SLR or PLR when the device and Catalyst Center do not have connectivity to CSSM, see Enable SLR/PLR When the Devices and Catalyst Center Are Not Connected to CSSM, on page 100.

Enable SLR/PLR When the Devices and Catalyst Center Are Connected to CSSM

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

Step 2 Select the devices for which you want to apply SLR or PLR, and choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.

Step 3 Choose **Specific License Reservation (SLR)** or **Permanent License Reservation (PLR)** and click **Continue** to obtain the request codes for the selected devices.

Step 4 After the request codes are generated for the selected devices, click **Continue**.

Step 5 Choose a virtual account from which you want to reserve licenses and click **Continue** to generate the authorization codes for the selected devices.

Step 6 After the authorization codes are generated, do any of the following:

- To apply SLR immediately, choose the devices and click **Continue**.
- To apply SLR later, click **Apply Later**.

Step 7 Click **Confirm** to apply SLR/PLR to the selected device.

You can now view the updated status of the devices under **Reservation Status** on the **All Licenses** window.

Enable SLR/PLR When the Devices and Catalyst Center Are Not Connected to CSSM

Use this procedure to enable SLR/PLR for the devices that are not connected to CSSM.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

Step 2 Select the devices for which you want to apply SLR or PLR, and choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.

Step 3 Choose **Specific License Reservation (SLR)** or **Permanent License Reservation (PLR)** and click **Continue** to obtain the request codes for the selected devices.

You also can connect to the device through Telnet to obtain the request code.

Step 4 After the request codes are generated for the selected devices, click **Export**. This downloads the requestcodes.csv file, which contains the IP address, serial number of the device, and the request code.

Step 5 Save the file to your preferred location.

Step 6 Obtain the authorization code for each device from CSSM and update it in the CSV file. See Generate the Authorization Code from CSSM.

Step 7 Click the **Upload CSV** link.

Step 8 Click the **Select a file from your computer** link to select the saved CSV file.

Step 9 Click **Continue**.

Step 10 Choose a virtual account from which you want to reserve licenses and click **Continue**. SLR or PLR is applied to the selected devices.

You can now view the updated status of the devices under **Reservation Status** on the **All Licenses** window.

Generate the Authorization Code from CSSM

Before you begin

You must have Smart Account credentials to log in to CSSM.

Step 1 Log in to **CSSM**.

Step 2 Choose **Inventory** > **Licenses** > **License Reservation**. The Smart License Reservation wizard appears.

The **License Reservation** button is visible on the **Licenses** tab only if you have specific license reservation enabled for your Smart Account.

Step 3 In the **Step 1: Enter Request Code** tab, enter the request code in the **Reservation Request Code** field and click **Next**.

Step 4 In the **Step 2: Select Licenses** tab, check the **Reserve a specific license** check box.

Step 5 In the **Quantity to Reserve** field, enter the number of licenses that you want to reserve and click **Next**.

Step 6 In the **Step 3: Review and Confirm** tab, click **Generate Authorization Code**.

Step 7 Obtain the authorization code from the **Step 4: Authorize Code** tab.

Cancel SLR or PLR Applied to Devices

You can cancel or return the SLR or PLR that is applied to a device.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Licenses**.

Step 2 Click the device and choose **Actions** > **Manage License Reservation** > **Cancel/Return License Reservation**.

Step 3 Click **Cancel** to return the licenses.

You can view the updated status of the devices under **Reservation Status** on the **All Licenses** window.

Install the Authorization Code and Enable the High Security License

Cisco offers a throughput of 250 Mbps by default. To increase the device throughput to more than 250 Mbps, you must get the authorization code from Cisco. You can install the authorization code and enable the High Security (HSEC) license in a single workflow or in separate workflows, as required.

Before you begin

Ensure that the device is running Cisco IOS XE Release 17.3.2 or later.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Alternatively, you can use **Workflows** > **Smart License Compliance**.

Step 2 Click the **Smart License Compliance** card.

Step 3 In the **Smart License Update** window, click **Let's Do It**.

To skip this window in the future, check **Don't show this to me again**.

Step 4 In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.

Step 5 Click **Next**.

Step 6 In the **Choose Sites and Devices** window, choose the devices on which you want to install the authorization code and click **Next**.

Step 7 In the **Policy Settings** window, review the CSSM policies and click **Next**.

Step 8 In the **Choose Device Features** window, do the following:

a) Choose the devices.
b) From the **Auth Codes** drop-down list, choose **Install**.
c) From the **HSEC** drop-down list, choose **Enable**.
d) Click **Next**.

Step 9 In the **Review Device Features** window, click **Next**.

Step 10 In the **Installing Device Features** window, view the authorization code and HSEC installation status and click **Next**.

Step 11 In the **Sync Data with Cisco** window, click **Next**.

Step 12 In the **Summary** window, review the authorization code and HSEC installation status; then, click **Finish**.

Disable the High Security License

You can disable the HSEC license from a device if you don't want to consume the HSEC license unnecessarily.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Step 2 Click the **Smart License Compliance** card.

Step 3 In the **Smart License Update** window, click **Let's Do It**.

To skip this window in the future, check **Don't show this to me again**.

Step 4 In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.

Step 5 Click **Next**.

Step 6 In the **Choose Sites and Devices** window, choose the devices from which you want to disable the HSEC license and click **Next**.

Step 7 In the **Policy Settings** window, click **Next**.

Step 8 In the **Choose Device Features** window, do the following:

a) Choose the devices.
b) From the **HSEC** drop-down list, choose **Disable**.
c) Click **Next**.

Step 9 In the **Review Device Features** window, click **Next**.

Step 10 In the **Installing Device Features** window, view the HSEC disable operation status and click **Next**.

Step 11 In the **Sync Data with Cisco** window, click **Next**.

Step 12 In the **Summary** window, click **Finish**.

Upload Resource Utilization Details to CSSM

You can upload resource utilization details to CSSM instantly or schedule an upload.

To upload resource utilization details to CSSM, devices don't have to have NETCONF enabled, and devices don't have to be added to the site.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Step 2 Click the **Smart License Compliance** card.

Step 3 In the **Smart License Update** window, click **Let's Do It**.

To skip this window in the future, check **Don't show this to me again**.

Step 4 In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.

Step 5 Click **Next**.

Step 6 In the **Choose Sites and Devices** window, choose the devices from which you want to retrieve the resource utilization details and click **Next**.

Step 7 To upload the resource utilization details instantly, click **Next** in the **Modify Policy** window. To modify the scheduled reporting frequency, do the following:

a) Under **Policy Settings**, click **Modify** corresponding to the **Reporting Interval** field.

b) In the **Change Reporting Interval** window, enter the value.

The reporting interval (in days) denotes the frequency of scheduled upload of resource utilization details from Catalyst Center to CSSM. The frequency of uploads can be increased but cannot be reduced below the minimum reporting frequency.

c) Click **Save**.

Step 8 In the **Sync Data with Cisco** window, click **Next**.

Step 9 In the **Summary** window, click **Finish**.

After successful synchronization of data with CSSM, Catalyst Center sends an acknowledgment to the devices.

What to do next

The number of devices for which the license usage reporting has failed is shown in a separate **Smart License Compliance** card with the **Retry** option. Click the **Smart License Compliance** card and redo the above procedure to send the license usage reports from the failed devices to CSSM.

Change Device Throughput

You can change the throughput of Smart License-enabled routers.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Step 2 Choose the device that you want to change.

Step 3 Click **More Actions** and choose **Change Throughput**.

Step 4 In the **Choose Throughput** window, choose the throughput value and click **Next**.

Step 5 In the **Apply Throughput** window, click **Next**.

Step 6 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the **Change Throughput** task status in the **Recent Task** window.

Transfer Licenses Between Virtual Accounts

You can transfer licenses between virtual accounts.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Licenses**.

Step 2 Choose the licenses that you want to transfer and click **Transfer Licenses**.

Step 3 In the **Transfer Licenses** window, choose the virtual account.

Step 4 Enter the **Transfer License Count** for each of the chosen licenses and click **Transfer**.

Step 5 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the **License Transfer** task status in the **Recent Task** window.

Manage Customer Tags on Smart License-Enabled Devices

You can add a maximum of four customer tags to a Smart License-enabled device to help identify telemetry data for a product instance. You can also update and delete the customer tags.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Step 2 Choose the devices on which you want to add customer tags.

Step 3 Click **More Actions** and choose **Manage Free Form Fields** to add, update, or delete customer tags.

Step 4 To add or update customer tags, do the following in the **Free Form Fields** window:

a) Enter the customer tags.
b) Click **Save**.

Step 5 To delete customer tags, do the following in the **Free Form Fields** window:

a) Click the delete icon for the customer tags that you want to delete.
b) Click **Save**.
c) In the **Warning** window, click **Continue**.

Step 6 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the **Manage Customer Tags** task status in the **Recent Task** window.

Modify License Policy

You can modify the reporting interval at which network devices report their feature usage to CSSM.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

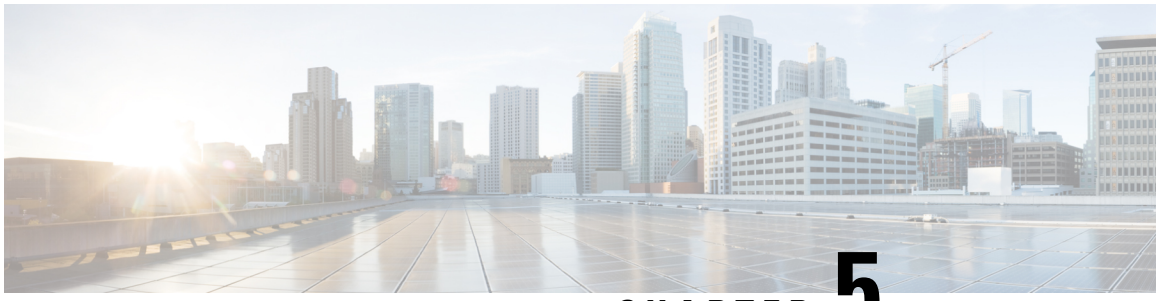
Step 2 In the **Smart License** table, click **Modify Policy**.

The **Modify Policy** window shows the policy settings and CSSM policy details.

Step 3 Under **Policy Settings**, click **Modify**.

Step 4 In the **Change Reporting Interval** window, enter the reporting interval value.

Step 5 Click **Save**.



CHAPTER 5

Backup and Restore

- About Backup and Restore, on page 107
- Backup and Restore Event Notifications , on page 109
- NFS Backup Server Requirements, on page 109
- Backup Physical Disk Nomenclature, on page 110
- Backup Storage Requirements, on page 110
- Add a Physical Disk for Backup and Restore, on page 111
- Add the NFS Server, on page 114
- Configure the Location to Store Backup Files, on page 115
- Create a Backup, on page 117
- Restore Data from Backups, on page 119
- Restore Data from a Physical Disk for a Faulty Virtual Appliance, on page 121
- Restore Data from an NFS Server for a Faulty Virtual Appliance, on page 127
- Schedule Data Backup, on page 130

About Backup and Restore

You can use the backup and restore functions to create the backup files and to restore to the same or different virtual appliance (if required for your network configuration).

Automation and Assurance data are unified to use a single data storage device. The data can be stored on a physical disk that is attached to the virtual machine or on a remote Network File System (NFS) server.

Backup

You can back up both automation and Assurance data.

Automation data consists of Catalyst Center databases, credentials, file systems, and files. The automation backup is always a full backup.

Assurance data consists of network assurance and analytics data. The first backup of Assurance data is a full backup. After that, backups are incremental.

Note Do not modify the backup files. If you do, you might not be able to restore the backup files to Catalyst Center.

Catalyst Center creates the backup files and posts them to a physical disk or an NFS server.

You can add multiple physical disks for backup. If the previous backup disk runs out of disk space, you can use the other added disks for backup. For information on how to add a physical disk, see Add a Physical Disk for Backup and Restore, on page 111. You must change the disk in the **System** > **Settings** > **Backup Configuration** window, and save changes for the new disk to be used as a backup location. For information on how to change the physical disk, see Configure the Location to Store Backup Files, on page 115.

You can also add multiple NFS servers for backup. For information on how to add an NFS server, see Add the NFS Server, on page 114. You must change the NFS server in the **System** > **Settings** > **Backup Configuration** window, and save changes for the new NFS server to be used as a backup location. For information on how to change the NFS server, see Configure the Location to Store Backup Files, on page 115.

Note Only a single backup can be performed at a time. Performing multiple backups at once is not supported.

When a backup is being performed, you cannot delete the files that have been uploaded to the backup server, and changes that you make to these files might not be captured by the backup process.

We recommend the following:

- Perform a daily backup to maintain a current version of your database and files.
- Perform a backup after making changes to your configuration, for example, when changing or creating a new policy on a device.
- Perform a backup only during a low-impact or maintenance period.

You can schedule weekly backups on a specific day of the week and time.

Restore

You can restore backup files from the physical disk or NFS server using Catalyst Center.

Catalyst Center on ESXi supports cross-version backup and restore; that is, you can create a backup on one version of Catalyst Center on ESXi and restore it to another version of Catalyst Center on ESXi. For example, a backup on Catalyst Center on ESXi 2.3.7.0-75530 version can be restored to Catalyst Center on ESXi 2.3.7.3-75176 version. The same applies to the later releases of Catalyst Center on ESXi.

Note A backup created on a virtual machine can only be restored on a virtual machine with the same or later software version.

When you restore the backup files, Catalyst Center removes and replaces the existing database and files with the backup database and files. While a restore is being performed, Catalyst Center is unavailable.

You can restore the backup files of a failed or faulty virtual appliance. For more information, see Restore Data from a Physical Disk for a Faulty Virtual Appliance, on page 121 and Restore Data from an NFS Server for a Faulty Virtual Appliance, on page 127.

Also, you can restore a backup to a Catalyst Center appliance with a different IP address.

Note After a backup and restore of Catalyst Center, you must access the **Integration Settings** window and update (if necessary) the **Callback URL Host Name** or **IP Address**.

Backup and Restore Event Notifications

You can receive a notification whenever a backup or restore event takes place. To configure and subscribe to these notifications, complete the steps described in the "Work with Event Notifications" topic of the *Cisco Catalyst Center Platform User Guide*. When completing this procedure, ensure that you select and subscribe to the SYSTEM-BACKUP and SYSTEM-RESTORE events.

Operation	Event
Backup	The process to create a backup file for your system has started.
	A backup file could not be created for your system. • This event typically happens because the necessary disk space is not available on remote storage. • You encountered connectivity issues or latency while creating a backup file on your system.
Restore	The process to restore a backup file has started.
	The restoration of a backup file failed. • This event typically happens because the backup file has become corrupted. • You encountered connectivity issues or latency while creating a backup file from your system.

NFS Backup Server Requirements

To support data backups on the NFS server, the server must be a Linux-based NFS server that meets the following requirements:

- Support NFS v4 and NFS v3. (To verify this support, from the server, enter **nfsstat -s**.)
- Have read and write permissions on the NFS export directory.
- Have a stable network connection between Catalyst Center on ESXi and the NFS server.
- Have sufficient network speed between Catalyst Center on ESXi and the NFS server.

Note You cannot use an NFS-mounted directory as the backup server. A cascaded NFS mount adds a layer of latency and is therefore not supported.

Requirements for Multiple Catalyst Center on ESXi Deployments

If your network includes multiple Catalyst Center clusters, the following example configuration shows how to name your NFS server backup directory structure:

Resource	Example Configuration
Catalyst Center on ESXi clusters	1. *cluster1* 2. *cluster2*
Backup server hosting automation and Assurance backups	The example directory is `/data/`, which has ample space to host both types of backups.

NFS export configuration	The content of the `/etc/exports` file:
	`/data/cluster1 *(rw,sync,no_subtree_check,all_squash)`
	`/data/cluster2 *(rw,sync,no_subtree_check,all_squash)`

Backup Physical Disk Nomenclature

To use a physical disk for backup, you must add a physical disk to the virtual machine. To easily identify the physical disks for backups, UUID is used.

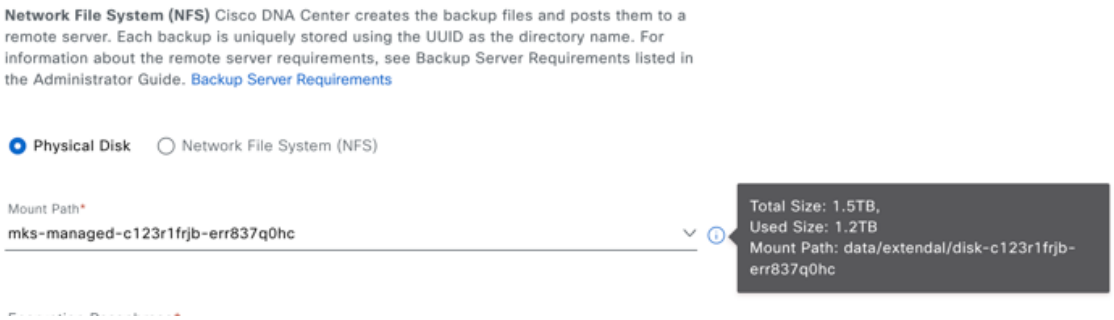
UUID is a unique identifier that is associated with the disk, which does not change across reboots. A disk that is removed and added to a different cluster will have the same UUID, as long as it is not formatted again.

The disk is explicitly labeled as `mks-managed`.

You can view the physical disks available for backup in the **System** > **Settings** > **Backup Configuration** window, under the **Mount Path** drop-down list.

Hover over the **i** icon to view the physical disk nomenclature, which is shown in the following format:

```
/data/external/disk-<uuid>
```



Backup Storage Requirements

Catalyst Center on ESXi stores backup copies of Assurance and automation data on a physical disk that is attached to the virtual machine or a remote NFS server. You must allocate enough external storage for your backups to cover the required retention. We recommend the following storage.

Virtual Appliance	Assurance Data Storage (14 Days Incremental)	Automation Data Storage (Daily Full)	Physical Disk/NFS Server (Assurance and Automation) Storage
DN-SW-APL	1.75 TB	50 GB	1.75 TB + 50 GB

Additional notes:

- The preceding table assumes fully loaded virtual appliance configurations that support the maximum number of access points and network devices for each appliance.
- The automation backup sizing is estimated for one daily backup. If you want to retain backups for additional days, multiply the required storage by the additional number of days. For example, if you have a DN-SW-APL virtual appliance and you want to store five copies of automation data backups generated once each day, the total storage required is 5 * 50 GB = 250 GB.
- The total backup time varies depending on your daily data load and the amount of historical data that you want to retain.
- The write path to Catalyst Center depends on the network throughput from Catalyst Center to the NFS server. The NFS server must have a throughput of at least 100 MB/sec.
- As with any other IT service, monitoring NFS performance is required to ensure optimal performance.

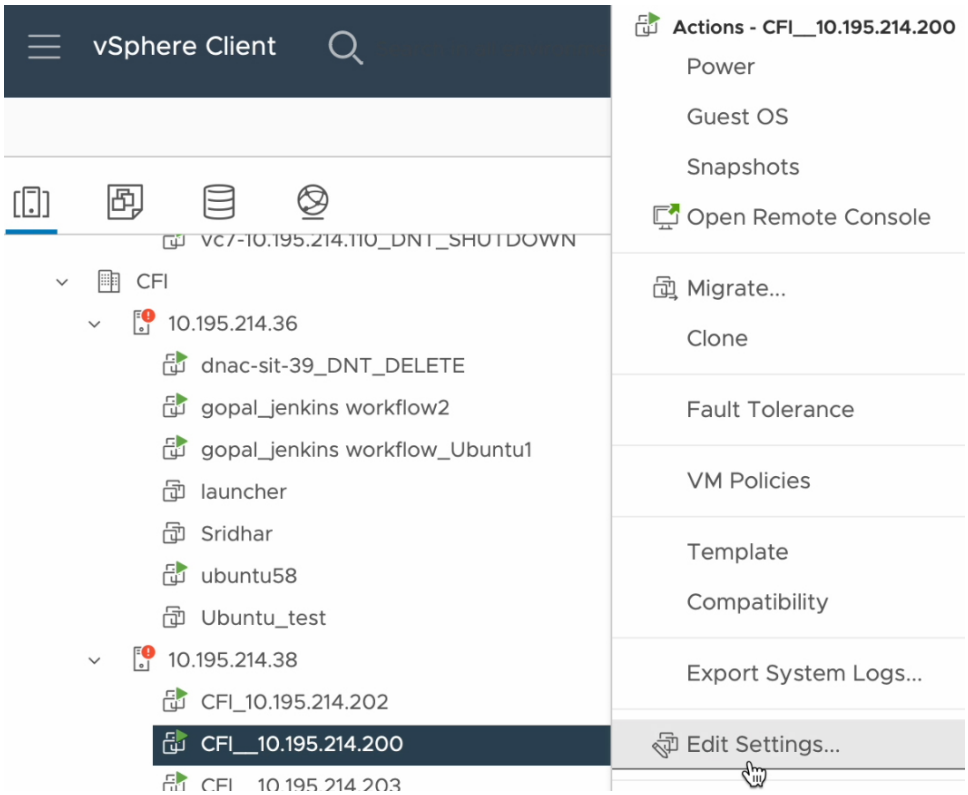
Add a Physical Disk for Backup and Restore

Use this procedure to add a physical disk that can be used for backup and restore operations.

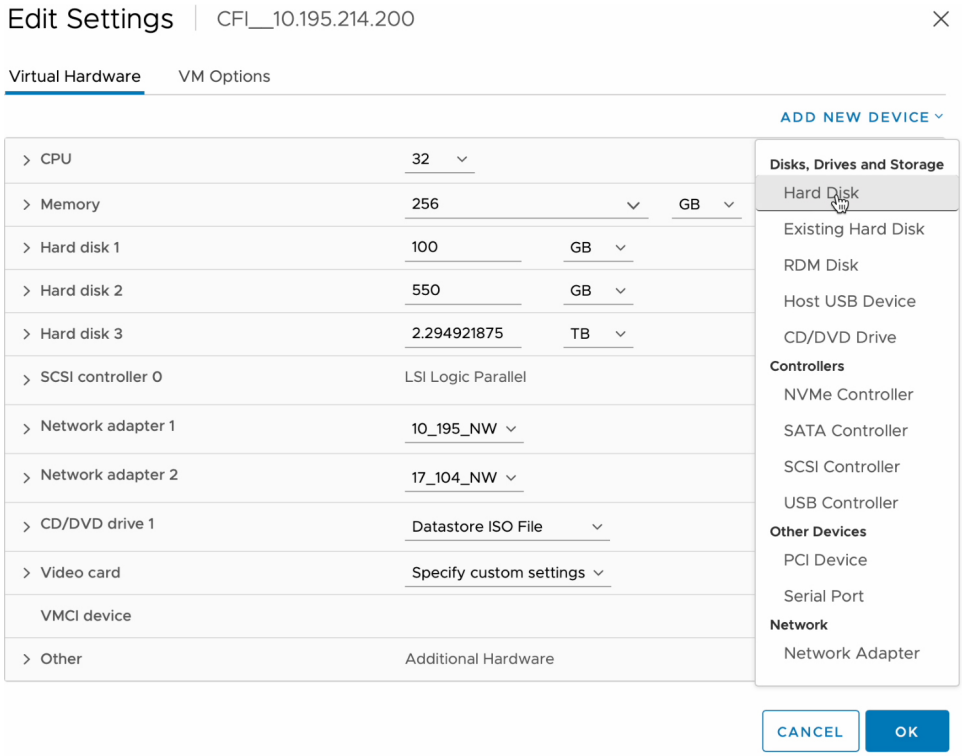
Step 1 If your appliance is running on the machine that's hosting Catalyst Center on ESXi, power off the appliance's virtual machine.

Step 2 Log in to VMware vSphere.

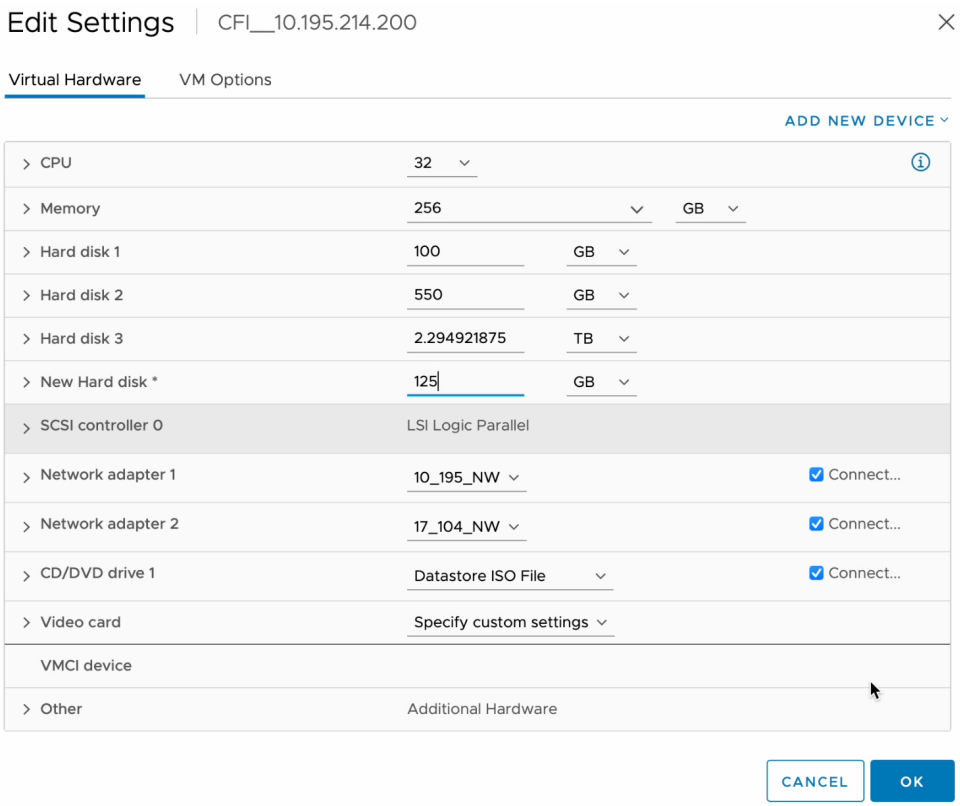
Step 3 From the vSphere client's left pane, right-click the ESXi host and then choose **Edit Settings**.



Step 4 In the **Edit Settings** dialog box, click **Add New Device** and then choose **Hard Disk**.



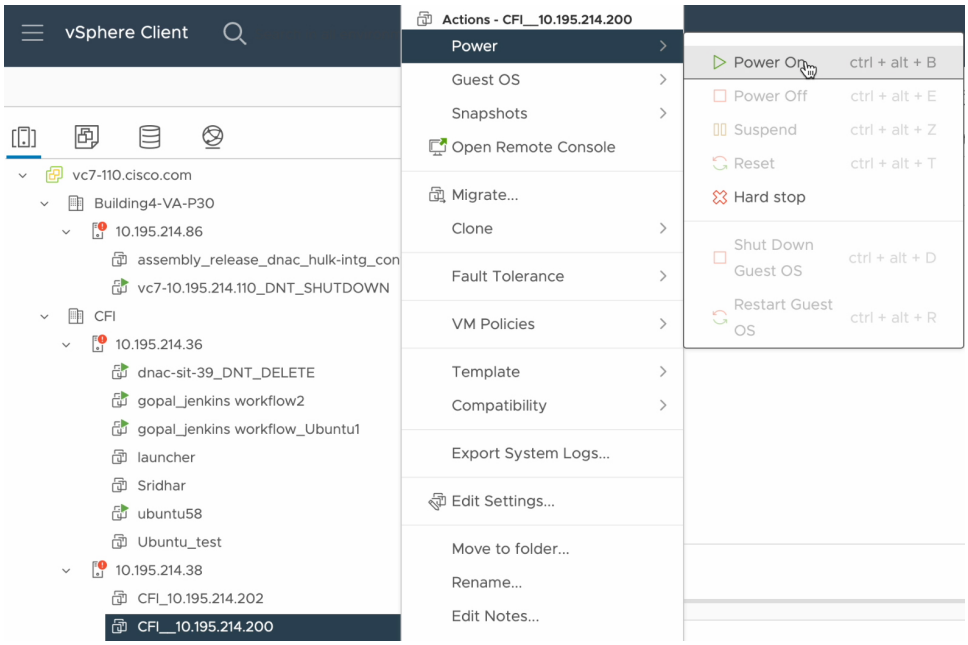
Step 5 In the **New Hard disk** field, enter the desired storage size.



Note For information on the recommended storage space for backup, see Backup Storage Requirements, on page 110.

Step 6 Click **OK**.

Step 7 Power on the appliance's virtual machine.



What to do next

You can now configure the added physical disk for backup. For information on how to configure the physical disk, see Configure the Location to Store Backup Files, on page 115.

Add the NFS Server

Catalyst Center allows you to add multiple Network File System (NFS) servers for backup purposes. Use this procedure to add an NFS server that can be used for the backup operation.

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

Step 2 Click **Add NFS**.

Step 3 In the **Add NFS** slide-in pane, do the following:

a) Enter the **Server Host** and **Source Path** in the respective fields.
b) Choose **NFS Version** from the drop-down list.
c) The **Port** is added by default. You can leave the field empty.
d) (Optional) Enter the **Port Mapper** number.
e) Click **Save**.

Step 4 Click **View NFS List** to view the available NFS servers.

The **NFS** slide-in pane displays the list of NFS servers, along with details.

Step 5 In the **NFS** slide-in pane, click the ellipsis under **Actions** to **Delete** the NFS server.

Note You can delete the NFS server only when there is no backup job in progress.

What to do next

Configure the added NFS server for backup. For more information, see Configure the Location to Store Backup Files, on page 115.

Configure the Location to Store Backup Files

Catalyst Center allows you to configure backups for automation and Assurance data.

Use this procedure to configure the storage location for backup files.

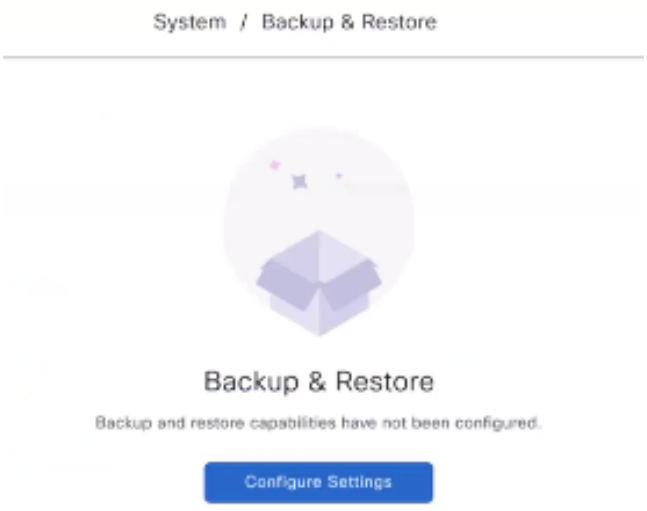
Before you begin

Make sure that the following requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in NFS Backup Server Requirements, on page 109.

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

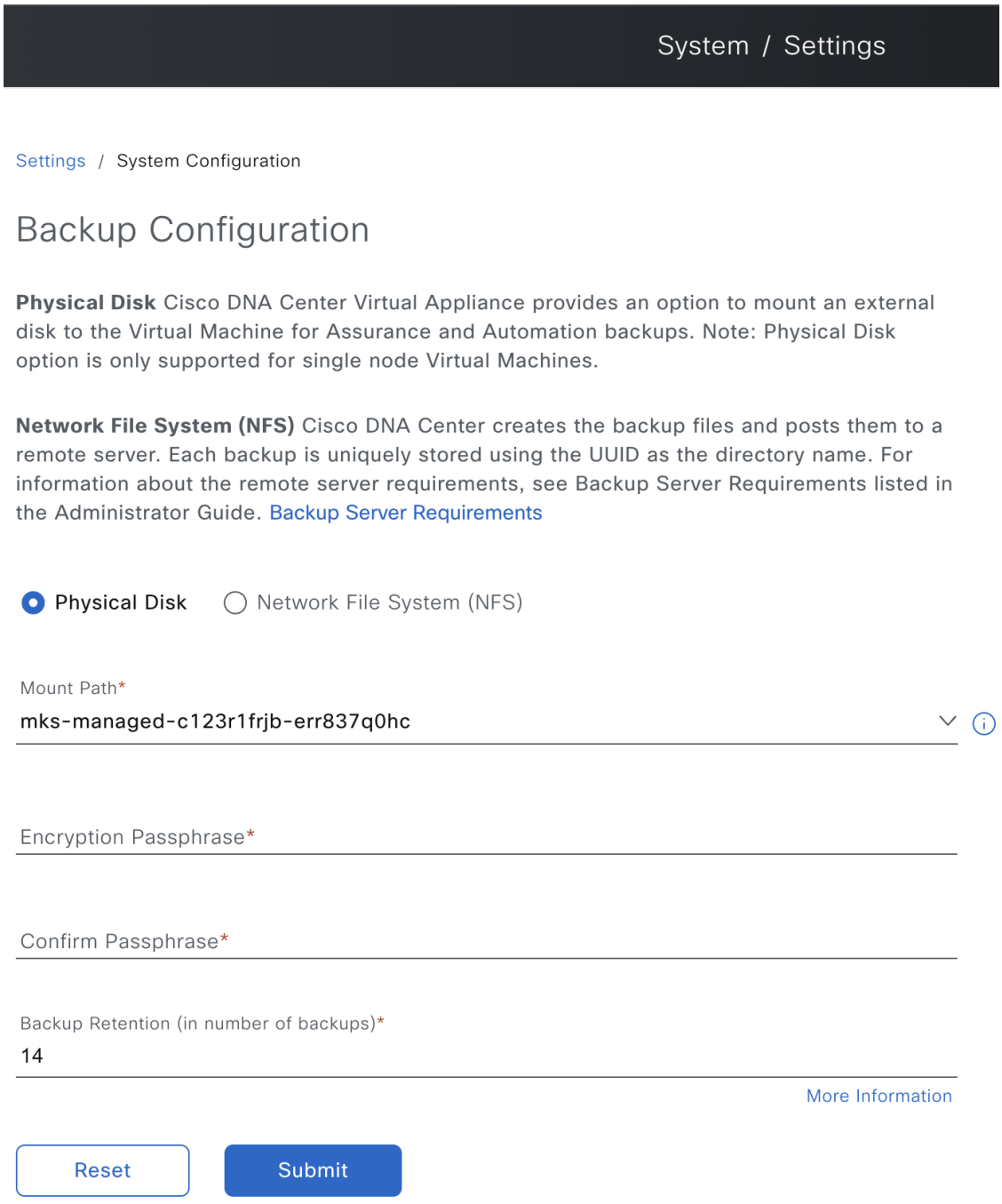
You can view the following window:



Step 2 Click **Configure Settings**.

Alternatively, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

Step 3 Choose the **Physical Disk** or **NFS** server option.



Step 4 **Physical Disk**: Catalyst Center provides an option to mount an external disk to the virtual machine, to store a backup copy of Assurance and automation data. To configure a physical disk, click the **Physical Disk** radio button and define the following settings:

Note The physical disk option is only supported for single-node virtual machines.

Field	Description
Mount Path	Location of the external disk.
Encryption Passphrase	Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials. This passphrase is required, and you will be prompted to enter this passphrase when restoring the backup files. Without this passphrase, backup files are not restored. After the passphrase is configured, if you want to change the passphrase, click **Update Passphrase**.
Backup Retention	Number of backups for which the data is retained. Data older than the specified number of backups is deleted.

Step 5 **NFS**: Catalyst Center creates the backup files and posts them to a remote NFS server. For information about the remote server requirements, see NFS Backup Server Requirements, on page 109. To configure an NFS backup server, click the **NFS** radio button and define the following settings:

Field	Description
Mount Path	Location of the remote server.
Encryption Passphrase	Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials. This passphrase is required, and you will be prompted to enter this passphrase when restoring the backup files. Without this passphrase, backup files are not restored. After the passphrase is configured, if you want to change the passphrase, click **Update Passphrase**.
Backup Retention	Number of backups for which the data is retained. Data older than the specified number of backups is deleted.

Step 6 Click **Submit**.

After the request is submitted, you can view the configured physical disk or NFS server under **System** > **Backup & Restore**.

Create a Backup

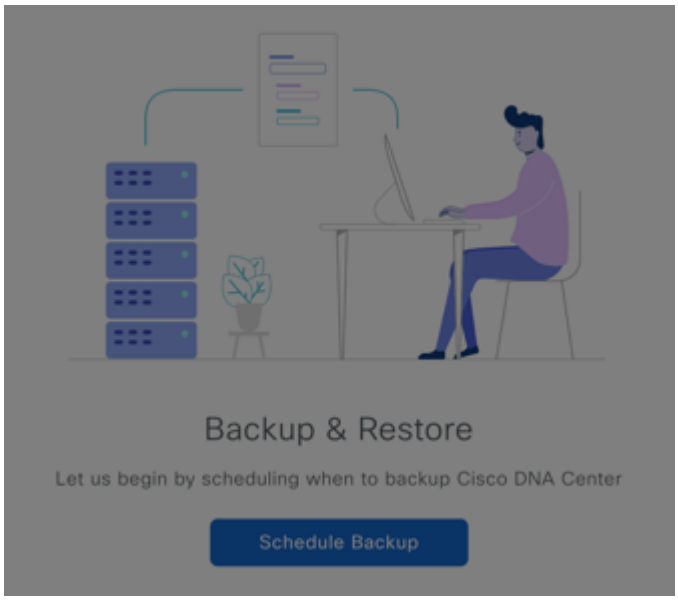
Use this procedure to create a backup of your virtual appliance.

Before you begin

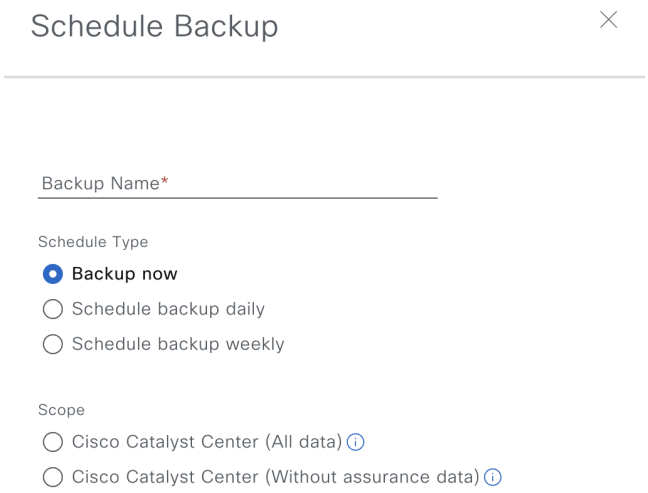
You must configure the backup location. For more information, see Configure the Location to Store Backup Files, on page 115.

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

Step 2 Click **Schedule Backup**.



The **Schedule Backup** slide-in pane opens.



Do the following in the **Schedule Backup** slide-in pane:

a. Enter a unique name for the backup.

b. In the **Schedule Type** area, choose one of the following options:

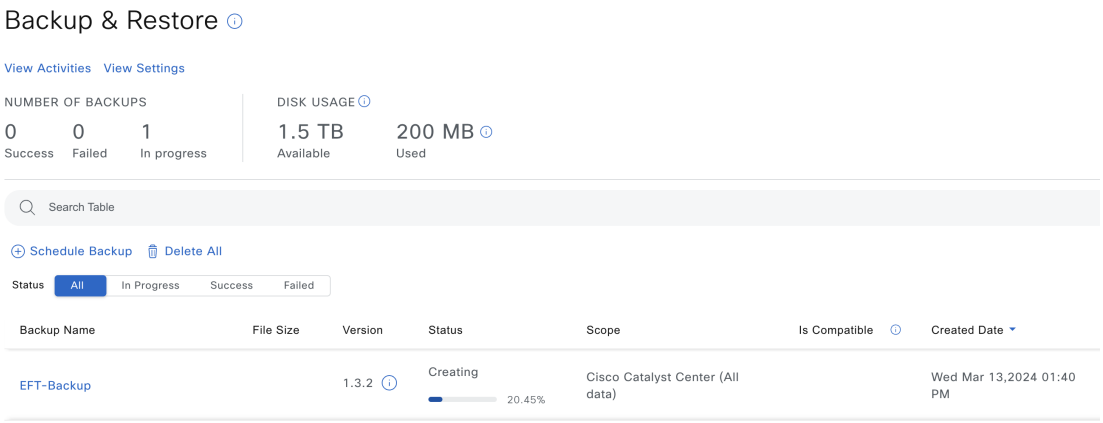
- **Backup Now**: To immediately create a backup.
- **Schedule Backup Daily**: To schedule the backup on a daily basis.
- **Schedule Backup Weekly**: To schedule the backup on a weekly basis.

c. In the **Scope** area, choose one of the following options:

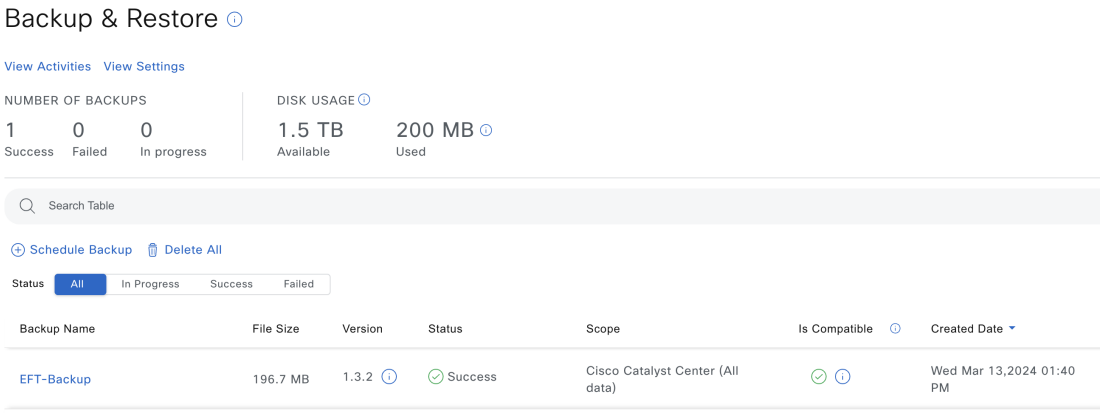
- **Cisco Catalyst Center (All Data)**: Choose this option to create a backup for automation and Assurance data.
- **Cisco Catalyst Center (Without Assurance Data)**: Choose this option to create a backup only for automation data.

d. Click **Save**.

Step 3 Catalyst Center begins the backup process. An entry for the backup is added to the **Backup & Restore** window.



When the backup is complete, its status changes from `Creating` to `Success`.



Restore Data from Backups

Use this procedure to restore backup data from your virtual appliance. To restore backup data from a failed or faulty virtual appliance, see Restore Data from a Physical Disk for a Faulty Virtual Appliance, on page 121.

Caution The Catalyst Center restore process restores only the database and files. The restore process does not restore your network state or any changes that were made since the last backup, including any new or updated network policies, passwords, certificates, or trustpool bundles.

Before you begin

Make sure that the following requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- You have backups from which to restore data.

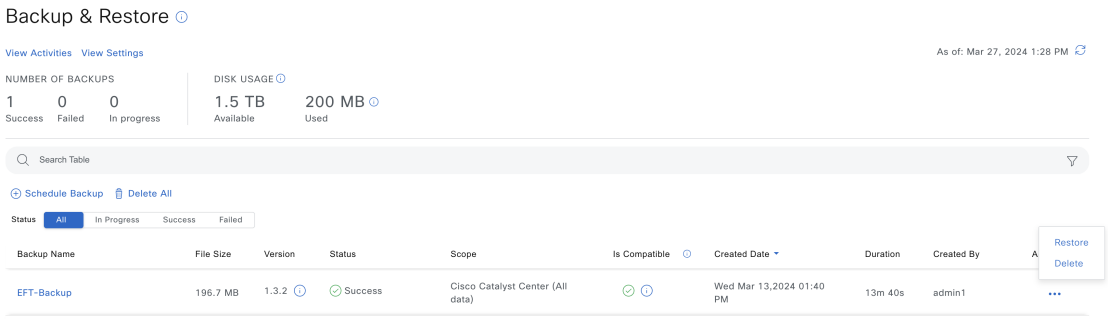
When you restore data, Catalyst Center on ESXi enters maintenance mode and is unavailable until the restore process completes. Make sure that you restore data at a time when Catalyst Center on ESXi can be unavailable.

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

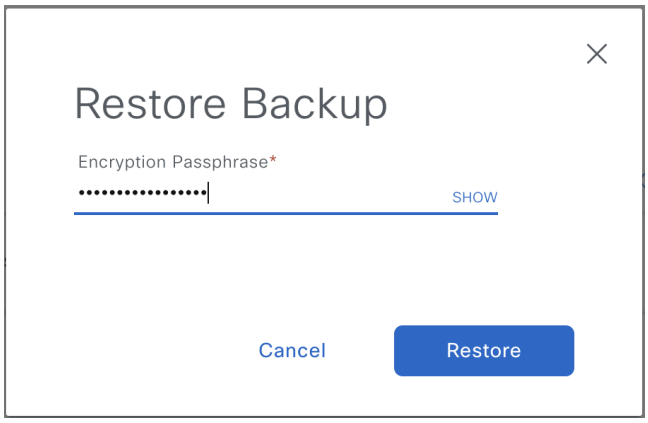
If you have created a backup, it appears in the **Backup & Restore** window.

Step 2 In the **Backup Name** column, locate the backup that you want to restore.

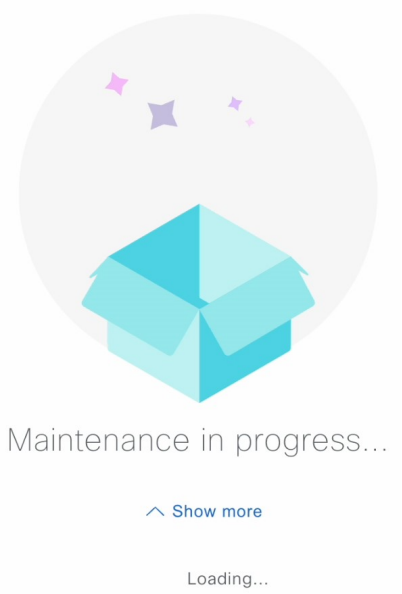
Step 3 In the **Actions** column, click the ellipsis and choose **Restore**.



Step 4 In the **Restore Backup** dialog box, enter the **Encryption Passphrase** that you used while configuring the backup location and click **Restore**.

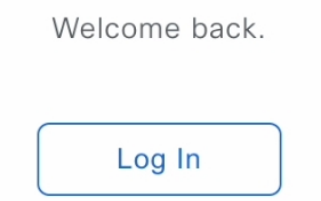


The appliance goes into maintenance mode and starts the restore process.

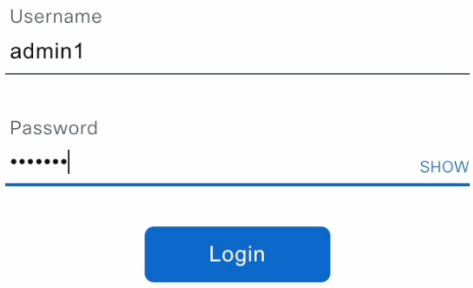


When the restore operation is complete, its status in the **Backup & Restore** window table changes to `Success`.

Step 5 After the restore operation completes, click **Log In** to log back in to Catalyst Center on ESXi.



Step 6 Enter the admin user's username and password, then click **Login**.



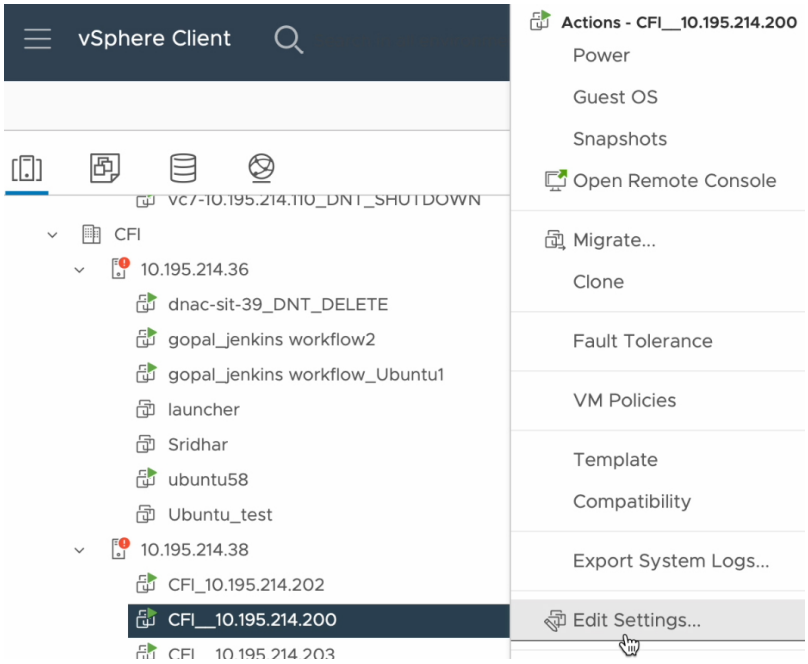
Restore Data from a Physical Disk for a Faulty Virtual Appliance

Use this procedure to restore data from a physical disk for a virtual appliance that has failed or is faulty.

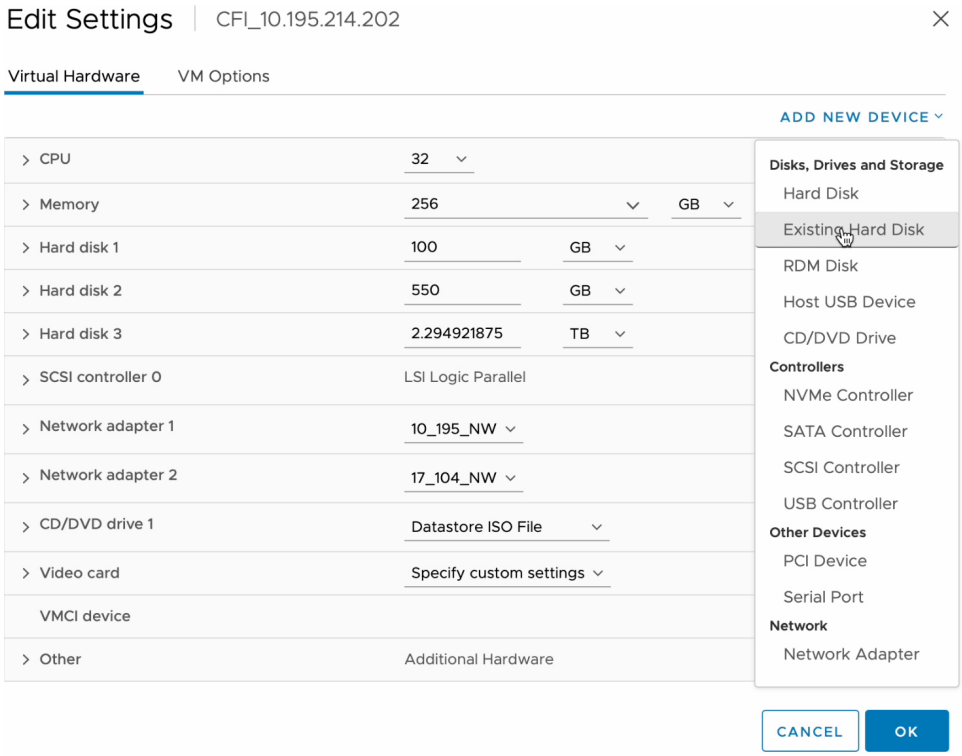
Step 1 For your new virtual appliance, do the following to configure Catalyst Center on ESXi to use the storage disk that you configured for the faulty virtual appliance:

a. Power OFF the appliance's virtual machine.

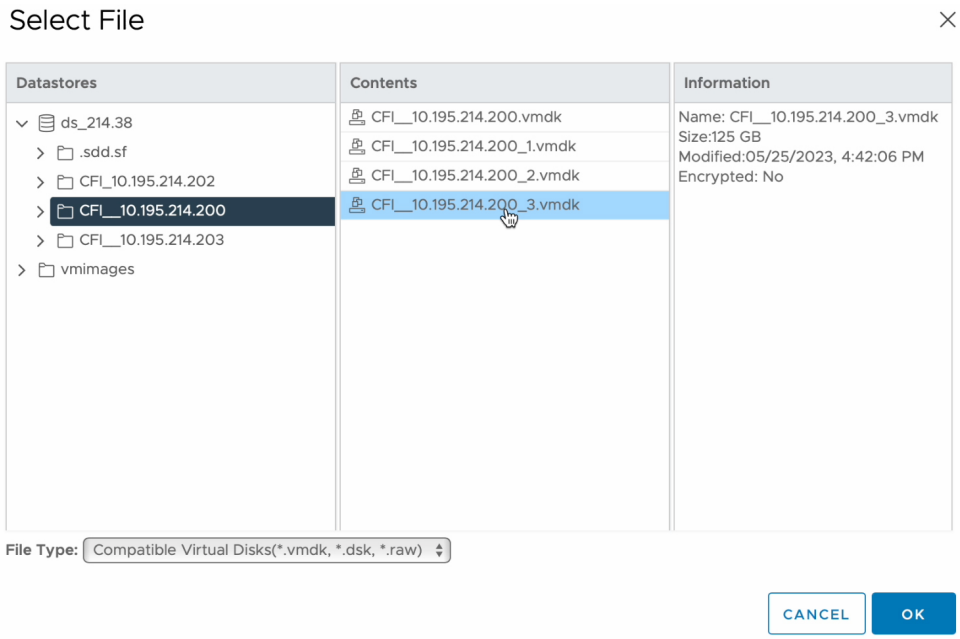
b. Open a vSphere Client, right-click the Catalyst Center on ESXi virtual machine in the left pane, and then choose **Edit Settings**.



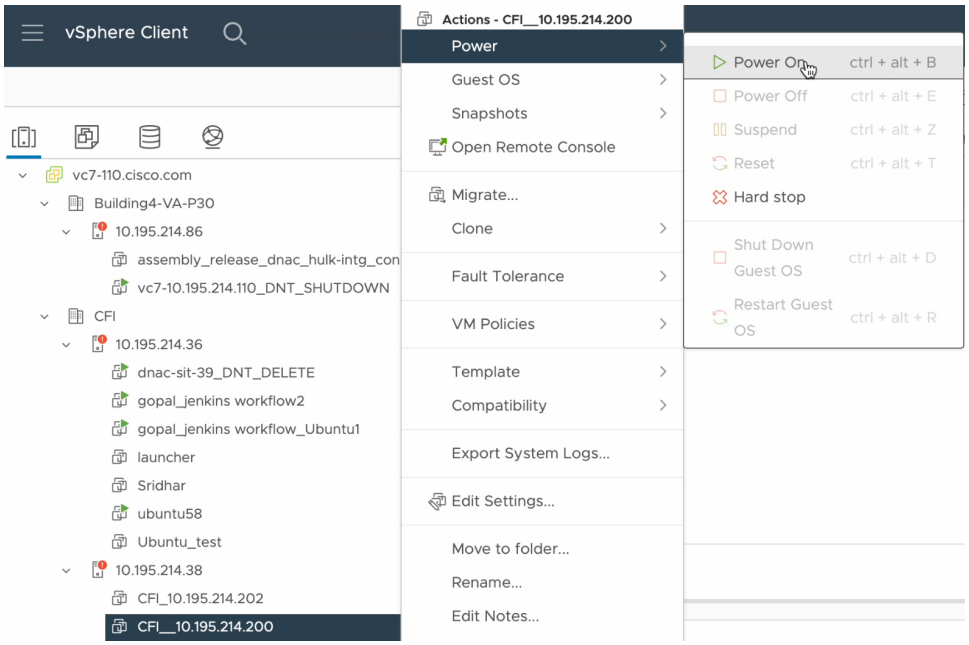
c. In the **Edit Settings** dialog box, click **Add New Device** and then choose **Existing Hard Disk**.



d. In the **Select File** dialog box, click your ESXi host, click the storage disk (.vmdk) that was created, and then click **OK**.



e. Power on the appliance's virtual machine.



It takes approximately 45 minutes for all the services to restart.

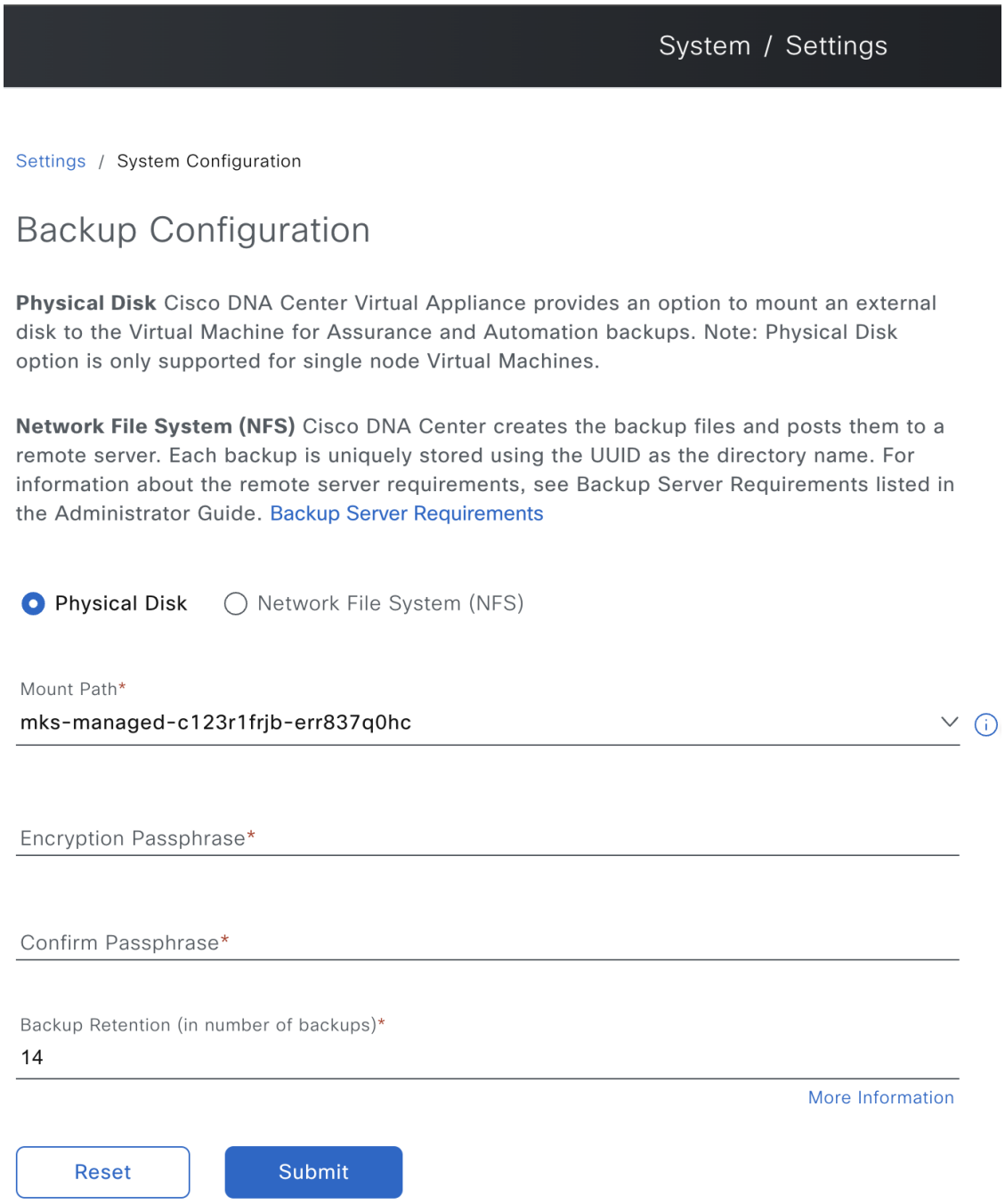
Note After the virtual machine comes back up, run the **magctl appstack status** command to confirm that the services are running.

Step 2 To configure the storage location for the backup, do the following:

a) From the Catalyst Center on ESXi menu, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

b) Click the **Physical Disk** radio button.

c) Choose the physical disk from the **Mount Path** drop-down list.



d) Enter the passphrase that will be used to encrypt the security-sensitive components of the backup (such as certificates and credentials).

Important Make sure that you don't lose this passphrase. You'll need to enter it later in the succeeding steps and won't be able to restore the backup you're about to create without it.

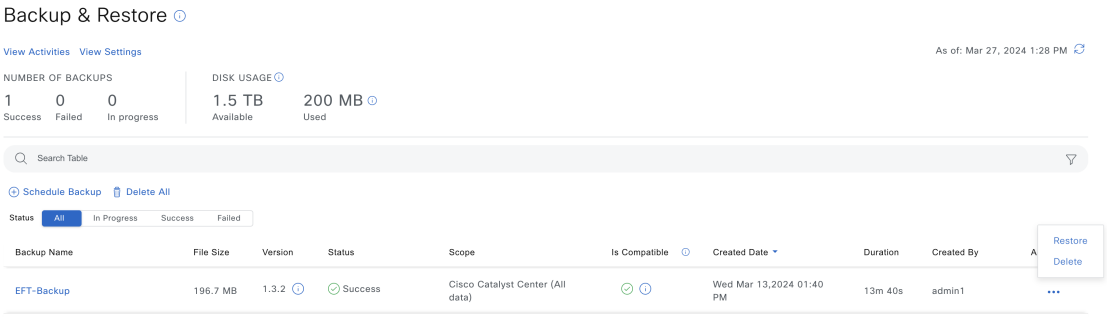
e) Set how long backup files are kept before they are deleted.

f) Click **Submit**.

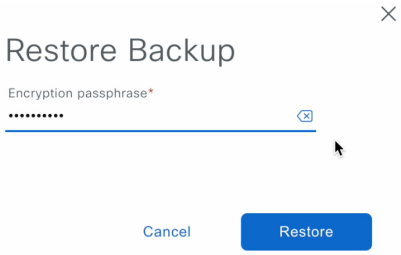
Step 3 To restore the backup, do the following:

a) From the Catalyst Center on ESXi menu, choose **System** > **Backup & Restore**.

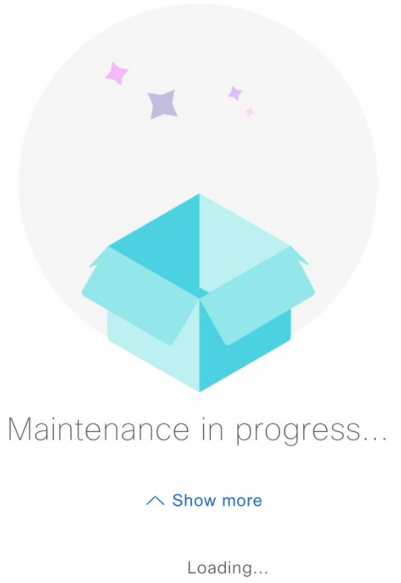
b) Locate the backup in the **Backup & Restore** window, click the ellipsis under **Actions** column, and choose **Restore**.



c) Enter the same encryption passphrase that you entered in the preceding step, and click **Restore**.

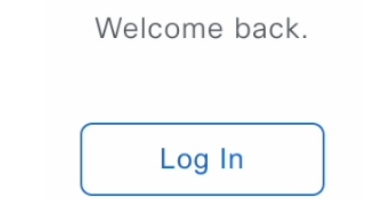


The appliance goes into maintenance mode and starts the restore process.

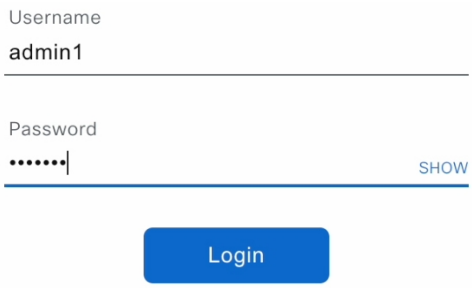


When the restore operation is complete, its status in the **Backup & Restore** window changes to `Success`.

d) After the restore operation completes, click **Log In** to log back in to Catalyst Center on ESXi.



e) Enter the admin user's username and password, then click **Login**.



Restore Data from an NFS Server for a Faulty Virtual Appliance

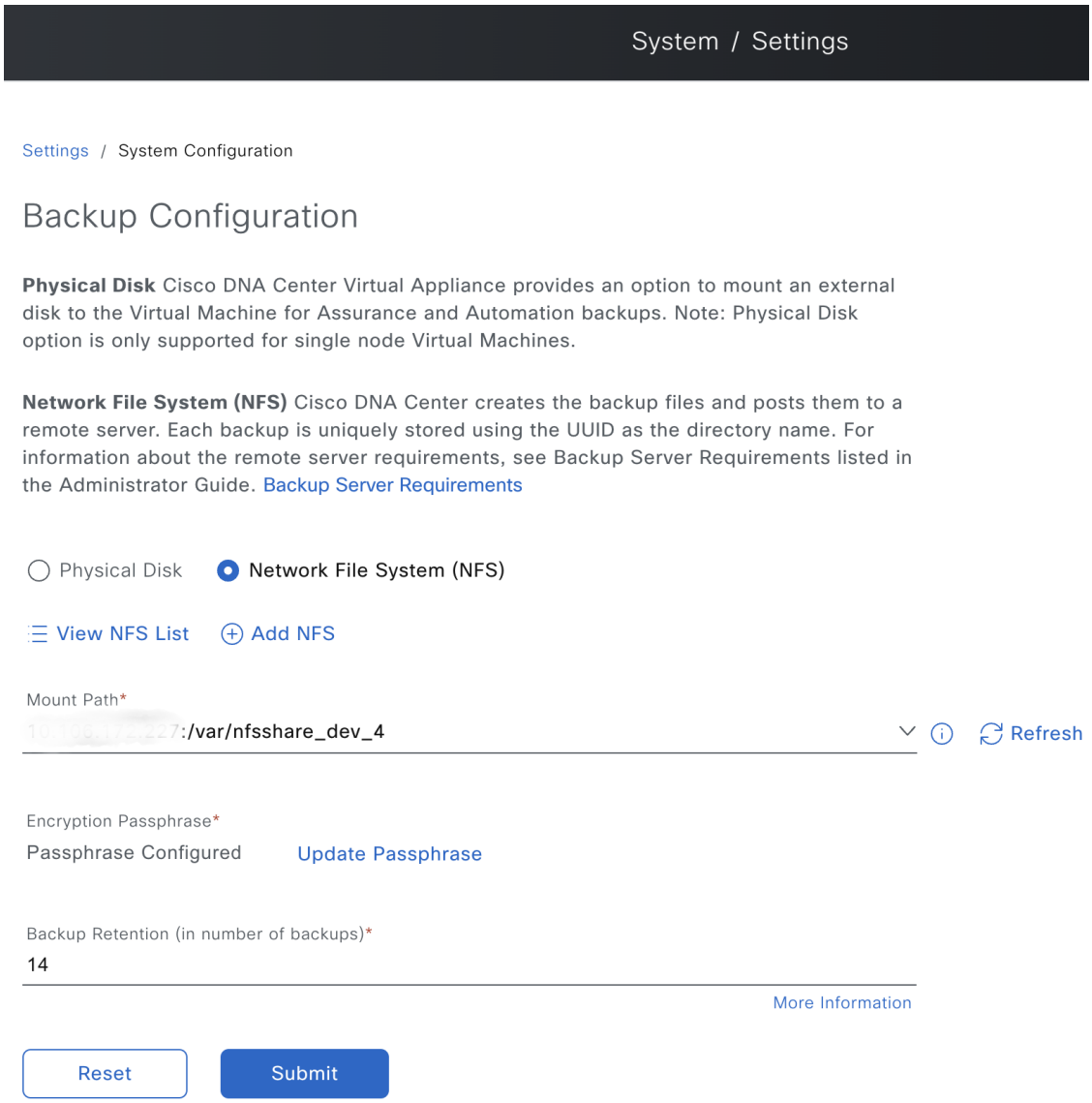
Use this procedure to restore data from an NFS server for a virtual appliance that has failed or is faulty.

Step 1 For your new virtual appliance, do the following to configure Catalyst Center on ESXi to use the NFS server that you configured for the faulty virtual appliance:

a) From the Catalyst Center on ESXi menu, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

b) Click the **NFS** radio button.

c) Choose the NFS server from the **Mount Path** drop-down list.



d) Enter the passphrase that will be used to encrypt the security-sensitive components of the backup (such as certificates and credentials).

After the passphrase is configured, if you want to change the passphrase, click **Update Passphrase**.

Important Make sure that you don't lose this passphrase. You'll need to enter it later in the succeeding steps and won't be able to restore the backup you're about to create without it.

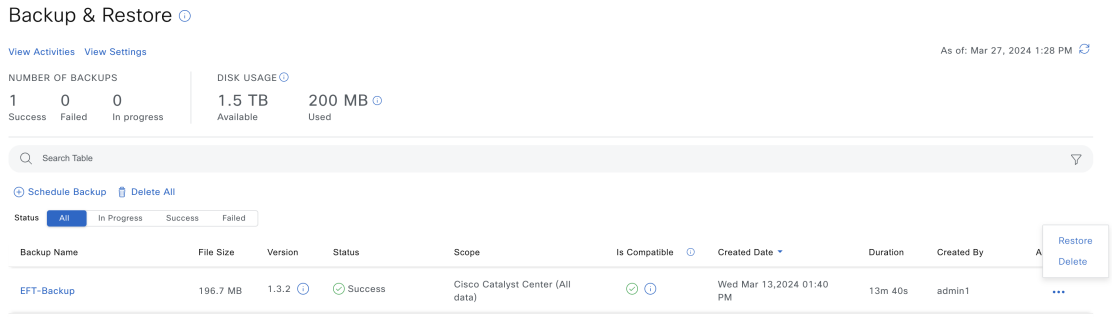
e) Set how long backup files are kept before they are deleted.

f) Click **Submit**.

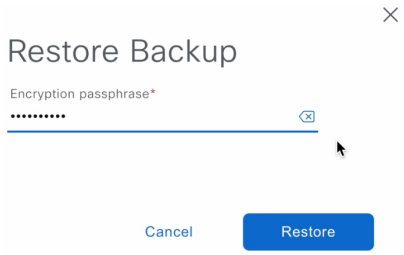
Step 2 To restore the backup, do the following:

a) From the Catalyst Center on ESXi menu, choose **System** > **Backup & Restore**.

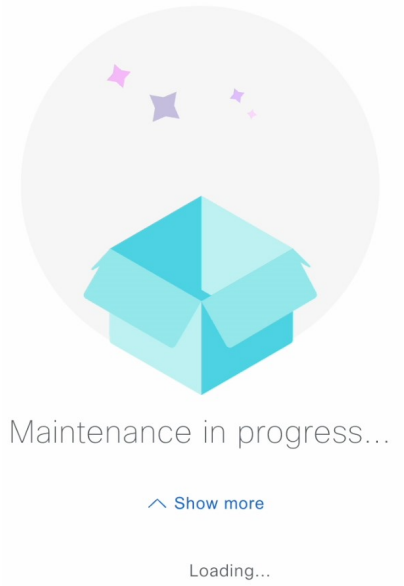
b) Locate the backup in the **Backup & Restore** window, click the ellipsis under the **Actions** column, and choose **Restore**.



c) Enter the same encryption passphrase that you entered in the preceding step, and click **Restore**.

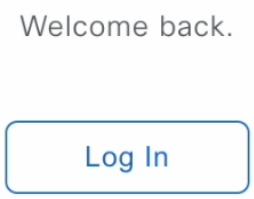


The appliance goes into maintenance mode and starts the restore process.

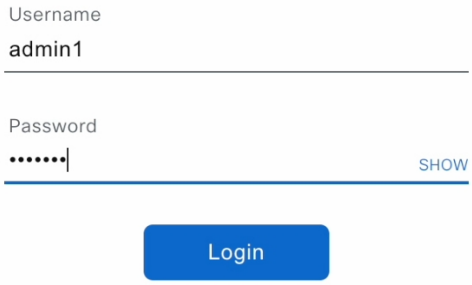


When the restore operation is complete, its status in the **Backup & Restore** window changes to `Success`.

d) After the restore operation completes, click **Log In** to log back in to Catalyst Center on ESXi.



e) Enter the admin user's username and password, then click **Login**.



Schedule Data Backup

You can schedule recurring backups and define the day of the week and the time of day when they will occur.

Before you begin

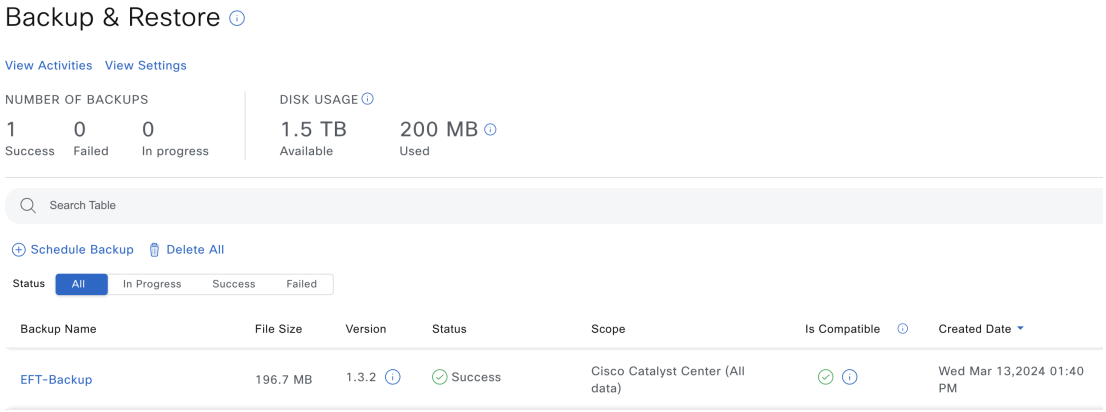
Make sure that the following requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in NFS Backup Server Requirements, on page 109.
- Backup servers have been configured in Catalyst Center. For more information, see Configure the Location to Store Backup Files, on page 115.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Backup & Restore**.
The **Backup & Restore** window is displayed.

Step 2 Click **Schedule Backup**.

Note You can schedule a new backup only when there is no backup job in progress.



Step 3 In the **Schedule Backup** slide-in pane, do the following:

a. In the **Backup Name** field, enter a unique name for the backup.

b. Choose a schedule option:

- **Schedule Backup Daily**: To schedule a daily backup job, choose the time of day when you want the backup to occur.
- **Schedule Backup Weekly**: To schedule a weekly backup job, choose the days of the week and time of day when you want the backup to occur.

c. Define the scope of the backup:

- **Cisco Catalyst Center (All data)**: This option allows the system administrator to create a backup for automation, Assurance, and system-specific sets.
- **Cisco Catalyst Center (without Assurance data)**: This option allows the administrator to create a backup for automation and system-specific sets.

d. Click **Save**.

The **Backup & Restore** window displays a banner message that shows the day and time for which the backup is scheduled.

Step 4 (Optional) Click **View Upcoming Backups** to make any changes to the upcoming schedules. If you don't want the backup to occur on a scheduled date and time, in the **Upcoming Schedules** slide-in pane, click the toggle button to disable a particular schedule.

Step 5 (Optional) Click **Edit Schedule** to edit the schedule.

Step 6 (Optional) Click **Delete Schedule** to delete the schedule.

Step 7 After the backup starts, it appears in the **Backup & Restore** window. Click the backup name to view the lists of steps executed.

Alternatively, you can click **View Activities** at the top left of the **Backup & Restore** window and click the **Execution ID**. The **Create Backup Details** slide-in pane opens and shows the list of steps executed.

Step 8 In the **Backup & Restore** window, click the **In Progress**, **Success**, or **Failure** tab to filter the list of backups to show only those tasks with a status of In Progress, Success, or Failure.

During the backup process, Catalyst Center creates the backup database and files. The backup files are saved to the specified location. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. The status of the backup job changes from **In Progress** to **Success** when the process is finished.

Note If the backup process fails, there is no impact to the appliance or its database. The most common reason for a failed backup is insufficient disk space. If your backup process fails, make sure that there is sufficient disk space on the remote server and attempt another backup.