



## **Cisco Digital Network Architecture Center Administrator Guide, Release 2.1.1**

**First Published:** 2020-06-12

### **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)

© 2020 Cisco Systems, Inc. All rights reserved.



# CONTENTS

---

## CHAPTER 1

---

### New and Changed Information 1

---

## CHAPTER 2

### Get Started with Cisco DNA Center 5

About Cisco DNA Center 5

Log In 5

Log In for the First Time as a Network Administrator 6

Default Home Page 7

Use Global Search 10

Enable Localization 12

Where to Start 13

---

## CHAPTER 3

### Configure System Settings 15

About System Settings 16

Use the System 360 16

View the Services in System 360 18

Monitor System Health 19

Establish Cisco IMC Connectivity 19

Delete Cisco IMC Settings 19

Subscribe to System Notification Events 20

View the System Topology 21

Troubleshoot Appliance and External System Issues 22

System Topology Notifications 23

Suggested Actions 24

Cisco DNA Center and Cisco ISE Integration 28

Anonymize Data 29

Configure Authentication and Policy Servers 30

Configure Cisco AI Network Analytics Data Collection	32
Disable Cisco AI Network Analytics Data Collection	34
Update the Machine Reasoning Knowledge Base	35
Cisco Accounts	36
Configure Cisco Credentials	36
Clear Cisco Credentials	37
Configure Connection Mode	37
Register Plug and Play	38
Configure Smart Account	38
Smart Licensing	39
Device Controllability	39
Configure Device Controllability	41
Accept the License Agreement	42
Cloud Access Keys	42
Integrity Verification	43
Upload the KGV File	43
Configure an IP Address Manager	45
Configure Debugging Logs	46
Configure the Network Resync Interval	47
View Audit Logs	48
Activate High Availability	49
Configure Integration Settings	49
Set Up a Login Message	49
Configure the Proxy	50
Security for Cisco DNA Center	51
Change the TLS Version and Enable RC4-SHA (Not Secure)	51
Configure Proxy Certificate	53
Certificate and Private Key Support	54
Certificate Chain Support	55
Update the Cisco DNA Center Server Certificate	56
Certificate Management	57
Configure the Device Certificate Lifetime	57
Change the Role of the PKI Certificate from Root to Subordinate	58
Provision a Rollover Subordinate CA Certificate	60

Renew Certificates	61
Configure Trustpool	62
Configure the SFTP Server	63
Configure SNMP Properties	64
About Product Usage Telemetry Collection	64
Configure vManage Properties	65
Account Lockout	65
Password Expiry	66

---

## CHAPTER 4

### Manage Applications 67

Application Management	67
Download and Update System Updates	67
Download and Install Packages and Updates	68
Uninstall a Package	69

---

## CHAPTER 5

### Manage Users 71

About User Profiles	71
About User Roles	71
Create a Local User	72
Edit a Local User	72
Delete a Local User	73
Reset a Local User Password	73
Change Your Own User Password	74
Reset a Forgotten Password	74
Configure Role-Based Access Control	74
Display Role-Based Access Control Statistics	79
Two-Factor Authentication	79
Prerequisites for Two-Factor Authentication	80
Two-Factor Authentication Workflow	80
Configure Two-Factor Authentication	80
Enable Two-Factor Authentication Using RADIUS	82
Enable Two-Factor Authentication Using TACACS+	82
Log In Using Two-Factor Authentication	85
Display External Users	85

---

**CHAPTER 6****Manage Licenses 87**

- License Manager Overview 87
- Integration with Cisco Smart Accounts 90
- Set Up License Manager 90
- Visualize License Usage and Expiration 91
- View License Details 92
- Change License Level 93
- Export License Information 94
- Auto Registration of Smart License-Enabled Devices 94
- Day 0 Configuration for Smart License-Enabled Devices 94
- Apply Specific License Reservation or Permanent License Reservation to Devices 95
  - Enable SLR/PLR when the Device and Cisco DNA Center Are Connected to CSSM 96
  - Enable SLR/PLR Using CSV when the Devices and Cisco DNA Center Are Not Connected to CSSM 96
  - Generate the Authorization Code from CSSM 97
- Cancel SLR or PLR Applied to Devices 97

---

**CHAPTER 7****Backup and Restore 99**

- About Backup and Restore 99
- Backup Server Requirements 100
- Example of NFS Server Configuration 101
- Configure Backup Servers 102
- Back Up Data Now 103
- Schedule Data Backups 104
- Restore Data from Backups 105



## CHAPTER 1

# New and Changed Information

The following table summarizes the new and changed features and tells you where they are documented.

**Table 1: New and Changed Features for Cisco DNA Center, Release 2.1.1**

Feature	Description	Where Documented
System health	From the <b>System Health</b> page, you can monitor the health of the physical components on your Cisco DNA Center appliances and keep tabs on any issues that may occur.	<a href="#">Monitor System Health, on page 19</a>
System topology	From the System Health page's system topology, you can view a graphical representation of your Cisco DNA Center appliances and the external systems that are connected to your network, such as Cisco Connected Mobile Experiences (Cisco CMX) and Cisco ISE. From here, you can quickly identify any network components that are experiencing an issue and require further attention.	<a href="#">View the System Topology, on page 21</a>
Role-based access control	Cisco DNA 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 Cisco DNA Center functions.	<a href="#">Configure Role-Based Access Control, on page 74</a>
Audit logging	<p>Audit logs 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.</p> <p>Audit logs also display northbound operation details such as POST, DELETE, and PUT with payload information, and southbound operation details such as the configuration pushed to a device.</p>	<a href="#">View Audit Logs, on page 48</a>
Smart License enablement	Smart Licensing is a cloud-based, software license management solution that allows you to manage and track the status of your license and software usage.	<a href="#">Smart Licensing</a>

Feature	Description	Where Documented
Connection mode	<p>Connection mode provides options to access the Cisco SSM cloud. The following connection modes are available:</p> <ul style="list-style-type: none"> <li>• Direct</li> <li>• On-prem CSSM</li> <li>• Smart Proxy</li> </ul>	<a href="#">Configure Connection Mode</a>
System settings	<p>The following system settings have been improved:</p> <ul style="list-style-type: none"> <li>• Cisco Accounts Credentials</li> <li>• Connection Mode</li> <li>• PnP Connect</li> <li>• Smart Account</li> <li>• Smart License Enablement</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Configure Cisco Credentials, on page 36</a></li> <li>• <a href="#">Register Plug and Play, on page 38</a></li> </ul>
Telemetry collection	The telemetry feature collects user information and provides valuable data about the status and capabilities of the Cisco DNA Center appliance.	<a href="#">About Product Usage Telemetry Collection, on page 64</a>
Device Controllability Enhancements	<p>The following device settings will be enabled as part of device controllability during discovery or at runtime:</p> <ul style="list-style-type: none"> <li>• <b>Device Discovery</b> <ul style="list-style-type: none"> <li>• SNMP Credentials</li> <li>• NETCONF Credentials</li> </ul> </li> <li>• <b>Adding Devices to Inventory</b> <ul style="list-style-type: none"> <li>• Cisco TrustSec (CTS) Credentials</li> <li>• IPDT Enablement</li> </ul> </li> <li>• <b>Assigning Devices to a Site</b> <ul style="list-style-type: none"> <li>• Controller Certificates</li> <li>• SNMP Trap Server Definitions</li> <li>• Syslog Server Definitions</li> <li>• NetFlow Server Definitions</li> <li>• Wireless Service Assurance (WSA)</li> </ul> </li> </ul>	<a href="#">Device Controllability, on page 39</a>
Smart Account credentials	Connect to your Smart Licensing account for entitlement and license management.	<a href="#">Configure Smart Account, on page 38</a>



Feature	Description	Where Documented
Login message	You can set a message for all users to see when they log in to the Cisco DNA Center appliance.	<a href="#">Set Up a Login Message, on page 49</a>
Machine Reasoning Knowledge Base	Whenever there is a new update in the existing network reasoner workflow, <b>AVAILABLE UPDATE</b> shows up in <b>Machine Reasoning Knowledge Base</b> window, which includes Version, and Details of new update.	<a href="#">Update the Machine Reasoning Knowledge Base, on page 35</a>





## CHAPTER 2

# Get Started with Cisco DNA Center

---

- [About Cisco DNA Center, on page 5](#)
- [Log In, on page 5](#)
- [Log In for the First Time as a Network Administrator, on page 6](#)
- [Default Home Page, on page 7](#)
- [Use Global Search, on page 10](#)
- [Enable Localization, on page 12](#)
- [Where to Start, on page 13](#)

## About Cisco DNA Center

Cisco Digital Network Architecture offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center GUI provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

## Log In

Access Cisco DNA Center by entering its network IP address in your browser. For compatible browsers, see the [Cisco DNA Center Release Notes](#). This IP address connects to the external network and is configured during the Cisco DNA Center installation. For more information about installing and configuring Cisco DNA Center, see the [Cisco DNA Center Installation Guide](#).

You should continuously use Cisco DNA Center to remain logged in. If you are inactive for too long, Cisco DNA Center logs you out of your session automatically.

---

### Step 1

Enter an address in your web browser's address bar in the following format. Here, *server-ip* is the IP address (or the hostname) of the server on which you have installed Cisco DNA Center:

`https://server-ip`

Example: `https://192.0.2.1`

Depending on your network configuration, you might have to update your browser to trust the Cisco DNA Center server security certificate. Doing so will help ensure the security of the connection between your client and Cisco DNA Center.

- Step 2** Enter the Cisco DNA Center username and password assigned to you by the system administrator. Cisco DNA Center displays its home page.
- If your user ID has the NETWORK-ADMIN-ROLE and no other user with the same role has logged in before, you will see a first-time setup wizard instead of the home page. For details, see [Log In for the First Time as a Network Administrator, on page 6](#).
- Step 3** To log out, click the **Menu** icon (≡) and choose **Sign Out**.
- 

## Log In for the First Time as a Network Administrator

If your user ID has the NETWORK-ADMIN-ROLE assigned, and no other user with the same role has logged in before, you will be redirected to the **Get Started** wizard.

The wizard is a quick way to get immediate value from Cisco DNA Center. It consists of a few screens that collect information needed to discover and monitor the condition of your network devices, and then help you visualize your network's overall health using the Cisco DNA Center home page dashboard.

You can perform all of the same tasks the wizard does using other Cisco DNA Center features. Using the wizard does not prevent you from using those features. You can choose to skip the wizard entirely at any point and it will not be shown again for you. However, Cisco DNA Center will continue to display the wizard at login to any user with the same role until one such user completes the wizard steps. After that, Cisco DNA Center never displays the wizard again.

If you skipped the **Get Started** wizard, you can always revisit it from the **Get Started** link at the top right of the home page.

### Before you begin

You need to have the following information to complete the wizard:

- The IP addresses of your SYSLOG and SNMP servers
  - The IP address and port of your NetFlow server
  - For discovery: The IP address to start from (if choosing CDP discovery) or the starting and ending IP addresses (if choosing Range discovery)
  - Optional: Your preferred management IP address
  - Device CLI credentials, including the Enable password
  - SNMP v2c credentials, including the read community string
- 

- Step 1** If you have not already done so, log in to Cisco DNA Center normally, as explained in [Log In, on page 5](#). You will be redirected to **Get Started** wizard if this is your first login.
- Step 2** Click **Get Started** in the Getting Started wizard to continue device discovery or **Exit** to return to the home page.
- Step 3** Enter the network properties for device discovery and click **Save & Next**. Click **Back** to return to the previous screen.

**Step 4** Specify the **Discovery Type**, **Starting IP Address**, and **CLI Credentials**.

**Step 5** When you are finished, click **Begin Discovery**. Cisco DNA Center displays the home page, which slowly fills with network health information as discovery completes.

---

## Default Home Page

After you log in, Cisco DNA Center displays its home page. The home page has the following main areas: **Assurance Summary**, **Network Snapshot**, **Network Configuration**, and **Tools**.

The **Assurance Summary** area includes:

- **Health**: Provides the health score of your overall enterprise, which includes network devices, wired clients, and wireless clients. Clicking **View Details** takes you to the **Overall Health** window.
- **Critical Issues**: Provides the count of P1 and P2 issues. Clicking **View Details** takes you to the **Open Issues** window.
  - **P1**: Critical issues that need immediate attention before they cause a wider impact on network operations.
  - **P2**: Major issues that can potentially impact multiple devices or clients.
- **Trends and Insights**: Provides insights about the performance of your network. Clicking **View Details** takes you to the **Network Insights** window.

The **Network Snapshot** area includes:

- **Sites**: Provides the number of sites discovered on your network along with the number of DNS and NTP servers. Clicking **Add Sites** takes you to the **Add Site** window.
- **Network Devices**: Provides the number of network devices discovered on your network along with the number of unclaimed, unprovisioned, and unreachable devices. Clicking **Find New Devices** takes you to the **New Discovery** window.
- **Application Policies**: Provides the number of application policies discovered on your network along with the number of successful and errored deployments. Clicking **Add New Policy** takes you to the **Application Policies** window.
- **Network Profiles**: Provides the number of profiles discovered on your network. Clicking **Manage Profiles** takes you to the **Network Profiles** window.
- **Images**: Provides the number of images discovered on your network along with the number of untagged and unverified images. Clicking **Import Images/SMUs** takes you to the **Image Repository** window.
- **Licensed Devices**: Provides the number of devices that have a Cisco DNA Center license along with the number of switches, routers, and access points. Clicking **Manage Licenses** takes you to the **License Management** window.

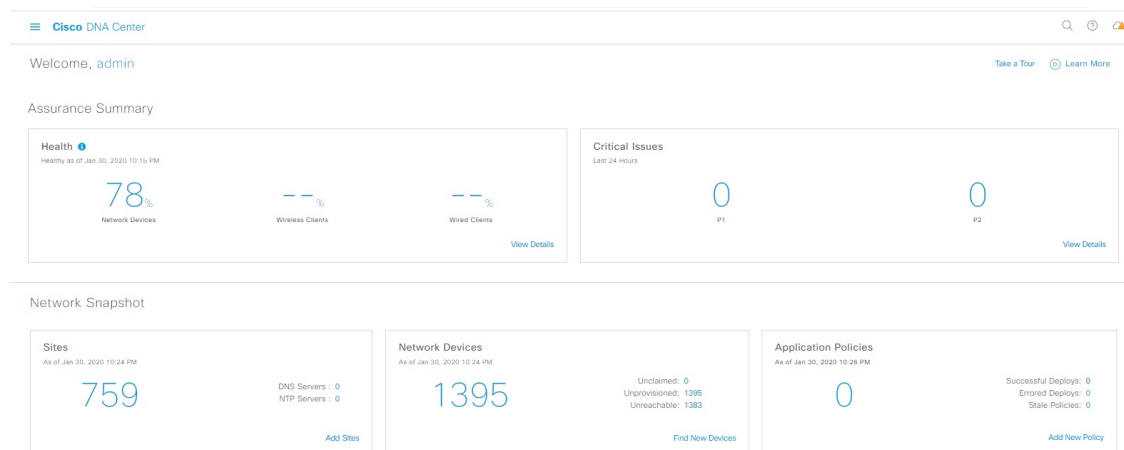
The **Network Configuration** area includes:

- **Design**: Create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network.

- **Policy:** Create policies that reflect your organization's business intent for a particular aspect of the network, such as network access. Cisco DNA Center takes the information collected in a policy and translates it into network-specific and device-specific configurations required by the different types, makes, models, operating systems, roles, and resource constraints of your network devices.
- **Provision:** Prepare and configure devices, including adding devices to sites, assigning devices to the inventory, deploying the required settings and policies, creating fabric domains, and adding devices to the fabric.
- **Assurance:** Provide proactive and predictive actionable insights about the performance and health of the network infrastructure, applications, and end-user clients.
- **Platform:** Allows you to programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions, and add support for multivendor devices.

**Tools:** Use the **Tools** area to configure and manage your network.

**Figure 1: Cisco DNA Center Home Page**



## Different Views of Home Page:

### Getting Started

When you log in to Cisco DNA Center for the first time as a Network Administrator or System Administrator, or when there are no devices in the system, you see the following dashlet. Click **Get Started** and complete the getting started workflow to discover new devices in your network.

In a few simple steps, discover your devices to begin your Cisco DNA Center journey!

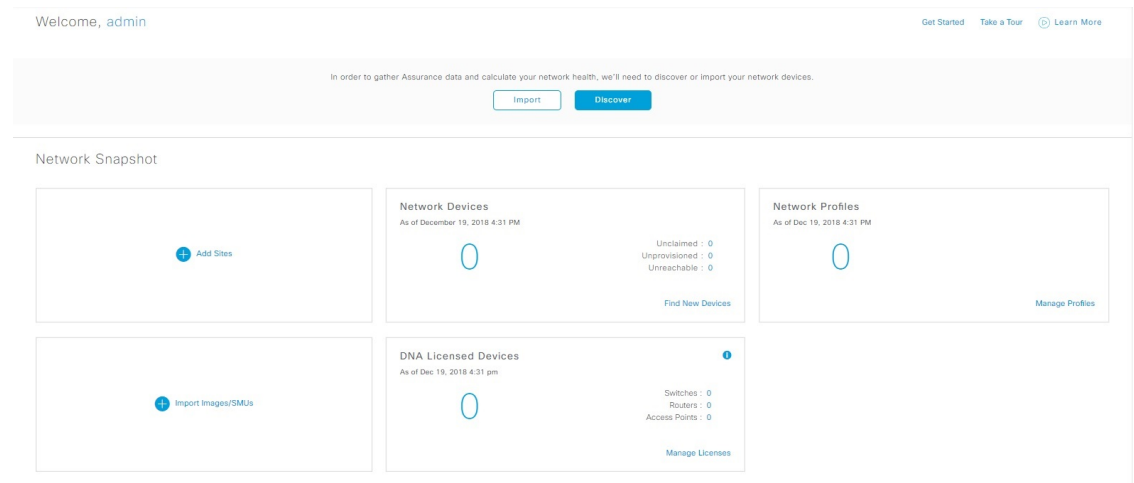
**Get Started**

When you log in to Cisco DNA Center for the first time as an Observer, you see the following message:

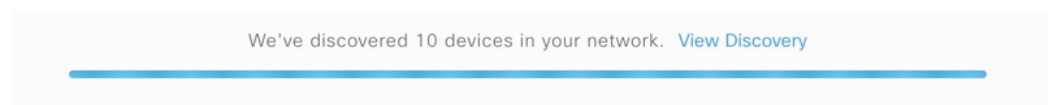
Ask your Network Administrator to add Network Devices to gather Assurance data.

### Day 0 Home Page

If you skipped getting started, or when there are no devices in the system, you see the following home page.



When discovery is in progress, you see a progress message with a link to the **Discovery** window.






When there are devices in the system, you see a network snapshot of discovered devices.

Click the **Menu** icon (≡) at the top-left corner of the home page to access the following menus:

- Design
- Policy
- Provision
- Assurance
- Workflows
- Tools
- Platform
- Activity
- System

Click the icons at the top- and bottom-right corner of the home page to perform common tasks:

Icon	Description
	<b>Search:</b> Search for devices, users, hosts, menus in the hamburger menu, and other items, anywhere they are stored in the Cisco DNA Center database. For tips on using Search, see <a href="#">Use Global Search, on page 10</a> .

Icon	Description
	<b>Help</b> <ul style="list-style-type: none"> <li>• <b>About:</b> Display the current Cisco DNA Center software version. Click <b>Release Notes</b> to launch the release notes in a separate browser tab. Click <b>Packages</b> to view the system and application package versions. Click <b>Serial number</b> to view the serial number of the Cisco DNA Center appliance.</li> <li>• <b>API Reference:</b> Open the Cisco DNA Center platform API documentation in Cisco DevNet.</li> <li>• <b>Developer Resources:</b> Open Cisco DevNet, where you can access developer tools.</li> <li>• <b>Help:</b> Launch context-sensitive online help in a separate browser tab.</li> <li>• <b>Contact Support:</b> Open a support case with the Cisco Technical Assistance Center (TAC).</li> <li>• <b>Make a Wish:</b> Submit your comments and suggestions to the Cisco DNA Center product team.</li> </ul>
	<b>Software Updates:</b> See a list of available software updates. Click the <b>Go to Software Updates</b> link to view system and application updates.
	<b>Interactive Help:</b> Opens a menu of interactive help flows that enable users to complete specific tasks from the GUI.

If you are new to Cisco DNA Center, see [Where to Start, on page 13](#) for tips and suggestions on how to begin.



#### Note

By default, the login name you provided is displayed in the Welcome text. To change the name, click the name link; for example, **admin**. You are taken to the **User Management** window, where you can edit the display name.


## Use Global Search

Use the global Search function to find items in the following categories anywhere in Cisco DNA Center:

- **Activities:** Search for Cisco DNA Center menu items, workflows, and features by name.
- **Applications:** Search for them by name.
- **Application Groups:** Search for them by name.
- **Authentication template:** Search for them by name or type.
- **Devices:** Search for them by collection status, reachability status, location, or tag.



- **Fabric:** Search by fabric name.
- **Hosts and Endpoints:** Search for them by name, IP address, or MAC address.
- **IP Pools:** Search for them by name or IP address.
- **Network Devices:** Search for them by name, IP address, serial number, software version, platform, product family, or MAC address.
- **Network Profiles:** Search by profile name.
- **Network Settings**
  - **Device Credentials:** Search by name.
  - **IP Address Pools:** Search for them by group name or pool CIDR.
  - **Service Provider Profiles:** Search for them by profile name, WAN provider, or model.
- **Policy:** Search for them by name or description.
- **Sites:** Search for them by name.
- **Traffic copy:** Search for them by name and description.
- **Transits:** Search by transit name.
- **Users:** Search for the system settings and users by username. Case-insensitivity and substring search are not supported for usernames.
- Other items, as new versions of Cisco DNA Center are released.

To start a global Search, click the  icon in the top-right corner of any Cisco DNA Center page. Cisco DNA Center displays a pop-up global search window, with a Search field where you can begin entering identifying information about an item.


You can enter all or part of the target item's name, address, serial number, or other identifying information. The Search field is case-insensitive and can contain any character or combination of characters.

As you begin entering your search string, Cisco DNA Center displays a list of possible search targets that match your entry. If more than one category of item matches your search string, Cisco DNA Center sorts them by category, with a maximum of five items in each category. The first item in the first category is selected automatically, and summary information for that item appears in the summary panel on the right.

You can scroll the list as needed, and click any of the suggested search targets to see information for that item in the summary panel. If there are more than five items in a category, click **View All** next to the category name. To return to the categorized list from the complete list of search targets, click **Go Back**.

As you add more characters to the search string, global Search automatically narrows the displayed list.

The summary panel includes links to more information. The link varies as appropriate for each category and item. For example, with Activities, the summary panel displays links to menu items and workflows elsewhere in the Cisco DNA Center system. For Applications, there is the **Application 360** view. You will see links to **Client 360** and **Topology** views for hosts and endpoints, and links to **Device 360** and **Topology** views for network devices.

When you are finished, click  to close the window.

Global search can display five results per category at a time.



# Enable Localization

You can view the Cisco DNA Center GUI screens in English (the default), Chinese, Japanese, or Korean.

To change the default language, perform the following task:

---

**Step 1** In your browser, change the locale to one of the supported languages: Chinese, Japanese, or Korean.

- From Google Chrome, do the following:
  - a. Click the  icon in the top-right corner, and then choose **Settings**.
  - b. Scroll down and click **Advanced**.
  - c. From the **Languages > Language** drop-down list, choose **Add languages**.  
The **Add languages** pop-up window appears.
  - d. Choose **Chinese**, **Japanese**, or **Korean**, and then click **Add**.
- From Mozilla Firefox, do the following:
  - a. Click the  icon in the top-right corner, and then choose **Options**.
  - b. From the **Language and Appearance > Language** area, choose **Search for more languages**.  
The **Firefox Language Settings** pop-up window appears.
  - c. From the **Select a language to add** drop-down list, choose **Chinese**, **Japanese**, or **Korean**.
  - d. Click **Ok**.

**Step 2** Log in to Cisco DNA Center.

The GUI screens are shown in the selected language.

Figure 2: Example Localized Login Screen



The image shows a localized login screen for Cisco DNA Center. At the top is the Cisco logo. Below it, the text "Cisco DNA Center" is displayed in blue, followed by the Japanese text "ネットワークの設計、自動化、保証" (Network Design, Automation, Assurance). There are two input fields: "ユーザ名\*" (Username\*) and "パスワード\*" (Password\*). Below the password field is a blue button labeled "ログイン" (Login).

## Where to Start

To start using Cisco DNA Center, you must first configure the Cisco DNA Center settings so that the server can communicate outside the network.

After you configure the settings, your current environment determines how you start using Cisco DNA Center:

- Existing infrastructure: If you have an existing infrastructure (brownfield deployment), start by running Discovery. After you run Discovery, all your devices are displayed on the **Inventory** window. For information about running Discovery, see the [Cisco DNA Center User Guide](#).
- New or nonexistent infrastructure: If you have no existing infrastructure and are starting from scratch (greenfield deployment), create a network hierarchy. For information about creating a network hierarchy, see the [Cisco DNA Center User Guide](#).





## CHAPTER 3

# Configure System Settings

---

- [About System Settings, on page 16](#)
- [Use the System 360, on page 16](#)
- [View the Services in System 360, on page 18](#)
- [Monitor System Health, on page 19](#)
- [Cisco DNA Center and Cisco ISE Integration, on page 28](#)
- [Anonymize Data, on page 29](#)
- [Configure Authentication and Policy Servers, on page 30](#)
- [Configure Cisco AI Network Analytics Data Collection, on page 32](#)
- [Update the Machine Reasoning Knowledge Base, on page 35](#)
- [Cisco Accounts, on page 36](#)
- [Device Controllability, on page 39](#)
- [Cloud Access Keys, on page 42](#)
- [Integrity Verification, on page 43](#)
- [Configure an IP Address Manager, on page 45](#)
- [Configure Debugging Logs, on page 46](#)
- [Configure the Network Resync Interval, on page 47](#)
- [View Audit Logs, on page 48](#)
- [Activate High Availability, on page 49](#)
- [Configure Integration Settings, on page 49](#)
- [Set Up a Login Message, on page 49](#)
- [Configure the Proxy, on page 50](#)
- [Security for Cisco DNA Center, on page 51](#)
- [Configure the SFTP Server, on page 63](#)
- [Configure SNMP Properties, on page 64](#)
- [About Product Usage Telemetry Collection, on page 64](#)
- [Configure vManage Properties, on page 65](#)
- [Account Lockout, on page 65](#)
- [Password Expiry, on page 66](#)

# About System Settings


To start using Cisco DNA 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 Cisco DNA Center configuration—including changes to the proxy server settings—must be done from the Cisco DNA Center GUI, and the 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.

## Use the System 360

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

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > System 360**.

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

**Cluster**

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

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

The side panel displays the following information:

- **Node Status:** Displays the health status of the node.  
If the node health is unhealthy, hover over the status to view additional information for troubleshooting.
- **Services Status:** Displays the health status of the services. Even if one service is down, the status is **Unhealthy**.
- **Name:** Service name.
- **Appstack:** App stack name.  
An app stack is a loosely coupled collection of services. A service in this environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.
- **Health:** Status of the service.
- **Version:** Version of the service.
- **Tools:** Displays metrics and logs for the service. Click the **Metrics** link to view service monitoring data in Grafana. Grafana is an open-source metric analytics and visualization suite. You can troubleshoot issues by reviewing the service monitoring data. For information about Grafana, see <https://grafana.com/>. Click the **Logs** link to view service logs in Kibana. Kibana is an open-source analytics and visualization platform. You can

troubleshoot issues by reviewing the service logs. For information about Kibana, see <https://www.elastic.co/products/kibana>.

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

**Important** Three or more hosts are required for HA to work in Cisco DNA Center.

- **Cluster Tools:** Lets you access the following tools:

- **Service Explorer:** Access the app stack and the associated services.

- **Monitoring:** Access multiple dashboards of Cisco DNA Center components using Grafana, which is an open-source metric analytics and visualization suite. Use the **Monitoring** tool to review and analyze key Cisco DNA Center metrics, such as memory and CPU usage. For information about Grafana, see <https://grafana.com/>.

**Note** In a multihost Cisco DNA Center environment, expect duplication in the Grafana data due to the multiple hosts.

- **Log Explorer:** Access detailed logs of Cisco DNA Center activity using Kibana, which is an open-source analytics and visualization platform designed to work with Elasticsearch. Use the **Log Explorer** tool to review detailed activity logs. For information about Kibana, see <https://www.elastic.co/products/kibana>.

- **Workflow:** Access the Workflow Visualizer, which provides detailed graphical representations of Cisco DNA Center infrastructure tasks, including Success, Failure, and Pending status markings. Use the Workflow tool to determine the location of a failure in a Cisco DNA Center task.

## System Management

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

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

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

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

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

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

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

## Externally Connected Systems

Displays information about external network services used by Cisco DNA Center.

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

- **IP Address Manager (IPAM):** Displays IP address manager configuration data. Click the **Configure** link to configure the IP Address Manager.

- **vManage**: Displays vManage configuration data. Click the **Configure** link to configure vManage.

---

## View the Services in System 360

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

---

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > System 360**.

**Step 2** On the **System 360** tab, in the **Cluster Tools** area, click **Service Explorer**.

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

- Hover over the node to view the node cluster health status. The healthy node clusters are marked in green. Unhealthy node clusters are marked in red.
- The Services table shows all the services associated with the node. The managed services are marked as (M).
- In the Service table, click the global filter icon to filter services by app stack name, service health status (Up, Down, or In Progress), or managed services.
- Enter a service name in the Global Search field to find a service. Click the service name to view the service in its associated node.

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

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

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

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

---



# Monitor System Health

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

## Establish Cisco IMC Connectivity

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



**Note** Only users with SUPER-ADMIN-ROLE permissions can enter Cisco IMC connectivity settings for an appliance.

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System > Settings > System Configuration > System Health Notifications**.

The IP address of each appliance in your cluster should be listed in the **Cisco DNA Center Address** column.

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

a) Click the IP address for an appliance.

The **Edit Cisco DNA Center Server Configuration** slide-in pane opens.

b) Enter the following information and then click **Save**:

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

c) Repeat Steps 2a and 2b for the other appliances in your cluster, if necessary.

## Delete Cisco IMC Settings

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



**Note** Only users with SUPER-ADMIN-ROLE permissions can delete these settings.


**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System > Settings > System Configuration > System Health Notifications**.

- Step 2** For the appliance whose settings you want to delete, click its **Delete** (🗑️) icon in the **Actions** column.  
A dialog box opens, prompting you to confirm the deletion of the settings.
- Step 3** Click **Ok**.

## Subscribe to System Notification Events

After you have established connectivity with Cisco IMC, Cisco DNA Center collects event information from Cisco IMC and stores this information as raw system events. These raw events are then processed by the rules engine and converted into system notification events. Complete the following procedure in order to instruct Cisco DNA Center to send these notification events to the subscribing endpoints that you specify.

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Platform > Developer Toolkit > Events**.

- Step 2** In the **Events** table, check the check box for the following events and then click  **Subscribe**:

- SYSTEM-EXTERNAL-CMX
- SYSTEM-EXTERNAL-IPAM
- SYSTEM-EXTERNAL-ISE-AAA-TRUST
- SYSTEM-EXTERNAL-ISE-PAN-ERS
- SYSTEM-EXTERNAL-ITSM
- SYSTEM-HARDWARE

**Note** The quickest way to view these events is to sort the table's **Event ID** column in descending order. You can also click the **Show More** link at the bottom of the page until you see the events listed.

The **Subscribe** dialog box opens.

- Step 3** In the **Name** field, enter a name for this event subscription.
- Step 4** In the **Subscription Type** drop-down list, choose **SNMP**.
- Step 5** Click the **Create a new endpoint** radio button, then enter the name and description of the endpoint that will receive notification events.
- Step 6** In the **Notification Trap Receiver** area, configure the endpoint that will send SNMP traps to the System Health trap receiver by entering the following information:
- The endpoint's IP address or hostname.
  - The port number that the endpoint will use to send SNMP traps.
- Step 7** In the **Community Configuration** area, configure the SNMP community credentials that are required to establish a connection with the trap receiver.
- a) In the **SNMP Version** drop-down list, choose the SNMP version that you want to use.
  - b) Do one of the following, depending on the SNMP version that you chose:
    - If you chose **V2C**, enter the appropriate community string.

- If you chose **V3**, enter the following information:
    - Username: Enter the username required to establish an SNMP connection. This field is required.
    - Mode: Choose **Authentication and Privacy** (authPriv), **Authentication, No Privacy** (authNoPriv), or **No Authentication, No Privacy** (noAuthnoPriv). This field is required.
    - Authentication Type: Choose SHA or MD5 hashing for the password you will enter in the **Authentication Password** field.
    - Authentication Password: Enter and then confirm the authentication password.
    - Privacy Type: Choose AES128 or DES encryption for the privacy password you will enter in the **Privacy Password** field.
- Note** Although DES encryption is an available option, we recommend that you choose the AES128 encryption option because it is more secure.
- Privacy Password: Enter and then confirm the privacy password.

**Step 8** Click **Subscribe**.

---

## View the System Topology

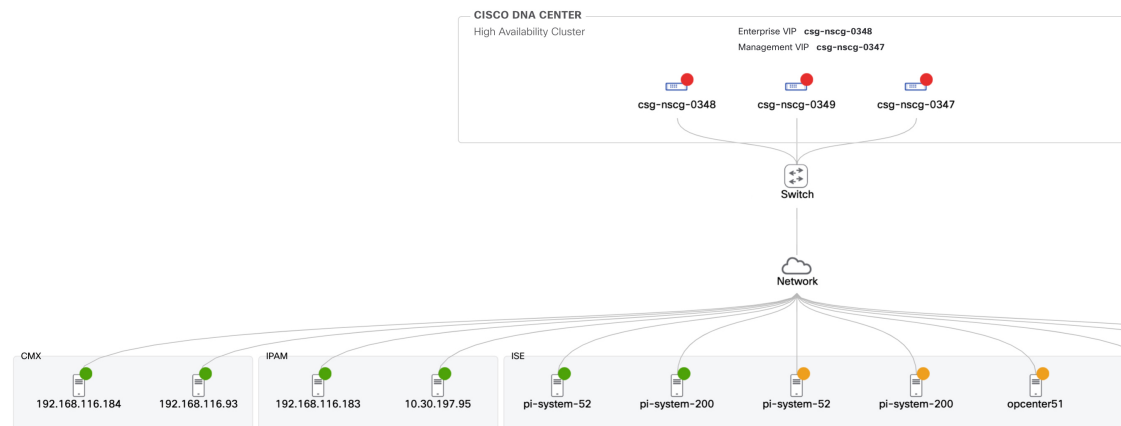
From the **System Health** page's topology, you can view a graphical representation of your Cisco DNA Center appliances and the external systems that are connected to your network, such as Cisco Connected Mobile Experiences (Cisco CMX) and Cisco Identity Services Engine (Cisco ISE). Here, you can quickly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

- [Establish Cisco IMC Connectivity, on page 19](#)
- [Subscribe to System Notification Events, on page 20](#)

To view this page, click the **Menu** icon (≡) in the Cisco DNA Center GUI and choose **System > System Health**. Your topology will look similar to the following example:

## Topology

Connectivity and health status of the Cisco DNA Center and corresponding External Systems in a topology view.



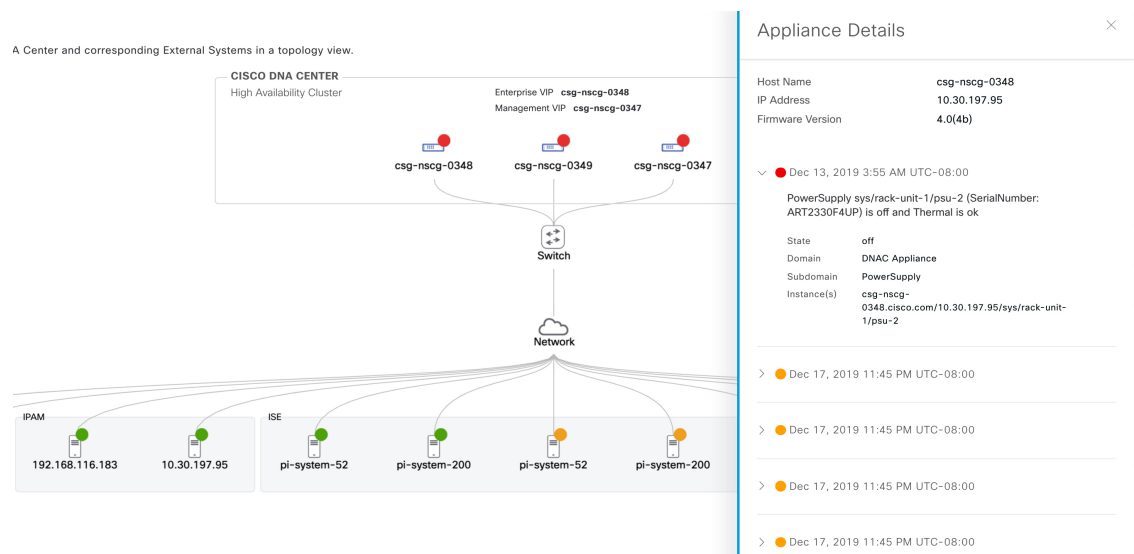
Topology data is polled every 30 seconds. If any new data is received, the topology automatically updates to reflect this data.

## Troubleshoot Appliance and External System Issues

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

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

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



## System Topology Notifications

The following tables list the various notifications that are displayed in the **System Health** page's system topology for your Cisco DNA Center appliances and any connected external systems. Notifications are grouped by their corresponding severity:

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



### Note

If all of the hardware components on an appliance are operating without any issues, an individual notification is not provided for each component. The following notification is displayed instead: *Cisco DNA Center Ok.*

**Table 2: Cisco DNA Center Appliance Notifications**

Component	Severity 1 Notification	Severity 2 Notification	Severity 3 Notification
CPU	Processor CPU1 (SerialNumber - xxxxxx) State is Disabled	Processor CPU1 (SerialNumber - xxxxxx) Health is NotOk and State is Enabled	Processor CPU1 (SerialNumber - xxxxxx) Health is Ok and State is Enabled
Disk	Driver - PD1 State is Disabled	Driver - PD1 Health is Critical and State is Enabled	Driver - PD1 Health is Ok and State is Enabled
MemoryV1	Memory Summary (TOTALSYSTEMMEMORYGIB - 256) Health is NotOk	—	Memory Summary (TOTALSYSTEMMEMORYGIB - 256) Health is Ok
MemoryV2	Storage DIMM1 (SerialNumber - xxxxx) Status is NotOperable	—	Storage DIMM1 (SerialNumber - xxxxx) Status is Operable

## Suggested Actions

Component	Severity 1 Notification	Severity 2 Notification	Severity 3 Notification
NIC	NIC Adapter Card MLOM State is Disabled	NIC Adapter Card MLOM State is Enabled and port0 is Down	NIC Adapter Card MLOM State is Enabled and port0 is Up
Power supply	PowerSupply PSU1 (SerialNumber - xxxx) State is Disabled	—	PowerSupply PSU1 (SerialNumber - xxxx) State is Enabled
RAID	Cisco 12G SAS Modular Raid Controller (SerialNumber - xxxxx) State is Disabled	Cisco 12G SAS Modular Raid Controller (SerialNumber - xxxxx) Health is NotOK and State is Enabled	Cisco 12G SAS Modular Raid Controller (SerialNumber - xxxxx) Health is OK and State is Enabled

Table 3: Connected External System Notifications

Component	Severity 1 Notification	Severity 2 Notification	Severity 3 Notification
Cisco Connected Mobile Experiences (CMX) server	—	There is a critical issue with the integrated CMX server.	CMX server is integrated and servicing.
IP address management (IPAM) server	There is a critical issue with the connected third-party IPAM provider	There is no third-party IPAM provider connected	A third-party IPAM provider is connected.
Cisco ISE—External RESTful Services (ERS)	—	ISE PAN ERS connection: ISE ERS API call unauthorized	ISE PAN ERS connection: ERS reachability with ISE - Success
Cisco ISE—Trust	—	ISE AAA Trust Establishment: Trust Establishment Error	ISE AAA Trust Establishment: Successfully established trust and discovered PSNs from PAN
IT service management (ITSM) server	Servicenow connection health status is NOT up and running	—	Servicenow connection health status is up and running

## Suggested Actions

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

Component	Subcomponent	Issue	Suggested Actions
Cisco ISE	External RESTful Services (ERS)—Reachability	Timeout elapsed (possibly because the Cisco ISE ERS API load threshold has been exceeded).	<ul style="list-style-type: none"> <li>• Check your proxy configuration for a proxy server between Cisco DNA Center and Cisco ISE.</li> <li>• Check whether you can reach Cisco ISE from Cisco DNA Center.</li> </ul>
		Unable to establish a connection with Cisco ISE.	<ul style="list-style-type: none"> <li>• Check whether a firewall is configured.</li> <li>• Check your proxy configuration for a proxy server between Cisco DNA Center and Cisco ISE.</li> <li>• Check whether you can reach Cisco ISE from Cisco DNA Center.</li> </ul>
	ERS—Availability	No response to ERS API call.	<ul style="list-style-type: none"> <li>• Check which version of Cisco ISE is installed.</li> <li>• Check if ERS is enabled on Cisco ISE. See the "Enable External RESTful Services APIs" topic in the <a href="#">Cisco Identity Services Engine Administrator Guide</a> for more information.</li> </ul>
	ERS—Authentication	Cisco ISE ERS API call is unauthorized.	Check whether the AAA settings credentials and the Cisco ISE credentials are the same.
	ERS—Configuration	Cisco ISE certificate has been changed.	From the Cisco DNA Center GUI, reestablish trust. See the "Enable PKI in Cisco ISE" topic in the <a href="#">Cisco Identity Services Engine Administrator Guide</a> for more information.
	ERS—Unclassified/Generic Error	An undefined diagnostic error occurred.	<ol style="list-style-type: none"> <li>1. Delete the AAA settings that are currently configured in Cisco DNA Center.</li> <li>2. Reenter the appropriate AAA settings. See the "Integrate Cisco ISE with Cisco DNA Center" in the <a href="#">Cisco Digital Network Architecture Center Second Generation Appliance Installation Guide</a> for more information.</li> <li>3. Reestablish trust. See the "Enable PKI in Cisco ISE" topic in the <a href="#">Cisco Identity Services Engine Administrator Guide</a> for more information.</li> </ol>
	Trust—Reachability	Unable to establish an SSH connection.	Check whether the AAA settings credentials and the Cisco ISE credentials are the same.

Component	Subcomponent	Issue	Suggested Actions
		The Cisco DNA Center endpoint URL configured for Cisco ISE certificate chain uploads is unreachable.	<ul style="list-style-type: none"> <li>• Check your proxy configuration for a proxy server between Cisco DNA Center and Cisco ISE.</li> <li>• Check whether you can reach Cisco ISE from Cisco DNA Center.</li> </ul>
	Trust—Configuration	Invalid Cisco ISE certificate chain.	<ul style="list-style-type: none"> <li>• If necessary, regenerate the Cisco ISE internal root CA chain. See the "ISE CA Chain Regeneration" topic in the <a href="#">Cisco Identity Services Engine Administrator Guide</a> for more information.</li> <li>• Ensure that the internal CA certificate chain has not been removed from Cisco ISE.</li> </ul>
		The Cisco DNA Center endpoint URL configured for Cisco ISE certificate chain uploads is forbidden.	<ul style="list-style-type: none"> <li>• Launch the URL and check whether you can access the /aaa/Cisco ISE/certificate directory on the endpoint.</li> <li>• Check whether the <b>Use CSRF Check for Enhanced Security</b> option is enabled in Cisco ISE. See the "Enable External RESTful Services APIs" topic in the <a href="#">Cisco Identity Services Engine Administrator Guide</a> for more information.</li> </ul>
	Trust—Authentication	The Cisco ISE password has expired.	<ul style="list-style-type: none"> <li>• Regenerate the Cisco ISE admin password. See the "Administrative Access to Cisco ISE" topic in the <a href="#">Cisco Identity Services Engine Administrator Guide</a> for more information.</li> <li>• Ensure that the GUI and SSH credentials configured for the admin user in Cisco ISE are the same.</li> </ul>
	Trust—Unclassified/Generic Error	An undefined diagnostic error occurred.	



Component	Subcomponent	Issue	Suggested Actions
			<ol style="list-style-type: none"> <li>1. Delete the AAA settings that are currently configured in Cisco DNA Center.</li> <li>2. Reenter the appropriate AAA settings. See the "Integrate Cisco ISE with Cisco DNA Center" in the <a href="#">Cisco Digital Network Architecture Center Second Generation Appliance Installation Guide</a> for more information.</li> <li>3. Reestablish trust. See the "Enable PKI in Cisco ISE" topic in the <a href="#">Cisco Identity Services Engine Administrator Guide</a> for more information.</li> </ol>
Cisco Connected Mobile Experiences (CMX) server IP address management (IPAM) server IT service management (ITSM) server	Reachability	Unable to establish connectivity with the server.	Check whether the server in question is currently down.
	Authentication	Unable to log in to the server.	Confirm that the correct login credentials are configured in Cisco DNA Center.
Hardware	Disk	The specified hardware component is experiencing an issue.	Replace the faulty component.
	Fan		
	Power supply		
	Memory module		
	CPU		
	Networking card		
	RAID controller		
System resources	Storage	The specified mount directory is full.	<ul style="list-style-type: none"> <li>• Clear up storage space in the current directory by removing unnecessary data.</li> <li>• Specify a new mount directory that has more storage space.</li> </ul>

# Cisco DNA Center and Cisco ISE Integration

Cisco ISE has three use cases with Cisco DNA 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 Cisco DNA Center and Cisco ISE. The process involves installing and configuring Cisco ISE with specific services, and configuring Cisco ISE settings in Cisco DNA Center. For more information about installing and configuring Cisco ISE with Cisco DNA Center, see the [Cisco DNA 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 Cisco DNA Center" in the [Cisco DNA Assurance User Guide](#).

After Cisco ISE is successfully registered and its trust established with Cisco DNA Center, Cisco DNA Center shares information with Cisco ISE. Cisco DNA Center devices that are assigned to a site that is configured with Cisco ISE as its AAA server have their inventory data propagated to Cisco ISE. Additionally, any updates on these Cisco DNA Center devices (for example, device credentials) in Cisco DNA Center also updates Cisco ISE with the changes.

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

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

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

**Note**

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

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

Cisco DNA Center polls Cisco ISE every 15 minutes. If the Cisco ISE server is down, (In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **> System > System 360**) shows the Cisco ISE server as red (unreachable).

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

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

- Cisco DNA Center and Cisco ISE integration is not supported over a proxy server. If you have Cisco ISE configured with a proxy server in your network, configure Cisco DNA Center such that it does not use the proxy server; it can do this by bypassing the proxy server's IP address.
- Cisco DNA Center and Cisco ISE integration is not currently supported through a Cisco DNA Center virtual IP address (VIP). If you are using an enterprise CA-issued certificate for Cisco DNA Center, make sure the Cisco DNA Center certificate includes the IP addresses of all interfaces on Cisco DNA Center in the Subject Alternative Name (SAN) extension. If Cisco DNA Center is a three-node cluster, the IP addresses of all interfaces from all three nodes must be included in the SAN extension of the Cisco DNA Center certificate.
- Cisco DNA Center needs access to both the Cisco ISE CLI (through an Ethernet routing switch) and GUI (through an SSH connection). Because you can define only one set of Cisco ISE credentials in Cisco DNA Center, make sure these credentials are the same for both the Cisco ISE GUI and CLI user accounts.
- Disable password expiry for the Admin user in Cisco ISE. Alternatively, make sure that you update the password before it expires. For more information, see the [Cisco Identity Services Engine Administrator Guide](#).
- When the Cisco ISE certificate changes (password, expiration, etc.), Cisco DNA Center must be updated. To do that, edit the AAA Server (Cisco ISE), reenter the password, and save. This forces Cisco DNA Center to download the certificate chain for the new admin certificate from Cisco ISE, and update Cisco DNA Center. If you are using Cisco ISE in High Availability mode, and the admin certificate changes on either the primary or secondary administrative node, you must update Cisco DNA Center. Cisco DNA Center connects to Cisco ISE via SSH and runs CLI to get the certificate info.
- Cisco DNA Center configures certificates for itself and for Cisco ISE to connect over pxGrid. You can use other certificates with pxGrid for connections to other pxGrid clients, such as Firepower. These other connections will not interfere with the Cisco DNA Center and Cisco ISE pxGrid connection.
- To change the RADIUS Secret Password: You provided the secret password when you configured Cisco ISE as an AAA Server on the **System > Settings > External Services > Authentication and Policy Servers** page. To change the secret password, navigate to **Design > Network Settings > Network**, and click the **Change Shared Secret** link. This causes Cisco ISE to use the new secret password when connecting to network devices managed by Cisco DNA Center.

## Anonymize Data

Cisco DNA 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.

Make sure 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 is not anonymized.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System > Settings > Trust & Privacy > Anonymize Data**.  
The Anonymize Data window is displayed.
- Step 2** 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, so on.
- 

## Configure Authentication and Policy Servers

Cisco DNA 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 Cisco DNA Center and Cisco ISE are integrated, as described in the [Cisco DNA Center Installation Guide](#).
- If you are using another product (not Cisco ISE) to perform AAA functions, make sure to do the following:
  - Register Cisco DNA Center with the AAA server, including defining the shared secret on both the AAA server and Cisco DNA Center.
  - Define an attribute name for Cisco DNA Center on the AAA server.
  - For a Cisco DNA 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:
  1. You deployed Cisco ISE version 2.3 or later in your network. If you have a multihost Cisco ISE deployment, integrate with the Cisco ISE admin node.
  2. SSH is enabled on the Cisco ISE node.
  3. The pxGrid service is enabled on the Cisco ISE host with which you plan to integrate Cisco DNA Center, and the ERS service is enabled for read/write operations.




---

**Note** Cisco ISE versions 2.4 and later supports pxGrid 2.0 and pxGrid 1.0. Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Cisco DNA Center does not currently support more than two pxGrid nodes.

---

4. The Cisco ISE GUI and Cisco ISE shell username and passwords are the same.

5. There is no proxy configured between Cisco DNA Center and Cisco ISE. If a proxy server is configured on Cisco ISE, the Cisco DNA Center IP address must bypass that proxy server.
6. There is no firewall between Cisco DNA Center and Cisco ISE. If there is a firewall, open the communication between Cisco DNA Center and Cisco ISE.
7. A ping between Cisco DNA Center and Cisco ISE succeeds with both the IP address and hostname.
8. The Cisco ISE admin node certificate contains the Cisco ISE IP address or FQDN in either the certificate subject name or the SAN.
9. If a third-party certificate is used, the certificate includes all IP addresses in the SAN field.
10. The pxGrid approval is set for automatic or manual approval in Cisco ISE to enable the pxGrid connection in Cisco DNA Center.

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > External Services > Authentication and Policy Servers**.

**Step 2** Click  **Add**.

**Step 3** Configure the primary AAA server by providing the following information:

- **Server IP Address:** IP address of the AAA server.
- **Shared Secret:** Key for device authentications. The shared secret can be up to 128 characters in length.

**Step 4** To configure a AAA server (not Cisco ISE), leave the **Cisco ISE Server** toggle to **Off** and proceed to the next step. To configure a Cisco ISE server, set the **Cisco ISE server** toggle to **On** and enter information in the following fields:

- **Username:** Name that is used to log into the Cisco ISE CLI.

**Note** This user must be a Super Admin.

- **Password:** Password for the Cisco ISE CLI username.
- **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*

Example: The FQDN for a Cisco ISE server can be ise.cisco.com.

- **SSH Key:**

The SSH key is a Diffie-Hellman crypto key in base64 encoded format. This key provides security for SSH connections to the Cisco ISE Administration console. You can retrieve the key with the Cisco ISE CLI command **show crypto authorized\_keys** and **show crypto host\_keys**.

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.

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

Cisco ISE server registration phase:

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

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** page: "Active"
- **System 360** page: "Primary Available" and "PXGRID Available"

If the status of the configured ISE server is "FAILED" due to password change, click **Retry**, and update the password to re-sync the ISE connectivity.

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

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

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

- **Authentication Port:** Port used to relay authentication messages to the AAA server. The default is UDP port 1812.
- **Accounting Port:** Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. The default UDP port is 1813.
- **Port:** Port used by TACAS. The default port is 49.
- **Retries:** Number of times that Cisco DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
- **Timeout:** Length of time the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

**Step 6** Click **Add**.

**Step 7** To add a secondary server, repeat Step 2 through Step 6.

## Configure Cisco AI Network Analytics Data Collection

Use this procedure to enable Cisco AI Network Analytics to export network event data from wireless controllers as well as the site hierarchy to the Cisco DNA Center.

### Before you begin

- Make sure that you have the Cisco DNA Advantage software license for Cisco DNA Center. The **AI Network Analytics** application is part of the Cisco DNA Advantage software license.
- Make sure that you have downloaded and installed the **AI Network Analytics** application. See [Download and Install Packages and Updates](#), on page 68.
- 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** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System > Settings**.

**Step 2** Scroll down to **System Configuration** and choose **AI Network Analytics**.  
The **AI Network Analytics** window appears.

*Figure 3: AI Network Analytics Window*

## AI Network Analytics

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

Configure

Recover from a config file ⓘ

**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 appears.
  - 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 appears.
- If this is the first time you are configuring 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**.

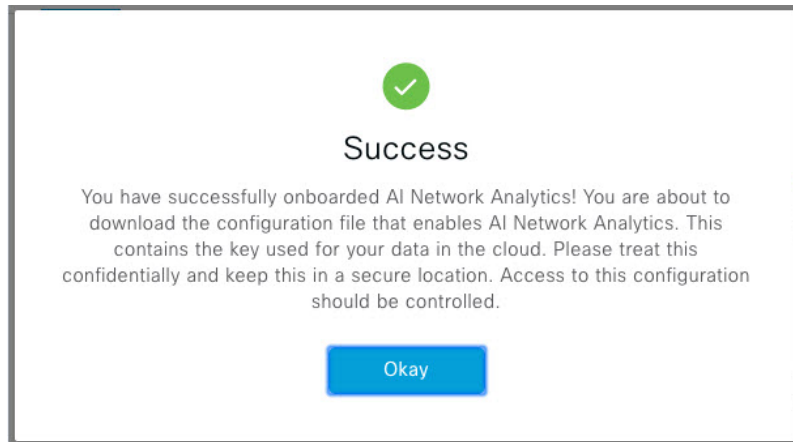
- c. Click **Next**.

The terms and conditions window appears.

- 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 appears.

**Figure 4: Success Dialog Box**




- Step 4** In the **Success** dialog box, click **Okay**.  
The **AI Network Analytics** window appears, and the **Cloud Connection** area displays ☒.
- Step 5** (Recommended) In the **AI Network Analytics** window, click **Download Configuration** file.

---

## Disable Cisco AI Network Analytics Data Collection

To disable the Cisco AI Network Analytics data collection, you must turn off (disable) the connection to the Cisco AI Network Analytics cloud service. This will disable all of the Cisco AI Network Analytics related features, such as AI-Driven Issues, Network Heatmap, Site Comparison, and Peer Comparison.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings**.
  - Step 2** Scroll down to **System Configuration** and choose **AI Network Analytics**.  
The **AI Network Analytics** window appears.
  - Step 3** In the **Cloud Connection** area, click the button to off, such that ☐ appears.



*Figure 5: AI Network Analytics Window with Data Collection Disabled*

## AI Network Analytics

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

Cloud Connection ⓘ



Update

Cloud Data Storage  
Europe (Germany)

[Download configuration file](#)

- 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** (Optional) 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 Cisco DNA Center to automatically update the Machine Reasoning Knowledge Base on a daily basis, or you can perform a manual update.

**Step 1** In the Cisco DNA Center GUI, 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 is a new update to the Machine Reasoning Knowledge Base, the **AVAILABLE UPDATE** area appears 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 Cisco DNA Center on a daily basis.

**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 Cisco DNA Center is successfully connected to the Machine Reasoning Engine in the cloud.

**Step 4** To manually update the Machine Reasoning Knowledge Base in Cisco DNA 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 Cisco DNA 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 Cisco DNA Center.

## Cisco Accounts

### Configure Cisco Credentials

You can configure Cisco credentials for Cisco DNA 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 Cisco DNA 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. For more information, see [About User Roles, on page 71](#).

**Step 1** In the Cisco DNA Center GUI, 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 is configured to the software and services.

## Clear Cisco Credentials

To delete the cisco.com credentials that are currently configured for Cisco DNA 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 will 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 Cisco DNA Center. Otherwise, you will 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 42](#) 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 71](#).

- 
- Step 1** In the Cisco DNA Center GUI, 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

The Connection mode manages the connections between smart-enabled devices in your network that interact with Cisco DNA Center and the CSSM. Ensure that you have SUPER-ADMIN access permission to configure the different connection modes.

**Before you begin**

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System > Settings > Cisco Accounts > Connection Mode**.
- Step 2** You can choose either of the following connection modes:
- **Direct**
  - **On-Prem CSSM**
  - **Smart Proxy**
- Step 3** Choose **Direct** to enable direct connection to the Cisco SSM cloud.
- Step 4** 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) Enter the details of **On-Prem CSSM Host**, **Smart Account Name**, **Client Id**, and **Client Secret**.

- b) Click **Test Connection** to validate the CSSM connection.
- c) Click **Save** and then **Confirm**. If there are any smart-enabled devices in your network which are already registered with CSSM, then those devices would be de-registered from CSSM.

**Note** To enable **On-Prem CSSM**, make sure that the satellite is deployed, up, and running in your network site.

**Step 5** **Smart Proxy** allows you to register your smart enabled devices with Cisco SSM cloud through DNA Center. With this mode, devices need not have direct connection to Cisco SSM Cloud. DNA Center will proxy the requests from device to Cisco SSM cloud through itself.

---

## Register Plug and Play


You can register Cisco DNA 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 Cisco DNA 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** In the Cisco DNA Center GUI, 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 account from the **Select Virtual Account** drop-down list.
- Step 4** Click the required **Controller** radio button.
- Step 5** Enter the IP address or FQDN (Fully Qualified Domain Name).
- Step 6** Enter the profile name. A profile is created for the selected virtual account with the configuration you provided.
- Step 7** Click **Save**.
- 

## 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** In the Cisco DNA Center GUI, 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 will be automatically registered to the selected virtual account.
- 

## Smart Licensing

Smart Licensing is a cloud-based, software license management solution that allows you to manage and track the status of your license and software usage. To enable smart licensing, you need to upload Cisco DNA Center license conventions in CSSM.

### Before you begin

You should have configured Cisco Credentials to enable Smart Licensing. See [Configure Cisco Credentials, on page 36](#).

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System > Settings > Cisco Accounts > Smart License Enablement**.
- By default, **Smart User** and **Smart Domain** details are displayed.
- Step 2** Select 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 Cisco DNA Center licenses.
- 

## Device Controllability

Device Controllability is a system-level process on Cisco DNA Center that enforces state synchronization for some device-layer features. Its purpose is to aid in the deployment of network settings that Cisco DNA 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 are pushed to the device, go to **Provision > Inventory** and choose **Provision** from the **Focus** drop-down list. Click **See Details** in the **Provision Status** column.



**Note** When Cisco DNA Center configures or updates devices, the transactions are captured in the Cisco DNA Center audit logs. You can use the audit logs to track changes and troubleshoot issues. For more information about the Cisco DNA Center audit logs, see [View Audit Logs, on page 48](#).

The following device settings will be 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 **Global** site is configured with Cisco ISE as AAA. Otherwise it is pushed to devices during "Assign to Site" when the site is configured with Cisco ISE as AAA.

- IPDT Enablement

- **Assigning Devices to a Site**

- Controller Certificates
- SNMP Trap Server Definitions
- Syslog Server Definitions
- NetFlow Server Definitions
- Wireless Service Assurance (WSA)

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 41](#).

When Device Controllability is disabled, Cisco DNA Center does not configure any of the credentials or features listed above on devices while running Discovery or when the devices are assigned to a site. However, the telemetry settings and related configuration are pushed when the device is provisioned or when **Update Telemetry Settings** action is performed from **Provision > Inventory > Actions**. At the time of the network settings creation on the site, if Device Controllability is enabled, the associated devices are configured accordingly.

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.
- **Device in Global Site:** When you successfully add, import, or discover a device, Cisco DNA 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, Cisco DNA 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, Cisco DNA 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, Cisco DNA Center does not remove the SNMP server, Syslog server, and NetFlow collector settings from the device.
- **Device Deleted from Cisco DNA Center:** If you delete a device from the Cisco DNA Center, then the SNMP server, Syslog server and NetFlow collector settings are removed from the device, only if you check the **Configuration Clean-up** check box.
- **Device Moved from Site to Site:** If you move a device—for example, from Site A to Site B—Cisco DNA 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 **Update Telemetry Settings** action is performed, even if device controllability is not enabled.

## Configure Device Controllability

Device controllability aids deployment of the required network settings that Cisco DNA Center needs to manage devices.

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



**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.

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles](#), on page 71.


- 
- Step 1** In the Cisco DNA Center GUI, 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** In the Cisco DNA Center GUI, 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**.
- 

## Cloud Access Keys

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

### Before you begin

- Obtain the access key ID and secret key from the Amazon Web Services (AWS) console.
- Subscribe to CSR or WLC products in the AWS marketplace and verify the image ID for the target region.
- Identify the key pair that CSRs will use during HA failover on AWS. The key pair's name is selected from a list in Cisco DNA Center when provisioning CSRs in that region.
- Identify the IAM role that CSRs will use during HA failover on AWS. The IAM role is selected from a list in Cisco DNA Center when provisioning CSRs.
- Configure the proxy for Cisco DNA Center to communicate with AWS via HTTPS REST APIs. See [Configure the Proxy, on page 50](#).
- The Cloud Connect extension to the eNFV app is enabled by deploying a separate Cloud Device Provisioning Application package. The package is not included by default in the standard Cisco DNA Center installation. You must download and install the package from a catalog server. For more information, see [Download and Install Packages and Updates, on page 68](#).

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > Cloud Access Keys**.



- Step 2** Click  **Add**.
- Step 3** Enter the **Access Key Name** and choose the **Cloud Platform** from the drop-down list. Enter the **Access Key ID** and **Secret Key** obtained from the AWS console.
- Step 4** Click **Save and Discover**.
- 

#### What to do next

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

## Integrity Verification

Integrity Verification (IV) monitors key device data for unexpected changes or invalid values that indicate possible compromise, if any, of the device. The objective is to minimize the impact of a compromise by substantially reducing the time to detect unauthorized changes to a Cisco device.

**Note**

For this release, IV runs integrity verification checks on software images that are uploaded into Cisco DNA 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/cscrd/security/center/files/trust/Cisco\\_KnownGoodValues.tar](https://tools.cisco.com/cscrd/security/center/files/trust/Cisco_KnownGoodValues.tar)

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

**Note**

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

---

**Before you begin**

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

**Step 1** In the Cisco DNA Center GUI, 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:** Cisco DNA 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 Cisco DNA Center.

**Note** A secure connection to <https://tools.cisco.com> is made using the certificates added to Cisco DNA 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 Cisco DNA Center.

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

IV automatically downloads the latest KGV file from cisco.com to your system 7 days after Cisco DNA 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 Cisco DNA 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.

---

#### 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 Cisco DNA Center to communicate with an external IP address manager. When you use Cisco DNA Center to create, reserve, or delete any IP address pool, Cisco DNA Center conveys this information to your external IP address manager.

#### Before you begin

- You should have an external IP address manager already set up and functional.
- Import the IPAM certificate manually to the trustpool.

---

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **System > Settings > External Services > IP Address Manager**.

**Step 2** In the **IP Address Manager** section, enter the required information in the following fields:

- **Server Name:** Name of server.
- **Server URL:** IP address of server.
- **Username:** Required username for server access.
- **Password:** Required password for server access.
- **Provider:** Choose a provider from the drop-down list.

**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.

- **View:** Choose a view from the drop-down list. If you only have one view configured, only **default** appears in the drop-down list.

**Step 3** Click **Apply** to apply and save your settings.

### What to do next

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

## Configure Debugging Logs

To assist in troubleshooting service issues, you can change the logging level for the Cisco DNA 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 Cisco DNA Center host. From this location, Cisco DNA Center can query and display logs in the GUI. The total compressed size of the log files is 2 GB. If the log files exceed 2 GB, the newer log files overwrite the older ones.

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > System Configuration > Debugging Logs**.

The **Debugging Logs** window displays the following fields:

- **Services**

- **Logger Name**
- **Logging Level**
- **Timeout**

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

The **Services** drop-down list displays the services that are currently configured and running on Cisco DNA 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.

Cisco DNA 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 **Timeout** 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 **Apply**.

(To cancel your selection, click **Cancel**.)


---

## Configure the Network Resync Interval

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

### Before you begin


- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

- 
- Step 1** In the Cisco DNA Center GUI, 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 Cisco DNA Center. Audit logs also capture information about device public key infrastructure (PKI) notifications. The information in these audit logs can be used to assist in troubleshooting issues, if any, involving the applications or the device PKI 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** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Activity > Audit Logs**.
- The **Audit Logs** window appears, where you can view logs about the current policies in your network. These policies are applied to network devices by the applications installed on Cisco DNA Center.
- Step 2** Click the timeline slider to specify the time range of data you want displayed on the window:
- In the **Time Range** area, choose a time range: Last 2 Weeks, Last 7 Days, Last 24 Hours, or Last 3 Hours.
  - To specify a custom range, click **By Date** and specify the start and end date and time.
  - 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 Cisco DNA Center. Child audit logs are subtasks to a task performed by Cisco DNA 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 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 [Cisco DNA Center Platform Intent APIs](#).
- Step 5** (Optional) Click **Filter** to filter the log by user ID or event ID.

- Step 6** In the right pane, use the **Search** field to search for specific text in the log message.
- Step 7** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Activity > Scheduled Tasks** to view upcoming, in progress, completed, and failed administrative tasks, such as OS updates or device replacements.
- 

## Activate High Availability

Complete the following procedure in order to activate high availability (HA) on your Cisco DNA Center cluster:

- Step 1** Click the **Menu** icon (≡) in the Cisco DNA Center GUI and choose **System > Settings > System Configuration > High Availability**.
- Step 2** Click **Activate High Availability**.
- For more information about HA, see the [Cisco DNA Center High Availability Guide](#).
- 

## Configure Integration Settings

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

### Before you begin

You have installed the Cisco DNA Center platform as described in the previous section.


- Step 1** Enter the **Callback URL Host Name** or **IP Address** that the third-party app needs to connect to when communicating with the Cisco DNA Center platform.
- Note** The **Callback URL Host Name** or **IP Address** is the external facing host name or IP address that is mapped internally to Cisco DNA Center. Configure the VIP address for a three node cluster setup.
- Step 2** Click the **Apply** button.
- 

## Set Up a Login Message

You can set a message that appears to all the users when they log in to Cisco DNA Center.

**Before you begin**

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


- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > System Configuration > Login Message**.
- Step 2** Enter a text message in the **Login Message** text box.
- Step 3** Click **Save**.
- The message appears when you log in to Cisco DNA Center.
- Step 4** If you want to remove the login message, click **Clear** in the **Login Message** screen.
- Step 5** Click **Save** to update the settings.
- 

## Configure the Proxy

If Cisco DNA Center has a proxy server configured as an intermediary between itself and the network devices it manages or the Cisco cloud from which it downloads software updates, you must configure access to the proxy server. You configure access using the **Proxy Config** window in the Cisco DNA Center GUI.

**Before you begin**

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > System Configuration > Proxy Config**.
- Step 2** Enter the proxy server's URL address.
- Step 3** Enter the proxy server's port number.
- For HTTP, the port number is usually 80.
- Step 4** (Optional) If the proxy server requires authentication, enter the username and password for access to the proxy server.
- Step 5** Check the **Validate Settings** check box to have Cisco DNA Center validate your proxy configuration settings when applying them.
- Step 6** Review your selections and click **Save**.

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

Note the following:

- After configuring the proxy, you are able to view the configuration in the **Proxy Config** window.
- If SSL decryption is enabled on the proxy server that is configured between Cisco DNA Center and the Cisco cloud from which it downloads software updates, or a proxy is configured between Cisco DNA Center and the devices that it manages, proceed to Step 7.



- If SSL decryption is *not* enabled on the proxy server that is configured between Cisco DNA Center and the Cisco cloud from which it downloads software updates, you can stop here.

**Step 7** Import the proxy certificate into Cisco DNA Center.

See [Configure Proxy Certificate, on page 53](#).

---

## Security for Cisco DNA Center

Cisco DNA Center provides many security features for itself, as well as 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 Cisco DNA Center behind a firewall that does not expose the management ports to an untrusted network, such as the internet.
- Replace the self-signed server certificate from Cisco DNA Center with one signed by a well-known certificate authority (CA).
- Upgrade Cisco DNA Center with critical upgrades, including security patches, as soon as possible after a patch announcement.
- Open the DNS access control list (ACL) and ports that are used by Cisco DNA Center, coupled with known IP address ranges.



---

**Note** We recommend that you configure a proxy gateway between Cisco DNA Center and the network devices it monitors and manages.

---

## Change the TLS Version and Enable RC4-SHA (Not Secure)

Northbound REST API requests from the external network to Cisco DNA Center (from northbound REST API-based apps, browsers, and network devices connecting to Cisco DNA Center using HTTPS) are made secure using the Transport Layer Security (TLS) protocol. You have an option to change the TLS version and enable RC4-SHA (a stream cipher) if your network devices under Cisco DNA Center control cannot support the existing TLS version or ciphers. For security reasons, however, we do not recommend that you downgrade your TLS version or enable RC4-SHA ciphers.

If you need to change the TLS version or enable RC4-SHA for Cisco DNA Center, you do so by logging in to the appliance and using the CLI.



---

**Note** CLI commands can change from one release to the next. The following CLI example uses command syntax that might not apply to all Cisco DNA Center releases.

---

**Before you begin**

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



**Important** This security feature applies to port 443 on Cisco DNA Center. Performing this procedure may disable traffic on the port to the Cisco DNA Center infrastructure for a few seconds. For this reason, you should configure TLS infrequently and only during off-peak hours or during a maintenance period.

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

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

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

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

**Example**

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

**Step 4** If you want to change the TLS version on the cluster, enter the following commands. For example, you might want to change the current TLS version to a lower version if your network devices under Cisco DNA Center control cannot support the existing TLS version.

**Example: Change from TLS version 1.1 to 1.0**

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

**Example: Change from TLS version 1.1 to 1.2 (only allowed if you haven't enabled RC4-SHA)**

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

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

**Step 5** Enter the following command to enable RC4-SHA on the cluster (not secure; proceed only if needed).

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

**Example: TLS version 1.2 is not enabled**

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

```
Enabling RC4-SHA cipher will have security risk
Do you want to continue? [y/N]: y
WARNING: Enabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

**Step 6** Enter the following command at the prompt to confirm that TLS and RC4-SHA are configured.

**Example**

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

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

**Step 7** If you want to disable the RC4-SHA ciphers that you enabled previously, enter the following command on the cluster.

```
Input
$ magctl service ciphers --ciphers-rc4=disable kong
Output
WARNING: Disabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

**Step 8** Log out of the Cisco DNA Center appliance.

---

## Configure Proxy Certificate

In some network configurations, proxy gateways might exist between Cisco DNA 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 Cisco DNA Center terminate at the proxy gateway. Therefore, the network devices located within these remote networks can only communicate with Cisco DNA Center through the proxy gateway. For the network devices to establish secure and trusted connections with Cisco DNA 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 Cisco DNA Center server certificate be the same so that network devices can trust and authenticate Cisco DNA Center securely.

In network topologies where a proxy gateway is present between Cisco DNA Center and the remote network it manages, perform the following procedure to import a proxy gateway certificate in to Cisco DNA Center.

**Before you begin**

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).
- You must use the proxy gateway's IP address to reach Cisco DNA 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 Cisco DNA Center by following this procedure.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System > Settings > Trust & Privacy > Proxy Certificate**.
- Step 2** 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 will appear in Cisco DNA Center's GUI two months before the date and time at which the certificate expires.
- Step 3** 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 Cisco DNA Center using this area. Additionally, private keys are neither required nor uploaded into Cisco DNA Center for this procedure.
- Step 4** Click **Save**.
- Step 5** 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 6** Click the **Enable** button to enable the proxy gateway certificate functionality.
- If you click the **Enable** button, the controller will return the imported proxy gateway certificate when requested by a proxy gateway. If you don't click the **Enable** button, the controller will return 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.
- 

## Certificate and Private Key Support

Cisco DNA Center supports the PKI Certificate Management feature, which is used to authenticate sessions (HTTPS). These sessions use commonly recognized trusted agents called CAs. Cisco DNA Center uses the PKI Certificate Management feature to import, store, and manage X.509 certificates from well-known CAs. The imported certificate becomes an identity certificate for Cisco DNA Center, and Cisco DNA 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 PEM or PKCS file format) using the Cisco DNA Center GUI:

- X.509 certificate

- Private key



**Note** For the private key, Cisco DNA Center supports the import of RSA keys. You should not import DSA, DH, ECDH, and ECDSA key types, because they are not supported. You should also keep the private key secure in your own key management system. The private key must have a minimum modulus size of 2048 bits.

Prior to import, you must obtain a valid X.509 certificate and private key issued by a well-known CA and the certificate must correspond to a private key in your possession. After import, the security functionality based on the X.509 certificate and private key is automatically activated. Cisco DNA 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 Cisco DNA Center.



**Note** We recommend that you do not use and import a self-signed certificate into Cisco DNA Center. We recommend that you import a valid X.509 certificate from a well-known CA. Additionally, you must replace the self-signed certificate (installed in Cisco DNA Center by default) with a certificate that is signed by a well-known CA for the PnP functionality to work correctly.

Cisco DNA 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

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



**Note** If you install a third-party certificate, ensure that the certificate specifies all of the IP addresses (for both physical ports and VIPs) and DNS names that are used to access Cisco DNA Center in the **alt\_names** section. For more information, see "Generate a Certificate Request Using Open SSL" in the [Cisco DNA Center Security Best Practices Guide](#).

- **Issuing (subordinate) CA certificate that issues the Cisco DNA Center certificate:** Its Subject field has CN of the (subordinate) CA that issues the Cisco DNA 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 Cisco DNA Center Server Certificate

Cisco DNA Center supports the import and storage of an X.509 certificate and private key into Cisco DNA Center. After import, the certificate and private key can be used to create a secure and trusted environment between Cisco DNA Center, northbound API applications, and network devices.

You can import a certificate and a private key using the **Certificate** window in the GUI.

### Before you begin

you must obtain a valid X.509 certificate issued by a well-known CA and the certificate must correspond to a private key in your possession.

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > Trust & Privacy > Certificate**.

**Step 2** In the **Certificate** window, view the current certificate data.

When you first view this window, the current certificate data that is displayed is the Cisco DNA 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 appears in the Cisco DNA Center GUI two months before the certificate expires.

The additional fields that are displayed in the **Certificate** window include:

- **Current Certificate Name:** Name of the current certificate
- **Issuer:** Name of the entity that has signed and issued the certificate
- **Certificate Authority:** Either self-signed or the name of the CA
- **Expires On:** Expiry date of the certificate

**Step 3** To replace the current certificate, click **Replace Certificate**.

The following new fields appear:

- **Certificate:** Fields to enter certificate data
- **Private Key:** Fields to enter private key data

**Step 4** From the **Certificate** drop-down list, choose the file format type for the certificate that you are importing into Cisco DNA Center:

- **PEM:** Privacy-enhanced mail file format
- **PKCS:** Public-Key Cryptography Standard file format

**Step 5** If you choose **PEM**, perform the following tasks:

- For the **Certificate** field, import the **PEM** file by dragging and dropping the file into the **Drag n' Drop a File Here** area.

**Note** A PEM file must have a valid PEM format extension (.pem, .cert, .crt). The maximum file size for the certificate is 10 KB.

- For the **Private Key** field, import the private key by dragging and dropping the file into the **Drag n' Drop a File Here** area.
  - Choose the encryption option from the **Encrypted** drop-down list for the private key.
  - If you chose encryption, enter the passphrase for the private key in the **Passphrase** field.

**Note** Private keys must have a valid private key format extension (.pem or .key).

**Step 6** If you choose **PKCS**, perform the following tasks:

- For the **Certificate** field, import the **PKCS** file by dragging and dropping the file into the **Drag n' Drop a File Here** area.

**Note** A PKCS file must have a valid PKCS format extension (.pfx, .p12). The maximum file size for the certificate is 10 KB.

- For the **Certificate** field, enter the passphrase for the certificate in the **Passphrase** 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 passphrase for the private key in the **Passphrase** field.

**Step 7** Click **Upload/Activate**.

**Step 8** Return to the **Certificate** window to view the updated certificate data. The information displayed in the **Certificate** window should have changed to reflect the new certificate name, issuer, and the certificate authority.

## Certificate Management

### Configure the Device Certificate Lifetime

Cisco DNA Center lets you change the certificate lifetime of network devices that are managed and monitored by the private (internal) Cisco DNA Center CA. The Cisco DNA Center default value for the certificate lifetime is 365 days. After the certificate lifetime value is changed using the Cisco DNA Center GUI, network devices that subsequently request a certificate from Cisco DNA Center are assigned this lifetime value.



**Note** The device certificate lifetime value cannot exceed the CA certificate lifetime value. Additionally, 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.

You can change the device certificate lifetime using the **PKI Certificate Management** window in the GUI.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System > Settings > Trust & Privacy > PKI Certificate**.
- Step 2** Click the **Device Certificate** tab.
- Step 3** Review the device certificate and the current device certificate lifetime.
- Step 4** In the **Device Certificate Lifetime** field, enter a new value, in days.
- Step 5** Click **Apply**.
- Step 6** (Optional) Refresh the **PKI Certificate Management** window to confirm the new device certificate lifetime value.
- 

## Change the Role of the PKI Certificate from Root to Subordinate

The device PKI CA, a private CA that is provided by Cisco DNA Center, manages the certificates and keys used to establish and secure server-client connections. To change the role of the device PKI CA from a root CA to a subordinate CA, complete the following procedure.

When changing the private Cisco DNA Center CA from a root CA to a subordinate CA, note the following:

- If you intend to have Cisco DNA 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 Cisco DNA Center as a subordinate CA.
- As long as the subordinate CA is not fully configured, Cisco DNA Center continues to operate as an internal root CA.
- You must generate a Certificate Signing Request file for Cisco DNA Center (as described in the following procedure) and have it manually signed by your external root CA.




---

**Note** Cisco DNA 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 Cisco DNA Center using the GUI (as described in the following procedure).

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

- The switchover from the internal root CA to the subordinate CA used by managed devices is not automatically supported. Therefore, it is assumed that no devices have been configured with the internal root CA yet. If devices are configured, it is the responsibility of the network administrator to manually revoke the existing device ID certificates before switching to the subordinate CA.
- 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 next July, 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. Due to 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.

You can change the role of the private (internal) Cisco DNA Center CA from a root CA to a subordinate CA using the **PKI Certificate Management** window in the GUI.

### Before you begin

You must have a copy of the root CA certificate.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > PKI Certificate**.
- 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).
  - **Change to Sub CA mode:** Enables a change from a root CA to a subordinate CA.
- Step 4** In the **CA Management** tab, for **Change to Sub CA mode**, click **Yes**.
- Step 5** Click **Next**.
- Step 6** Review the **Root CA to Sub CA** warnings that appear:
- 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 7** Click **OK** to proceed.
- The **PKI Certificate Management** window displays the **Import External Root CA Certificate** field.
- Step 8** Drag and drop your root CA certificate into the **Import External Root CA Certificate** field and click **Upload**.
- The root CA certificate is uploaded into Cisco DNA Center and used to generate a Certificate Signing Request. After the upload process finishes, a `Certificate Uploaded Successfully` message appears.
- Step 9** Click **Next**.
- Cisco DNA Center generates and displays the Certificate Signing Request.
- Step 10** View the Cisco DNA 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 11** 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 Cisco DNA Center.
- Step 12** After receiving the subordinate CA file from your root CA, access the Cisco DNA Center GUI again and return to the **PKI Certificate Management** window.
- Step 13** Click the **CA Management** tab.
- Step 14** Click **Yes** for the **Change CA mode** button.  
After clicking **Yes**, the GUI view with the Certificate Signing Request is displayed.
- Step 15** Click **Next**.  
The **PKI Certificate Management** window displays the **Import Sub CA Certificate** field.
- Step 16** Drag and drop your subordinate CA certificate into the **Import Sub CA Certificate** field and click **Apply**.  
The subordinate CA certificate is uploaded into Cisco DNA Center.  
After the upload finishes, the GUI displays the subordinate CA mode under the **CA Management** tab.
- Step 17** 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

Cisco DNA Center lets you apply a subordinate certificate as a rollover subordinate CA when 70 percent of the existing subordinate CA's lifetime has elapsed.

### Before you begin

- To initiate subordinate CA rollover provisioning, you must have changed the PKI certificate role to subordinate CA mode. See [Change the Role of the PKI Certificate from Root to Subordinate, on page 58](#).
- Seventy percent or more of the lifetime of the current subordinate CA certificate must have expired. When this occurs, Cisco DNA Center displays a **Renew** button under the **CA Management** tab.
- You must have a signed copy of the rollover subordinate CA PKI certificate.

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > Trust & Privacy > PKI Certificate**.

**Step 2** Click the **CA Management** tab.

**Step 3** 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 4** Click **Renew**.

Cisco DNA Center uses the existing subordinate CA to generate and display the rollover subordinate CA Certificate Signing Request.

**Step 5** 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 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 6** 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 Cisco DNA 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 7** After receiving the rollover subordinate CA file from your root CA, return to the **PKI Certificate Management** window.

**Step 8** Click the **CA Management** tab.

**Step 9** Click **Next** in the GUI in which the Certificate Signing Request is displayed.

The **PKI Certificate Management** window displays the **Import Sub CA Certificate** field.

**Step 10** 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 Cisco DNA Center.

After the upload finishes, the GUI changes to disable the **Renew** button under the **CA Management** tab.

---

## Renew Certificates

Cisco DNA 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. Cisco DNA 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 Cisco DNA 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 Trustpool

Cisco DNA Center contains a preinstalled Cisco trustpool bundle (Cisco Trusted External Root Bundle). Cisco DNA Center also supports the import and storage of an updated trustpool bundle from Cisco. The trustpool bundle is used by supported Cisco networking devices to establish a trust relationship with Cisco DNA Center and its applications.




**Note** The Cisco trustpool 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 trustpool bundle is available on the Cisco cloud (Cisco InfoSec). The link is located at <https://www.cisco.com/security/pki/>.

The trustpool 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 Cisco DNA Center certificate. The trustpool bundle is used by Cisco DNA Center to validate its own certificate as well as a proxy gateway certificate (if any), to determine whether it is a valid CA-signed certificate. Additionally, the trustpool bundle is available for upload to Network


PnP-enabled devices at the beginning of their PnP workflow so that they can trust Cisco DNA Center for subsequent HTTPS-based connections.

You import the Cisco trust bundle using the **Trustpool** window in the GUI.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > Trust & Privacy > Trustpool**.
- Step 2** In the **Trustpool** window, click the **Update** button to initiate a new download and install of the trustpool bundle.
- The **Update** button becomes active only when an updated version of the ios.p7b file is available and internet access is available.
- After the new trustpool bundle is downloaded and installed on Cisco DNA Center, Cisco DNA Center makes this trustpool 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.
- 

## Configure the SFTP Server

The SFTP server can be used as a backup of an internal file server. The local SFTP server in Cisco DNA Center supports secure ciphers.


- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > Device Settings > SFTP**.
- Step 2** Configure the SFTP settings:
- **Host:** Hostname or IP address of the SFTP server.
  - **Username:** Name that is used to log in to the SFTP server. The username must have read/write privileges on the working root directory on the server.
  - **Password:** Password that is used to log in to the SFTP server.
  - **Port Number:** Port number on which the SFTP server is running.
  - **Root Location:** Working root directory for file transfers.
- Step 3** Because some legacy wireless controller software versions support only weak ciphers (such as SHA1-based ciphers) for SFTP, Cisco DNA 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 Cisco DNA Center SFTP server for up to 90 days. To allow weak ciphers, check the **Compatibility mode** check box and then enter a duration (from 1 minute to 90 days).
- Step 4** Click **Save**.
- Step 5** Review the new SFTP settings in the **SFTP** window.
-

# Configure SNMP Properties

You can configure retry and timeout values for SNMP.

## Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

- 
- Step 1** In the Cisco DNA Center GUI, 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 Cisco DNA 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 **Apply**.
- Step 4** (Optional) To return to the default settings, click **Revert to Defaults**.
- 

# About Product Usage Telemetry Collection


The Cisco DNA Center collects product usage telemetry and provides valuable data about the status and capabilities of Cisco DNA Center appliance. The data and insights enable Cisco to proactively address operational and product usage issues. The product usage telemetry data is locally collected in the Cisco DNA Center appliance and is sent to Cisco Connected DNA. All data transmitted to Cisco is through an encrypted channel. The encrypted channel is also used for other purposes such as cloud-delivered software updates.



---

**Note** Product usage telemetry collection cannot be disabled.

---

In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings**, and then choose **Terms and Conditions > Telemetry Collection**. You can review the license agreement, the privacy data, and the Cisco privacy statement from the **Telemetry Collection** page.

The collection of product usage telemetry will be enabled by default. We recommend you to contact **Cisco Technical Assistance Center (TAC)** for the following:

- Change telemetry settings.
- Any other specific questions or requests related to telemetry.

# Configure vManage Properties

Cisco DNA Center supports Cisco's vEdge deployment by using integrated vManage setups. You can save the vManage details from the Settings page before provisioning any vEdge topologies.

---

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > External Services > VManage**.

**Step 2** Configure the vManage Properties:

- **Host Name/IP Address:** IP address of vManage.
- **Username:** Name that is used to log in to vManage.
- **Password:** Password that is used to log in to vManage.
- **Port Number:** Port that is used to log in to vManage.
- **vBond Host Name/IP Address:** IP address of vBond. Required if you are using vManage to manage NFV.
- **Organization Name:** Name of the organization. Required if you are using vManage to manage NFV.

**Step 3** To upload the vManage certificate, click **Select a file from your computer**.


**Step 4** Click **Save**.

---

## Account Lockout

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

---

**Step 1** In the Cisco DNA Center GUI, 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 over **Info** to view details for each parameter.


**Step 4** Click **Save** to set the account lockout settings.

---

# Password Expiry

You can configure the password expiration policy to manage the password expiration frequency, the number of days that users are notified before their password expires, and the grace period.

---

**Step 1** In the Cisco DNA Center GUI, 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 over **Info** to view details for each parameter.

**Step 4** Click **Save** to set the password expiry settings.

---





## CHAPTER 4

# Manage Applications

- [Application Management](#), on page 67
- [Download and Update System Updates](#), on page 67
- [Download and Install Packages and Updates](#), on page 68
- [Uninstall a Package](#), on page 69

## Application Management

Cisco DNA 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 Updates** window will vary, depending on your Cisco DNA Center version and your Cisco DNA 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 Cisco DNA Center deployment. For a description of a package and whether it is required, hover over that package's name in the **Updates** tab.

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



### Important


Perform all application management procedures from the Cisco DNA Center GUI. Although you can perform many of these procedures using the CLI (after logging in to the shell), we do not recommend this. In particular, if you use the CLI to deploy or upgrade packages, you must ensure that no **deploy** or **upgrade** command is entered unless the results of the **maglev package status** command show all the packages as NOT\_DEPLOYED, DEPLOYED, or DEPLOYMENT\_ERROR. Any other state indicates that the corresponding activity is in progress, and parallel deployments or upgrades are not supported.

## Download and Update System Updates

You can perform application management procedures from the **Software Updates** window, including downloading and installing system updates.

**Before you begin**

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Software Updates**. Alternately, click the cloud icon and click the **Go to Software Updates** link.

**Step 2** In the **Software Updates** window, review the following tabs:

- **Updates:** Shows the system and the application updates. **System Update** shows the system version that is installed and the system updates that are available and have been downloaded from the Cisco cloud. **Application Updates** shows the available applications that can be downloaded and installed from the Cisco cloud, the size of the application, and the appropriate action (Download, Install, or Update). Hover over the package to view the available version and a basic description.
- **Installed Apps:** Shows the application packages that are currently installed.

**Important** After you launch the **Software Updates** window, a connectivity check is performed and the status is displayed. If there is a connectivity issue, the **Software Updates** window does not show the new updates.

**Step 3** If a system update appears in the **Software Update** window, click **Update** to update Cisco DNA Center.

During the update process, the system reboots. The Cisco DNA Center GUI is unavailable while the system reboots.


## Download and Install Packages and Updates

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

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

**Before you begin**

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Software Updates**. Alternately, click the cloud icon and click the **Go to Software Updates** link.

**Step 2** In the **Software Updates** window, review the following tabs:

- **Updates:** Shows the system and the application updates. **System Update** shows the system version that is installed and the system updates that are available and have been downloaded from the Cisco cloud. **Application Updates** shows the available applications that can be downloaded and installed from the Cisco cloud, the size of the application, and the appropriate action (Download, Install, or Update). Hover over the package to view the available version and a basic description.
- **Installed Apps:** Shows the application packages that are currently installed.

**Important** After you launch the **Software Updates** window, a connectivity check is performed and the status is displayed. If there is a connectivity issue, the **Software Updates** window does not show the new updates.

- Step 3** Download the applications by doing one of the following:
- To download all applications at once, click **Download All** at the top of the **Application Updates** field.
  - To download a specific application group, click **Download All** next to that group.

- Step 4** Update the applications by doing one of the following:
- To update all applications at once, click **Update All** at the top of the **Application Updates** field.
  - To update a specific application group, click **Update All** next to that group.

- Step 5** Ensure that each application has been updated by reviewing its version on the **Installed Apps** tab.

The application versions should be updated on this tab.

**Note** There may be some new application packages that were not part of your previous Cisco DNA Center configuration, and for this reason have not been installed by this procedure (for example, the Test Support package listed on this page).

---

## Uninstall a Package

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

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

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Software Updates**. Alternately, click the cloud icon and click the **Go to Software Updates** link.
- Step 2** Click the **Installed Apps** tab to view the installed applications.
- Step 3** Click **Uninstall** for the package that you want to remove.
- You cannot uninstall multiple packages simultaneously.
- After the package is uninstalled, it is removed from the **Installed Apps** tab.
-





## CHAPTER 5

# Manage Users

---

- [About User Profiles, on page 71](#)
- [About User Roles, on page 71](#)
- [Create a Local User, on page 72](#)
- [Edit a Local User, on page 72](#)
- [Delete a Local User, on page 73](#)
- [Reset a Local User Password, on page 73](#)
- [Change Your Own User Password, on page 74](#)
- [Reset a Forgotten Password, on page 74](#)
- [Configure Role-Based Access Control, on page 74](#)
- [Display Role-Based Access Control Statistics, on page 79](#)
- [Two-Factor Authentication, on page 79](#)
- [Display External Users, on page 85](#)

## About User Profiles

A user profile defines a user's login, password, and role (permissions).

You can configure both internal and external profiles for users. Internal user profiles reside in Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA Center functions. Users with an observer role cannot access any functions that configure or control Cisco DNA Center or the devices it manages.

## Create a Local User

You can create a user and assign this user one of the following roles: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE, or OBSERVER-ROLE.

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

- 
- |               |                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the Cisco DNA Center GUI, click the <b>Menu</b> icon (≡) and choose <b>System &gt; Users &amp; Roles &gt; User Management</b> .          |
| <b>Step 2</b> | Click <b>Add</b> .                                                                                                                          |
| <b>Step 3</b> | Enter a first name, last name, and username for the new user.                                                                               |
| <b>Step 4</b> | Under <b>Role List</b> , choose one of the following roles: <b>SUPER-ADMIN-ROLE</b> , <b>NETWORK-ADMIN-ROLE</b> , or <b>OBSERVER-ROLE</b> . |
| <b>Step 5</b> | Enter a password for the role and confirm it.                                                                                               |
| <b>Step 6</b> | Click <b>Save</b> .                                                                                                                         |
- 

## Edit a Local User

You can change a user role (but not the username).

### Before you begin


Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

- 
- |               |                                                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the Cisco DNA Center GUI, click the <b>Menu</b> icon (≡) and choose <b>System &gt; Users &amp; Roles &gt; User Management</b> . |
| <b>Step 2</b> | Click the radio button next to the user that you want to edit.                                                                     |
| <b>Step 3</b> | Click <b>Edit</b> .                                                                                                                |
| <b>Step 4</b> | Under <b>Role List</b> , choose a new role: <b>SUPER-ADMIN-ROLE</b> , <b>NETWORK-ADMIN-ROLE</b> , or <b>OBSERVER-ROLE</b> .        |
| <b>Step 5</b> | Click <b>Save</b> .                                                                                                                |
-

# Delete a Local User

## Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

- 
- Step 1** In the Cisco DNA Center GUI, 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 Local User Password

You can reset another user's password.


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

## Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).

- 
- Step 1** In the Cisco DNA Center GUI, 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** Click **Reset Password**.
- Step 4** Enter a new password and confirm it. The new password must:
- Contain at least eight characters.
  - Contain 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

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Users & Roles > Change Password**.
- Step 2** Enter information in the required fields.
- Step 3** Click **Update**.
- 

## Reset a Forgotten Password

If you forgot your password, you can reset it through the CLI.

- 
- Step 1** Enter the following command to check if the user is created in the system.
- ```
magctl user display <username>
```
- The command returns the tenant-name, which can be used to reset the password. The output looks similar to the following:
- ```
User admin present in tenant TNT0 (where TNT0 is the tenant-name)
```
- Step 2** Enter the tenant-name in the following command to reset the password.
- ```
magctl user password update <username> <tenant-name>
```
- You are prompted to enter a new password.
- Step 3** Enter a new password.
- You are prompted to re-enter the new password to confirm.
- Step 4** Enter the new password. The password is reset and you can log in to Cisco DNA Center using the new password.
- 

## Configure Role-Based Access Control

Cisco DNA 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 Cisco DNA Center functions.



Use this procedure to define a custom role and then assign a user to that role. Permissions are explained in the table that follows this procedure.

### Before you begin

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

- 
- Step 1** Define a custom role.




- a) In the Cisco DNA Center GUI, 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) Click **Let's Do it**.  
If you want to skip this screen in the future, check the **Don't show this to me again** check box.  
The **Create a New Role** window appears.
- d) Enter a name for the role and then click **Next**.  
The **Define the Access** window appears with a list of options. By default, the observer role is set for all Cisco DNA 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 appears.
- h) Review the summary. If the information is correct, click **Create Role**. Otherwise, click **Edit** and make the appropriate changes.  
The **Done, Role-Name** window appears.

**Step 2**

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

The **User Management > Internal Users** window appears, 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 appears.
  - b. From the **Role List** 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 appears.
  - b. Enter the first name, last name, and username in the fields provided.
  - c. From the **Role List** 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 making changes to your access permissions, you must log out of Cisco DNA Center and then log back in for the new permission settings to take effect.

**Table 4: Cisco DNA Center User Permissions**

Capability	Description
<b>Assurance</b>	Assure consistent service levels with complete visibility across all aspects of your network.
Monitoring and Troubleshooting	<p>Monitor and manage the health of your network with issue troubleshooting and remediation, proactive network monitoring, and insights driven by AI Network Analytics.</p> <p>This role lets you:</p> <ul style="list-style-type: none"> <li>• Resolve, close, and ignore issues.</li> <li>• Run Machine Reasoning Engine (MRE) workflows.</li> <li>• Analyze trends and insights.</li> <li>• Troubleshoot issues, including path trace, sensor dashboards, and rogue management.</li> </ul>
Monitoring Settings	<p>Configure and manage issues. Update network, client, and application health thresholds.</p> <p>Note: You must have at least Read permissions on Monitoring and Troubleshooting.</p>
Troubleshooting Tools	<p>Create and manage sensor tests. Schedule on-demand forensic packet captures (Intelligent Capture) for troubleshooting clients.</p> <p>Note: You must have at least Read permissions on Monitoring and Troubleshooting.</p>
<b>Network Design</b>	Set up 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, trustpool, cloud access keys, Stealthwatch, Umbrella, and data anonymization.
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.
Network Profiles	<p>Create network profiles for routing, enterprise NFV, switching, and wireless, and assign profiles to sites. This role includes Template Editor, Tagging, Model Config Editor, and Authentication Template.</p> <p>Note: To create SSIDs, you must have Write permissions on Network Settings.</p>
Network Settings	<p>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.</p> <p>Note: To create wireless profiles, you must have Write permissions on Network Profiles.</p>

Capability	Description
Virtual Network (VN)	Manage virtual networks (VNs). Segment physical networks into multiple logical networks for traffic isolation and controlled inter-VN communication.
<b>Network Provision</b>	Configure, upgrade, provision, schedule, and manage your network devices.
Image Update	Upgrade a software image on devices that does not 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 permissions on <b>Network Provision &gt; PnP</b> .
License	Unified view of your software and network assets relative to license usage and compliance.
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, and Umbrella provisioning.  Note: To provision devices that are in sites with network profiles attached, you must have at least Read permissions on Network Profiles.
Scheduler	Integrated with other back-end services, scheduler lets you schedule tasks such as deploy policies, provision network devices, or upgrade.
<b>Network Services</b>	Provision services in your network.
App Hosting	Deploy, manage, and monitor virtualized and container-based applications running on network devices.
Bonjour	Enable 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 permissions on the following components: <ul style="list-style-type: none"> <li>• <b>Network Design &gt; Network Settings</b></li> <li>• <b>Network Provision &gt; Provision</b></li> <li>• <b>Network Provision &gt; Scheduler</b></li> <li>• <b>Network Services &gt; Stealthwatch</b></li> </ul>


Capability	Description
Umbrella	<p>Configure network elements to use Cisco Umbrella as the first line of defense against cybersecurity threats.</p> <p>To provision Umbrella, you must have Write permissions on the following components:</p> <ul style="list-style-type: none"> <li>• <b>Network Design &gt; Network Settings</b></li> <li>• <b>Network Provision &gt; Provision</b></li> <li>• <b>Network Provision &gt; Scheduler</b></li> <li>• <b>Network Services &gt; Stealthwatch</b></li> </ul> <p>You must also have Read permissions on Advanced Network Settings.</p>
Platform	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
APIs	Drive value by accessing Cisco DNA Center through REST APIs.
Bundles	Enhance productivity by configuring and activating preconfigured bundles for ITSM integration.
Events	<p>Subscribe to get notified in near real time about network and system events of interest and initiate corrective actions.</p> <p>You can configure Email and Syslog logs in <b>System Settings &gt; Destinations</b>.</p>
Reports	<p>Generate reports using predefined reporting templates for all aspects of your network.</p> <p>You can configure webhooks in <b>System Settings &gt; Destinations</b>.</p>
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 tag. 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 your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.
Basic	Personalize user settings based on preferences. (Set the default to Write for all defined custom roles.)
Machine Reasoning	Configure automatic updates to the machine reasoning knowledge base to rapidly identify security vulnerabilities and improve automated issue analysis.

Capability	Description
System Management	Manage core system functionality and connectivity settings. This role includes Cisco Credentials, Integrity Verification, Device EULA, HA, Integration Settings, Disaster Recovery, Debugging Logs, Telemetry Collection, System EULA, IPAM, vManage Servers, Backup & Restore, and Data Platform. Manage user roles and configure external authentication.
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 Cisco DNA Center.
Network Reasoner	Initiate logical and automated troubleshooting for network issues while drawing on the knowledge wealth of network domain experts.
Search	Search for various objects in Cisco DNA 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** In the Cisco DNA Center GUI, 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.

---

## 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 Cisco DNA 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.

The topics in this section describe:

- The requirements that need to be in place in order to implement two-factor authentication.

- The necessary configuration settings you need to make.
- The Cisco DNA Center login procedure using two-factor authentication.

## Prerequisites for Two-Factor Authentication

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

- An authentication server that is able to return attribute-value pairs to convey RBAC role authorizations for authenticated Cisco DNA 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 Cisco DNA 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 Cisco DNA Center login page, they enter their username and token code.
3. Cisco DNA 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 that the user has been authenticated successfully.
6. Cisco ISE matches the authenticated user with their configured authorization profile and returns the **role=NETWORK-ADMIN-ROLE** attribute-value pair.
7. Cisco DNA 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 Cisco DNA Center appliance, complete the following procedure.

### Step 1 Integrate RSA Authentication Manager with Cisco ISE:

- a) In RSA Authentication Manager, create two users: **cdnac\_admin** (for the Admin user role) and **cdnac\_observer** (for the Observer role).

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

1. Open the [RSA Self-Service Console Help](#).
2. In the **Search help** field, enter **Add a User to the Internal Database** and then click **Search help**.
- b) Create a new authentication agent.  
For more information, see the "Add an Authentication Agent" topic in the [RSA Self-Service Console Help](#).
- c) Generate the Authentication Manager agent configuration file (sdconf.rec):
  1. From the RSA Security Console, choose **Access > Authentication Agents > Generate Configuration File**.  
The **Configure Agent Timeout and Retries** tab opens.
  2. For the **Maximum Retries** and **Maximum Time Between Each Retry** fields, use the default values.
  3. Click **Generate Configuration File**.  
The **Download Configuration File** tab opens.
  4. Click the **Download Now** link.
  5. When prompted, click **Save to Disk** to save a local copy of the zip file.
  6. Unzip the file and use this version of the sdconf.rec file to overwrite the version that is currently installed on the agent.
- d) Generate a PIN for the **cdnac\_admin** and **cdnac\_observer** users 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** field: Enter the profile's name.
  - **Access Type** field: 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 Cisco DNA Center appliance.

In the [Cisco Identity Services Engine Administrator Guide, Release 2.3](#), 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, Release 2.3](#), 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 Cisco DNA Center.  
In the [Cisco DNA Center Installation Guide](#), see the "Integrate Cisco ISE with Cisco DNA Center" topic.
- Step 2** Configure Cisco DNA 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 Cisco DNA 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 and ensure that a shared secret has already been configured for the Cisco DNA Center device 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 cdnac\_admin and cdnac\_observer user roles:
- Click **Add**.
  - Complete the following tasks:
    - Enter the profile's name.
    - After clicking the **Raw View** tab, enter the following text into the **Profile Attributes** text box:
      - For the cdnac\_admin user role, enter **Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE**
      - For the cdnac\_observer user role, enter **Cisco-AVPair=ROLE=OBSERVER-ROLE**
  - Click **Save**.



**Step 5** Integrate Cisco ISE with Cisco DNA Center.

In the [Cisco DNA Center Installation Guide](#), see the "Integrate Cisco ISE with Cisco DNA Center" topic.

**Step 6** Configure Cisco DNA 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 Cisco DNA Center.

---

## Configure External Authentication

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

### Before you begin

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).
- You must configure at least one authentication server.

---

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Users & Roles > External Authentication**.


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

**Step 3** (Optional) Configure the AAA attribute.

For most cases, the default AAA attribute setting (Cisco-AVPair) is sufficient, as long as you have set the Cisco DNA Center user profile on the AAA server with **Cisco-AVPair** as the AAA attribute. You only have to change the default setting in Cisco DNA Center if you have a different value set in the Cisco DNA Center user profile on the AAA server. For example, you might manually define the AAA attribute as **Cisco-AVPair=Role=SUPER-ADMIN-ROLE**.

- a) In the **AAA Attribute** field, leave the default value of **Cisco-AVPair** or enter the new AAA attribute value.
- 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. To view the AAA servers that are available to In the Cisco DNA Center GUI, 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 5: Cisco ISE Server Settings

Name	Description
Shared Secret	Key for device authentications. The shared secret can be up to 128 characters in length.
Username	Name that is used to log in to the Cisco ISE CLI.
Password	Password for the Cisco ISE CLI username.
FQDN	Fully qualified domain name (FQDN) of the Cisco ISE server. The FQDN consists of two parts, a hostname and the domain name, in the following format:  <i>hostname.domainname.com</i>  For example, the FQDN for a Cisco ISE server might be ise.cisco.com.
Subscriber Name	A unique text string—for example, <i>acme</i> —that is used during Cisco DNA Center-to-Cisco ISE integration to set up a new pxGrid client in Cisco ISE.
SSH Key	Diffie-Hellman-Group14-SHA1 SSH key used to connect and authenticate with 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 6: AAA Server Advanced Settings

Name	Description
Protocol	TACACS or RADIUS.
Authentication Port	Port used to relay authentication messages to the AAA server. <ul style="list-style-type: none"> <li>For RADIUS, the default is UDP port 1812.</li> <li>For TACACS, the port is 49 and cannot be changed.</li> </ul>
Accounting Port	Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. <ul style="list-style-type: none"> <li>For RADIUS, the default UDP port is 1813.</li> <li>For TACACS, the port is 49 and cannot be changed.</li> </ul>
Retries	Number of times that Cisco DNA Center can attempt to connect with Cisco ISE.
Timeout	Length of time that Cisco DNA Center waits for Cisco ISE to respond. The maximum timeout value is 60 seconds.

- e) Click **Update**.


## Log In Using Two-Factor Authentication

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

- 
- Step 1** From the Cisco DNA 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 in to the Cisco DNA Center login page's **Password** field.
  - Step 4** Click **Log In**.
- 

## Display External Users

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

- 
- Step 1** In the Cisco DNA Center GUI, 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 6

# Manage Licenses

This chapter contains the following topics:

- [License Manager Overview, on page 87](#)
- [Integration with Cisco Smart Accounts, on page 90](#)
- [Set Up License Manager, on page 90](#)
- [Visualize License Usage and Expiration, on page 91](#)
- [View License Details, on page 92](#)
- [Change License Level, on page 93](#)
- [Export License Information, on page 94](#)
- [Auto Registration of Smart License-Enabled Devices, on page 94](#)
- [Day 0 Configuration for Smart License-Enabled Devices, on page 94](#)
- [Apply Specific License Reservation or Permanent License Reservation to Devices, on page 95](#)
- [Cancel SLR or PLR Applied to Devices, on page 97](#)

## License Manager Overview

The Cisco DNA Center License Manager feature helps you visualize and manage all of your Cisco product licenses, including Smart Account licenses. In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools > License Manager**. The **License Manager** page contains tabs with the following information:

- **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 access points.
- **ISE:** Shows purchased and in-use license information for devices managed by Cisco Identity Services Engine (ISE).
- **All License:** Shows comprehensive details for all types of licenses for all Cisco devices.


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 that not all controls are shown in all tabs.

Table 7: License Management Controls

Control	Description
<b>Filter</b>	Click <b>Filter</b> to specify one or more filter values and then click <b>Apply</b> . You can apply multiple filters. To remove a filter, click the <b>x</b> icon next to the corresponding filter value.
<b>Change Cisco DNA License</b>	Select one or more licenses and click <b>Actions &gt; Change Cisco DNA License</b> to change the level of a selected Cisco DNA Center license to Essential or Advantage. You can also use this control to remove a Cisco DNA Center license. For more information, see <a href="#">Change License Level, on page 93</a> .
<b>Change Virtual Account</b>	Select one or more licenses and click <b>Actions &gt; Change Virtual Account</b> to specify the Virtual Account used to manage these licenses.
<b>Manage Smart License &gt; Register</b>	Select one or more Smart License-enabled devices and click <b>Actions &gt; Manage Smart License &gt; Register</b> to register the Smart License-enabled devices.  Cisco DNA Center does not support Smart Account licenses for Cisco SD-Access.
<b>Manage Smart License &gt; Deregister</b>	Select one or more Smart License-enabled devices and click <b>Actions &gt; Manage Smart License &gt; Deregister</b> to unregister the Smart License-enabled devices.
<b>Manage License Reservation &gt; Enable License Reservation</b>	Choose the device for which you want to apply Specific License Reservation (SLR) or Permanent License Reservation (PLR), and click <b>Actions &gt; Manage License Reservation &gt; Enable License Reservation</b> .
<b>Manage License Reservation &gt; Update License Reservation</b>	The device must be in SLR registered state.  You can update the SLR applied to a wireless device or switches with a wireless controller package.  Choose the device for which you want to update Specific License Reservation (SLR) then click <b>Actions &gt; Manage License Reservation &gt; Update License Reservation</b>
<b>Manage License Reservation &gt; Cancel/Return License Reservation</b>	Choose the device and click <b>Actions &gt; Manage License Reservation &gt; Cancel/Return License Reservation</b> to cancel or return the SLR or PLR applied to the device.
<b>Manage License Reservation &gt; Factory License Reservation</b>	Choose the device and click <b>Actions &gt; Manage License Reservation &gt; Factory License Reservation</b> to enable the factory-installed SLR on the device.
<b>Recent Tasks</b>	Click <b>Recent Tasks</b> to see a list of all 50 of the most recently performed Cisco DNA Center tasks. Use the drop-down at the top of the list to narrow the list to show only those tasks that ended in <b>Success</b> or <b>Failure</b> , or those that are still <b>In Progress</b> .
<b>Refresh</b>	Click this control to refresh the window.
<b>Export</b>	Click to export the list of displayed licenses as a CSV file. For more information, see <a href="#">Export License Information, on page 94</a> .
<b>Find</b>	Enter a search term in the <b>Find</b> 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.
<b>Show entries</b>	Select the total number of entries to show 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. Additionally, some of the columns are hidden in the default column view setting, which can be customized by clicking the More icon (  ) at the right end of the column headings.

**Table 8: License Usage Information**

Column	Description
Device Type: Device Series	Name of the device product series (for example, Catalyst 3850 Series Ethernet Stackable Switch). Click this link to view the license details window. For more information, see <a href="#">View License Details, on page 92</a> .
Device Type: Total Devices	The total number of devices in this product series that are under active management by Cisco DNA Center.
Purchased Licenses	The total number of purchased Cisco DNA 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 Cisco DNA 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 like security, AVC, and so on.

**Table 9: All License Information**

Column	Description
Device Name	Name of the device. Click this link to view the license details window. For more information, see <a href="#">View License Details, on page 92</a> .
Device Family	The category of device as defined by Cisco DNA Center (for example, Switches and Hubs).
IP Address	IP address of the device.
Device Series	The full name of the Cisco product series to which the listed device belongs (for example, Cisco Catalyst 3850 Series Ethernet Stackable Switch).
Cisco DNA License	The Cisco DNA Center license level.
Cisco DNA License Expiry	The date the Cisco DNA Center license expires.
License Mode	The Cisco DNA Center license mode.

Column	Description
Network License	The type of network license.
Virtual Account	The name of the Cisco Virtual Account managing the license for this device.
Site	The Cisco DNA 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	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 Cisco DNA Center subscription license is in effect.
Days to Expiry	The number of days remaining until the Cisco DNA Center license term expires.
Software Version	The version of the network operating system currently running on the device.

## Integration with Cisco Smart Accounts

Cisco DNA 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.

If you already have a Cisco Smart Account, you can use Cisco DNA 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
- Retire unused licenses

You can accomplish this automatically, without leaving Cisco DNA Center.

For more on the service itself, see [Cisco Smart Accounts](#) on cisco.com. For more on setting up your Cisco Smart Account for use with Cisco DNA Center, see [Set Up License Manager, on page 90](#).


## Set Up License Manager

You must set up access to your Cisco Smart Account before you can use the Cisco DNA 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 one or more Smart Accounts: Select the Smart Account that you want to use with Cisco DNA Center, and collect that account's user ID and password.
- To enable a Smart Account, Cisco DNA Center must have reachability to tools.cisco.com.
- To apply licenses to a device in Cisco DNA 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 DNA Center Installation Guide](#) are allowed on any firewall or proxy.


- 
- Step 1** Log in using a Cisco DNA Center system administrator username and password.
- Step 2** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > Cisco Accounts > Cisco.com Credentials**.
- Step 3** Under **Cisco.com Credentials**, enter the username and password for your Smart Account.
- Step 4** 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 5** Click **View all virtual accounts** to view all virtual Smart License Accounts.
- Step 6** Click **Apply**.
- 

### What to do next

Register the Cisco DNA 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 Cisco DNA Center Plug and Play. For more information, see "Register or Edit a Virtual Account" in the [Cisco DNA Center User Guide](#).

## Visualize License Usage and Expiration

Cisco DNA 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** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Tools > License Manager**.
- Step 2** Select the type of device category whose license usage you want to see: **Switches**, **Routers**, **Wireless**, **ISE**, or **All Licenses**.

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

Under the graphs, the **License Usage** table gives 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 given in the **Device Series** column in the table.

Cisco DNA Center displays a window giving details for the product family you selected.

**Step 4** To see a graphical representation of license duration, scroll down to the **License Timeline** section of the window. 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 License Details


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

The simplest method for getting the most comprehensive license details for a single device is to use the License Manager's **All Licenses** table, as explained in the following steps.


**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools > License Manager > All Licenses**.

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 may 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 belonging to a particular site, navigate to the site in the left pane, and click the site. The devices will be 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 matching your entry in the **Find** field.
- **Customize:** Click  and select the columns you want displayed in the table. For example: Deselect **Device Model** or select **Days to Expiry**. When you click **Apply**, the table displays only the columns you selected.

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

Cisco DNA Center displays a slider panel **License Details** window giving complete license details and license history for the device you selected. The **Actions** displays actions that can be performed on the device or its licenses.

When you are finished, click  to close the **License Details** window.



---

## Change License Level

You can upgrade or downgrade the feature level of your device licenses. You can do this with Cisco DNA 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 Cisco DNA Center license level is changed.)

Whenever you change a device's license level, Cisco DNA 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 as soon as the license level change is complete. You can choose not to reboot with the license change, but you will need to schedule the reboot at a later time, or your license level change will not be applied.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Tools > License Manager > All Licenses**. 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 92](#) 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 Cisco DNA License**. Cisco DNA Center displays a **Change License Level** window appropriate for the license type you want to change.
- Step 4** Click the license level you want for these devices: **Essentials** or **Advantage**. To remove the license from the device, click **Remove**.
- Step 5** Click **Next**. Cisco DNA Center asks if you want the change to be applied right away or at a later time. You also must choose whether you want to reboot the device as soon as 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 as soon as 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**.

---

## Export License Information

You can quickly export license information from Cisco DNA Center to backup PDF or Microsoft Excel files. These license backup files are intended to assist your organization's accounting and reporting needs.


---

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Tools > License Manager**.
  - Step 2** Click **All Licenses**. Cisco DNA Center displays a list of all your currently assigned licenses.
  - Step 3** Click **Export**. Cisco DNA Center displays the Export Licenses window.
  - Step 4** Choose the destination file format.
  - Step 5** (Optional) Check the check box next to each type of license information that you want to exclude or include in the export. Check the check box at the bottom to save your choices as the default for later exports.
  - Step 6** Click **Export** and specify the location and file name for the exported license file.
  - Step 7** Click **OK** to complete the export.
- 

## 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 Cisco DNA Center are automatically registered to the chosen virtual account.

---

- Step 1** Log in using a Cisco DNA Center system administrator username and password.
  - Step 2** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > Cisco Accounts > Cisco.com Credentials**.
  - 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 Cisco DNA Center before enabling auto registration are not automatically registered. You can view the Smart License-enabled devices that are not registered in the **All License** page.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Tools > License Manager > All License**.
- The **License Manager** window displays a banner message with the number of SL-enabled devices that are not auto registered and a table listing all of your discovered devices and their licenses with a link to set up auto registration.
- Alternatively, you can filter the unregistered devices by using the **Registration Status** column.
- Step 2** Choose the SL-enabled devices that you want to register and choose **Actions > Manage Smart License > Register**.
- Step 3** Choose the virtual account and click **Continue**.
- Step 4** To register the devices:
- If you want to register the devices immediately, choose **Now** and click **Confirm**.
  - If you want to register the devices later, choose **Later** and specify a date and time. When you are finished 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 Cisco DNA Center customers to reserve licenses securely from CSSM using an API-based workflow. In Cisco DNA 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](mailto:licensing@cisco.com) for support.

To enable SLR or PLR when both the device and Cisco DNA Center are connected to CSSM, see [Enable SLR/PLR when the Device and Cisco DNA Center Are Connected to CSSM, on page 96](#).

To enable SLR or PLR when the device and Cisco DNA Center do not have connectivity to CSSM, see [Enable SLR/PLR Using CSV when the Devices and Cisco DNA Center Are Not Connected to CSSM, on page 96](#).

## Enable SLR/PLR when the Device and Cisco DNA Center Are Connected to CSSM

### Before you begin

Ensure that both the device for which you want to generate SLR/PLR and Cisco DNA Center are connected to CSSM.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools > Licenses > All Licenses**.
- 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 at a later time, 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** page.
- 

## Enable SLR/PLR Using CSV when the Devices and Cisco DNA Center Are Not Connected to CSSM

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

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools > Licenses > All Licenses**.
- 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** Get 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/PLR are applied to the selected devices.
- You can now view the updated status of the devices under **Reservation Status** on the **All Licenses** page.
- 

## 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** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Tools > Licenses > All 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** page.
-







## CHAPTER 7

# Backup and Restore

---

- [About Backup and Restore, on page 99](#)
- [Backup Server Requirements, on page 100](#)
- [Example of NFS Server Configuration, on page 101](#)
- [Configure Backup Servers, on page 102](#)
- [Back Up Data Now, on page 103](#)
- [Schedule Data Backups, on page 104](#)
- [Restore Data from Backups, on page 105](#)

## About Backup and Restore

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

### Backup

You can back up Automation data only or both Automation and Assurance data.

The Automation data consists of Cisco DNA Center databases, credentials, file systems, and files. The Automation backup is a full backup.

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



---

#### Important

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

---

Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see [Backup Server Requirements, on page 100](#).

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

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

We recommend the following:

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

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

### Restore

You can restore the backup files from the remote server using Cisco DNA Center.

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

You cannot take a backup from one version of Cisco DNA Center and restore it to another version of Cisco DNA Center. You only can restore a backup to an appliance that is running the same Cisco DNA Center software version, applications, and application versions as the appliance and applications from which the backup was taken. To view the current applications and versions on Cisco DNA Center, choose **System > Software Updates**.

You can restore a backup to a Cisco DNA Center appliance with a different IP address. This situation could happen if the IP address is changed on Cisco DNA Center and you need to restore from an older system.

## Backup Server Requirements

The backup server should run one of the following operating systems:

- RedHat Enterprise (or Centos) 7 or greater
- Ubuntu 16.04 (or Mint, etc) or greater

### Server Requirements for Automation Data Backup

To support Automation data backups, the server must meet the following requirements:

- Must use SSH (port22)/Rsync. Cisco DNA Center does not support using FTP (port 21) when performing a backup.
- Linux rsync utility must be installed.
- The backup user should own the destination folder for the backup or should have read-write permissions for the user's group. For example, assuming the backup user is 'backup' and the user's group is 'staff,' the following sample outputs show the required permissions for the backup directory:
  - Example 1: Backup directory is owned by 'backup' user:

```
$ ls -l /srv/
drwxr-xr-x 4 backup root 4096 Apr 10 15:57 acme
```

- Example 2: 'backup' user's group has required permissions:

```
$ ls -l /srv/
drwxrwxr-x. 7 root staff 4096 Jul 24 2017 acme
```

- SFTP subsystem must be enabled. The following line must be uncommented and present in the SSHD configuration:

```
Subsystem sftp /usr/libexec/openssh/sftp-server
```

The file where you need to uncomment the preceding line is usually located in `/etc/ssh/sshd_config`.

### Server Requirements for Assurance Backup

To support Assurance data backups, the server must meet 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 Cisco DNA Center and the NFS server
- Have sufficient network speed between Cisco DNA Center and the NFS server

## Example of NFS Server Configuration

The remote share for backing up an Assurance database (NDP) must be an NFS share. If you need to configure an NFS server, use the following procedure (Ubuntu distribution) as an example.

- 
- Step 1** Run the **sudo apt-get update** command to access and update the advanced packaging tool (APT) for the NFS server. For example, enter a command similar to the following:
- ```
$ sudo apt-get update
```
- Step 2** Run the **sudo apt-get install** command to install the advanced packaging tool for NFS. For example, enter a command similar to the following:
- ```
$ sudo apt-get install -y nfs-kernel-server
```
- Step 3** Run the **sudo mkdir -p** command to create nested directories for the NFS server. For example, enter a command similar to the following:
- ```
$ sudo mkdir -p /var/nfsshare/
```
- Step 4** Run the **sudo chown nobody:nogroup** command to change the ownership of the group to nobody and nogroup. For example, enter a command similar to the following:
- ```
$ sudo chown nobody:nogroup /var/nfsshare
```
- Step 5** Run the **sudo vi /etc/exports** command to add the following line to the end of `/etc/exports`:
- ```
$ sudo vi /etc/exports
/var/nfsshare *(rw,all_squash,sync,no_subtree_check)
```
- Step 6** Run the **sudo exportfs -a** command to export the file systems for the NFS server. For example, enter a command similar to the following:
- ```
$ sudo exportfs -a
```

**Step 7** Run the `sudo systemctl start nfs-server` command to restart the NFS server.

For example, enter a command similar to the following:

```
$ sudo systemctl start nfs-server
```

**Step 8** Enter the following command to set the permission on the NSF directory to 777:

```
chmod 777 -R <your_NFS_directory>
```

---

### What to do next

After you configure an NFS share, back up the Assurance data or schedule a backup for a later time. For information, see [Back Up Data Now, on page 103](#) or [Schedule Data Backups, on page 104](#).

## Configure Backup Servers

If you plan to back up the Automation data only, you need to configure the Cisco DNA Center Core System server. If you plan to back up both the Automation and Assurance data, you need to configure the Cisco DNA Center Core System backup server and the NFS backup server.

This procedure shows you how to set up both servers.

### Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).
- The server that you plan to use for data backups must meet the requirements described in [Backup Server Requirements, on page 100](#).

---

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Backup & Restore > Configure**.

**Step 2** To configure the Core System backup server, do the following:

a) Define the following settings:

Field	Description
SSH IP Address	IP address of the remote server that you can SSH into.
SSH Port	Port address of the remote server that you can SSH into.
Server Path	Path to the folder on the server where the backup files are saved.
Username	Username used to protect the encrypted backup.
Password	Password used to protect the encrypted backup.

Field	Description
Encryption Passphrase	Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials.  This is a required passphrase for which you will be prompted and that must be entered when restoring the backup files. Without this passphrase, backup files are not restored.

b) Click **Apply**.

**Step 3** To configure the NFS backup server, click the **NFS** tab and define the following settings:

Field	Description
Host	IP address or host name of the remote server that you can SSH into.
Server Path	Path to the folder on the server where the backup files are saved.

**Step 4** Click **Apply**.

## Back Up Data Now

You can choose to back up one of the following data sets:

- Automation data only.
- Both Automation and Assurance data.

When you perform a backup, Cisco DNA Center copies and exports the data to the location on the remote server that you configured.



**Note** Data is backed up using SSH/Rsync. Cisco DNA Center does not support using FTP (port 21) when performing a backup.

### Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).
- Backup servers meet the requirements described in [Backup Server Requirements, on page 100](#).
- Backup servers have been configured in Cisco DNA Center. For information, see [Configure Backup Servers, on page 102](#).

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Backup & Restore > Backups**.

**Note** If you have not yet configured a backup server, Cisco DNA Center requires that you configure one before proceeding. Click **Configure your backups** and see [Configure Backup Servers, on page 102](#) for information.

**Step 2** Click **Add**.

The **Create Backup** pane appears.

**Step 3** In the **Backup Name** field, enter a unique name for the backup.

**Step 4** Click **Create now** to perform the backup immediately.

**Step 5** Define the scope of the backup:

- Click **Cisco DNA Center (All data)** to back up the Automation and Assurance data.
- Click **Cisco DNA Center (without Assurance data)** to back up only the Automation data.

**Step 6** Click **Create**.

**Note** You can view the current backup status and the history of previous backups in the **Activity** tab.

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

You can view the successfully completed backup jobs in the **Backup** tab.

During the backup process, Cisco DNA Center creates the backup database and files. The backup files are saved to the specified location on the remote server. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. You receive a **Backup done!** notification when the process is finished.

**Note** If the backup process fails, there is no impact to the appliance or its database. Cisco DNA Center displays an error message stating the cause of the backup failure. 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.

---

## Schedule Data Backups

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 the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).
- Backup servers meet the requirements described in [Backup Server Requirements, on page 100](#).
- Backup servers have been configured in Cisco DNA Center. For information, see [Configure Backup Servers, on page 102](#).

---

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Backup & Restore > Schedule**.

The **Schedule** window appears.

**Step 2** Click **Add**.

The **Create Backup** pane appears.

**Step 3** In the **Backup Name** field, enter a unique name for the backup.

**Step 4** Click **Schedule weekly**.

**Step 5** Choose the days and time for scheduling the backup.

**Step 6** Define the scope of the backup:

- Click **Cisco DNA Center (All data)** to back up the Automation and Assurance data.
- Click **Cisco DNA Center (without Assurance data)** to back up the Automation data only.

**Step 7** Click **Schedule**.

**Note** You can view the scheduled backup jobs in the **Schedule** tab. After the backup starts, you can view backup status in the **Activity** tab.

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

You can view the successfully completed backup jobs in the **Backup** tab.

During the backup process, Cisco DNA Center creates the backup database and files. The backup files are saved to the specified location on the remote server. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. You receive a **Backup done!** notification when the process is finished.

**Note** If the backup process fails, there is no impact to the appliance or its database. Cisco DNA Center displays an error message stating the cause of the backup failure. The most common reason for a failed backup is insufficient disk space. If your backup process fails, make sure that there is sufficient disk space on the remote server and attempt another backup.

---

## Restore Data from Backups

When you restore data from a backup file, Cisco DNA Center removes and replaces the existing database and files with the backup database and files. The data that is restored depends on what is on the backup:

- Automation data backup: Cisco DNA Center restores the full Automation data.
- Automation and Assurance data backup: Cisco DNA Center restores the full Automation data and the Assurance data as far back as the date that you choose.



---

### Caution

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

---



**Note** You cannot do a backup from one version of Cisco DNA Center and restore it to another version of Cisco DNA Center. You can only restore a backup to an appliance that is running the same Cisco DNA Center software version, applications, and application versions as the appliance and applications from which the backup was taken. To view the current apps and versions, choose **System > Software Updates**.

### Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 71](#).
- You have backups from which to restore data.

When you restore data, Cisco DNA Center enters maintenance mode and is unavailable until the restore process is done. Make sure you restore data at a time when Cisco DNA Center can be unavailable.

If you restore from a backup (on either the Cisco ISE or Cisco DNA Center side), Group-Based Access Control policy data does not synchronize automatically. You must run the policy migration operation manually to ensure that Cisco ISE and Cisco DNA Center are synchronized.

---

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System > Backup & Restore**.

The **Backup & Restore** window displays the following tabs: **Backups**, **Schedule**, and **Activity**.

If you already successfully created a backup on a remote server, it appears in the **Backups** tab.

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

**Step 3** In the **Actions** column, choose **Restore**.

The Cisco DNA Center restore process restores the database and files. The restore process does not restore your network state and any changes made since the last backup, including any new network policies that have been created, any new or updated passwords, or any new or updated certificates and trustpool bundles.

During a restore, the backup files remove and replace the current database.

During the restore process, Cisco DNA Center goes into maintenance mode. Wait until Cisco DNA Center exits maintenance mode before proceeding.

**Step 4** Click the **Backups** tab to view the results of a successful restore.

---