



## **Cisco DNA Center Administrator Guide, Release 2.2.1**

**First Published:** 2021-02-08

### **Americas Headquarters**

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

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

© 2021 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

<b>CHAPTER 1</b>	<b>New and Changed Information</b>	<b>1</b>
------------------	------------------------------------	----------

---

<b>CHAPTER 2</b>	<b>Get Started with Cisco DNA Center</b>	<b>3</b>
	About Cisco DNA Center	3
	Log In	3
	Complete the Quick Start Workflow	4
	Default Home Page	8
	Use Global Search	11
	Enable Localization	13
	Where to Start	14

---

<b>CHAPTER 3</b>	<b>Configure System Settings</b>	<b>15</b>
	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 Event Notifications	20
	Event Notification Information	20
	View the System Topology	23
	Troubleshoot Appliance and External System Issues	24
	Troubleshoot External System Connectivity Issues	24
	System Topology Notifications	25
	Suggested Actions	26
	Cisco DNA Center and Cisco ISE Integration	30

Anonymize Data	31
Configure Authentication and Policy Servers	32
Configure Cisco AI Network Analytics Data Collection	34
Disable Cisco AI Network Analytics Data Collection	36
Update the Machine Reasoning Knowledge Base	37
Cisco Accounts	38
Configure Cisco Credentials	38
Clear Cisco Credentials	38
Configure Connection Mode	39
Register Plug and Play	40
Configure Smart Account	40
Smart Licensing	41
Device Controllability	42
Configure Device Controllability	44
Accept the License Agreement	44
Cloud Access Keys	44
Integrity Verification	45
Upload the KGV File	46
Configure an IP Address Manager	47
Configure Debugging Logs	48
Configure the Network Resync Interval	50
View Audit Logs	50
Export Audit Logs to Syslog Servers	51
View Audit Logs in Syslog Server Using APIs	52
Activate High Availability	52
Configure Integration Settings	52
Set Up a Login Message	53
Configure the Proxy	53
Security for Cisco DNA Center	54
Change the Minimum TLS Version and Enable RC4-SHA (Not Secure)	55
Configure the Proxy Certificate	57
Certificate and Private Key Support	58
Certificate Chain Support	59
Update the Cisco DNA Center Server Certificate	59

Use an External SCEP Broker	61
Switch Back to an Internal PKI Certificate	62
Certificate Management	62
Configure the Device Certificate Lifetime	62
Change the Role of the PKI Certificate from Root to Subordinate	63
Provision a Rollover Subordinate CA Certificate	65
Renew Certificates	66
Configure Trustpool	67
Configure the SFTP Server	68
Configure SNMP Properties	68
About Product Usage Telemetry Collection	69
Configure vManage Properties	69
Account Lockout	70
Password Expiry	70

---

**CHAPTER 4**
**Manage Applications 73**

Application Management	73
Download and Update System Updates	73
Download and Install Packages and Updates	74
Uninstall a Package	75

---

**CHAPTER 5**
**Manage Users 77**

About User Profiles	77
About User Roles	77
Create an Internal User	78
Edit a User	78
Delete a User	79
Reset a User Password	79
Change Your Own User Password	80
Reset a Forgotten Password	80
Configure Role-Based Access Control	80
Cisco DNA Center User Role Permissions	82
Display Role-Based Access Control Statistics	85
Configure External Authentication	85

- Two-Factor Authentication **88**
  - Prerequisites for Two-Factor Authentication **88**
  - Two-Factor Authentication Workflow **88**
  - Configure Two-Factor Authentication **89**
    - Enable Two-Factor Authentication Using RADIUS **90**
    - Enable Two-Factor Authentication Using TACACS+ **90**
  - Log In Using Two-Factor Authentication **91**
- Display External Users **91**

---

**CHAPTER 6**

**Manage Licenses 93**

- License Manager Overview **93**
- Integration with Cisco Smart Accounts **96**
- Set Up License Manager **97**
- Visualize License Usage and Expiration **98**
- View License Details **99**
- Change License Level **99**
- Export License Information **100**
- Auto Registration of Smart License-Enabled Devices **101**
- Day 0 Configuration for Smart License-Enabled Devices **101**
- Apply Specific License Reservation or Permanent License Reservation to Devices **102**
  - Enable SLR/PLR When the Devices and Cisco DNA Center Are Connected to CSSM **102**
  - Enable SLR/PLR When the Devices and Cisco DNA Center Are Not Connected to CSSM **103**
  - Generate the Authorization Code from CSSM **103**
- Cancel SLR or PLR Applied to Devices **104**
- Install the Authorization Code and Enable the High Security License **104**
- Upload Resource Utilization Details to CSSM **105**
- Change Device Throughput **105**
- Transfer Licenses Between Virtual Accounts **106**
- Manage Customer Tags to Smart License-Enabled Devices **106**
- Modify License Policy **107**

---

**CHAPTER 7**

**Backup and Restore 109**

- About Backup and Restore **109**
- Backup Server Requirements **110**

Backup Storage Requirements	111
Example of NFS Server Configuration—Ubuntu	112
Example of NFS Server Configuration—CentOS	113
Configure Firewall Rules to Allow NFS	114
Configure Firewall Rules—Debian/Ubuntu	114
Configure Firewall Rules—RedHat/CentOS	114
Configure Backup Servers	115
Back Up Data Now	116
Schedule Data Backups	117
Restore Data from Backups	118

**CHAPTER 8****Implement Disaster Recovery 121**

Overview	121
Key Terms	121
Data Replication Overview	123
Navigate the Disaster Recovery GUI	123
Prerequisites	125
Configure Disaster Recovery After an Upgrade	127
Scenario 1	127
Scenario 2	128
Scenario 3	128
Add the Disaster Recovery Certificate	128
Configure the Witness Site	130
Configure Disaster Recovery	131
Replace the Current Witness Site	135
Deregister Your System	135
Monitor the Event Timeline	136
System and Site States	137
Failovers: An Overview	141
Initiate a Manual Failover	141
Pause Your Disaster Recovery System	144
Place Your System on Pause	144
Rejoin Your System	146
Backup and Restore Considerations	148

Disaster Recovery Event Notifications	148
Supported Events	149
Troubleshoot Your Disaster Recovery System	150
Troubleshoot BGP Route Advertisement Issues	156





# 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 2.2.1**

Feature	Description	Where Documented
Change license level support for Cisco AireOS controllers	You can change the license level of the following Cisco AireOS controllers: <ul style="list-style-type: none"> <li>• Cisco 3500 Series Wireless LAN Controller</li> <li>• Cisco 5500 Series Wireless LAN Controller</li> <li>• Cisco 8500 Series Wireless LAN Controller</li> </ul>	—
Report license usage support for traditional devices such as Cisco Catalyst 2000, Cisco Catalyst 4000, and Cisco Catalyst 6000	The Cisco DNA Center license manager checks the customer smart account and virtual account for the entitlement tags and reports the count-based usage in the <b>All Licenses</b> page.	—
Install authorization code and enable an HSEC license	You can install an authorization code and enable an HSEC license in a single workflow or in separate workflows.	<a href="#">Install the Authorization Code and Enable the High Security License, on page 104</a>
Upload resource utilization details to CSSM	You can upload the resource utilization details to CSSM immediately or schedule the uploading event.	<a href="#">Upload Resource Utilization Details to CSSM, on page 105</a>
Change device throughput	You can change the throughput of smart license-enabled routers.	<a href="#">Change Device Throughput, on page 105</a>
Transfer licenses between virtual accounts	You can transfer licenses between virtual accounts.	<a href="#">Transfer Licenses Between Virtual Accounts, on page 106</a>
Manage customer tags to smart license-enabled devices	You can add a maximum of four customer tags to a smart license-enabled device to help identify telemetry data for a product instance. You can also update and delete the customer tags.	<a href="#">Manage Customer Tags to Smart License-Enabled Devices, on page 106</a>

Feature	Description	Where Documented
Reporting APs in License Manager inventory	While exporting data from the <b>All Licenses</b> page, the number of access points connected to a wireless controller can be exported by checking the <b>Total APs</b> check box under <b>Select Columns to Export</b> in the <b>Export Licenses</b> window.	—
Idle session timeout	If you leave the session idle, a <b>Session Timeout</b> dialog box appears 5 minutes before the session timeout. Click <b>Stay signed in</b> if you want to continue the session. You can click <b>Sign out</b> to end the session immediately.	<a href="#">Account Lockout, on page 70</a>
FQDN support for Cisco Catalyst 9800 controllers	With this release, Cisco DNA Center FQDN supports the image version 17.4 or later for Cisco Catalyst 9800 Series Wireless Controller, ECA, and embedded wireless controller.	—
View Audit Logs	<p>Cisco DNA Center now allows you to add multiple syslog servers to receive audit logs and events from external services.</p> <p>Multiple syslog servers enable you to select multiple destinations for audit log export to syslog servers in case the primary syslog server data is corrupted.</p> <p>With this release, the Cisco DNA Center audit log feature also allows you to filter the multiple audit logs by the description.</p>	<a href="#">View Audit Logs, on page 50</a>
About backup and restore and configure integration settings	After a backup and restore of Cisco DNA Center, you need to access the Integration Settings page and update (if necessary) the <b>Callback URL Host Name</b> or <b>IP Address</b> .	<a href="#">About Backup and Restore, on page 109</a>



**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.



## CHAPTER 2

# Get Started with Cisco DNA Center

---

- [About Cisco DNA Center, on page 3](#)
- [Log In, on page 3](#)
- [Complete the Quick Start Workflow, on page 4](#)
- [Default Home Page, on page 8](#)
- [Use Global Search, on page 11](#)
- [Enable Localization, on page 13](#)
- [Where to Start, on page 14](#)

## 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 SUPER-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.
- Step 3** To log out, click the **Menu** icon (☰) and choose **Sign Out**.
- 

## Complete the Quick Start Workflow

After you have installed and configured the Cisco DNA Center appliance, you can log in to its GUI. Use a compatible, HTTPS-enabled browser when accessing Cisco DNA Center.

When you log in for the first time as the admin superuser (with the username `admin` and the SUPER-ADMIN-ROLE assigned), the Quick Start workflow automatically starts. Complete this workflow to discover the devices that Cisco DNA Center will manage and enable the collection of telemetry from those devices.

### Before you begin

To log in to Cisco DNA Center and complete the Quick Start workflow, you will need:

- The `admin` superuser username and password that you specified while completing one of the following procedures in the [Cisco DNA Center Second-Generation Appliance Installation Guide](#):
    - Configure the Primary Node Using the Maglev Wizard
    - Configure the Primary Node Using the Expert Configuration Wizard (44- or 56-core appliance)
    - Configure the Primary Node Using the Expert Configuration Wizard (112-core appliance)
  - The requisite information, as described in the installation guide's Required First-Time Setup Information topic.
- 

- Step 1** After the Cisco DNA Center appliance reboot is completed, launch your browser.
- Step 2** Enter the host IP address to access the Cisco DNA Center GUI, using **HTTPS://** and the IP address of the Cisco DNA Center GUI that was displayed at the end of the configuration process.
- After entering the IP address, one of the following messages appears (depending on the browser you are using):
- Google Chrome: `Your connection is not private`
  - Mozilla Firefox: `Warning: Potential Security Risk Ahead`
- Step 3** Ignore the message and click **Advanced**.
- One of the following messages appears:
- Google Chrome:
 

```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted by your computer's
```

operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

- **Mozilla Firefox:**

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust *GUI-IP-address* because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

These messages appear because the controller uses a self-signed certificate. For information on how Cisco DNA Center uses certificates, see the "Certificate and Private Key Support" section in the [Cisco DNA Center Administrator Guide](#).

**Step 4** Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to *GUI-IP-address* (unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Cisco DNA Center login screen appears.

**Step 5** Enter the admin's username (admin) and password that you set when you configured Cisco DNA Center, then click **Log In**.

In the resulting screen, you are prompted to specify a new admin password (as a security measure).

**Step 6** Do the following, then click **Next**:

- a) Enter the same admin password you specified in Step 5.
- b) Enter and confirm a new admin password.

**Step 7** In the resulting screen, enter your cisco.com username and password and then click **Next**.

These credentials are used to register software downloads and receive system communications.

The **Terms & Conditions** screen opens, providing links to the software End User License Agreement (EULA) and any supplemental terms that are currently available.

**Step 8** After reviewing these documents, click **Next** to accept the EULA.

The **Quick Start Overview** slider opens. Click > to view a description of the tasks that the Quick Start workflow will help you complete in order to start using Cisco DNA Center.

**Step 9** Complete the Quick Start workflow:

- a) Click **Let's Do it**.
- b) In the **Discover Devices: Provide IP Ranges** screen, enter the following information and then click **Next**:
  - The name for the device discovery job.
  - The IP address ranges of the devices you want to discover. Click + to enter additional ranges.
  - Specify whether you want to designate your appliance's loopback address as its preferred management IP address. For more information, see the "Preferred Management IP Address" topic in the [Cisco DNA Center User Guide](#).
- c) In the **Discover Devices: Provide Credentials** screen, enter the information described in the following table for the type of credentials you want to configure and then click **Next**:

Field	Description
<b>CLI (SSH) Credentials</b>	
Username	Username used to log in to the CLI of the devices in your network.
Password	Password used to log in to the CLI of the devices in your network.
Name/Description	Name or description of the CLI credentials.
Enable Password	Password used to enable a higher privilege level in the CLI. Configure this password only if your network devices require it.
<b>SNMP Credentials: SNMPv2c Read tab</b>	
Name/Description	Name or description of the SNMPv2c read community string.
Community String	Read-only community string password used only to view SNMP information on the device.
<b>SNMP Credentials: SNMPv2c Write tab</b>	
Name/Description	Name or description of the SNMPv2c write community string.
Community String	Write community string used to make changes to the SNMP information on the device.
<b>SNMP Credentials: SNMPv3</b>	
Name/Description	Name or description of the SNMPv3 credentials.
Username	Username associated with the SNMPv3 credentials.
Mode	Security level that SNMP messages require: <ul style="list-style-type: none"> <li>• <b>No Authentication, No Privacy</b> (noAuthnoPriv): Does not provide authentication or encryption.</li> <li>• <b>Authentication, No Privacy</b> (authNoPriv): Provides authentication, but does not provide encryption.</li> <li>• <b>Authentication and Privacy</b> (authPriv): Provides both authentication and encryption.</li> </ul>
Authentication Password	Password required to gain access to information from devices that use SNMPv3. The password must be at least eight characters in length. Note the following points: <ul style="list-style-type: none"> <li>• Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>

Field	Description
Authentication Type	Hash-based Message Authentication Code (HMAC) type used when either <b>Authentication and Privacy</b> or <b>Authentication, No Privacy</b> is set as the authentication mode: <ul style="list-style-type: none"> <li>• <b>SHA</b>: HMAC-SHA authentication.</li> <li>• <b>MD5</b>: HMAC-MD5 authentication.</li> </ul>
Privacy Type	Privacy type used when <b>Authentication and Privacy</b> is set as the authentication mode: <ul style="list-style-type: none"> <li>• <b>DES</b>: 56-bit DES encryption. <p><b>Note</b> DES encryption is being deprecated and will be removed in a future release.</p> </li> <li>• <b>AES128</b>: 128-bit AES encryption.</li> <li>• <b>None</b>: No privacy.</li> </ul>
Privacy Password	Password used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords must be at least eight characters long. Note the following points: <ul style="list-style-type: none"> <li>• Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>
<b>NETCONF</b>	
Port	The NETCONF port that Cisco DNA Center should use in order to discover wireless controllers that run Cisco IOS-XE.

- d) In the **Create Site** screen, group the devices you are going to discover into one site in order to facilitate telemetry and then click **Next**.

You can enter the site's information manually or click the location you want to use in the provided map.

- e) In the **Enable Telemetry** screen, check the network components that you want Cisco DNA Center to collect telemetry for and then click **Next**.

To open a pop-up window that lists the commands Cisco DNA Center will send to enable telemetry on a particular component, click its **View Sample Commands** link.

- f) In the **Summary** screen, review the settings that you have entered and then do one of the following:
- If you want to make changes, click the appropriate **Edit** link to open the relevant screen.

- If you're happy with the settings, click **Start Discovery and Telemetry**. Cisco DNA Center validates your settings to ensure that they will not result in any issues. After validation is complete, the screen updates.  
Cisco DNA Center begins the process of discovering your network's devices and enabling telemetry for the network components you selected. The process will take a minimum of 30 minutes (more for larger networks).

g) Click **Launch Homepage** to open the Cisco DNA Center homepage.

While Cisco DNA Center discovers your network's devices and enables telemetry, you can click the **Explore** link to open a page that provides pointers to product documentation and videos.

A message appears at the top of the homepage to indicate when the Quick Start workflow has completed.

---

## 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.



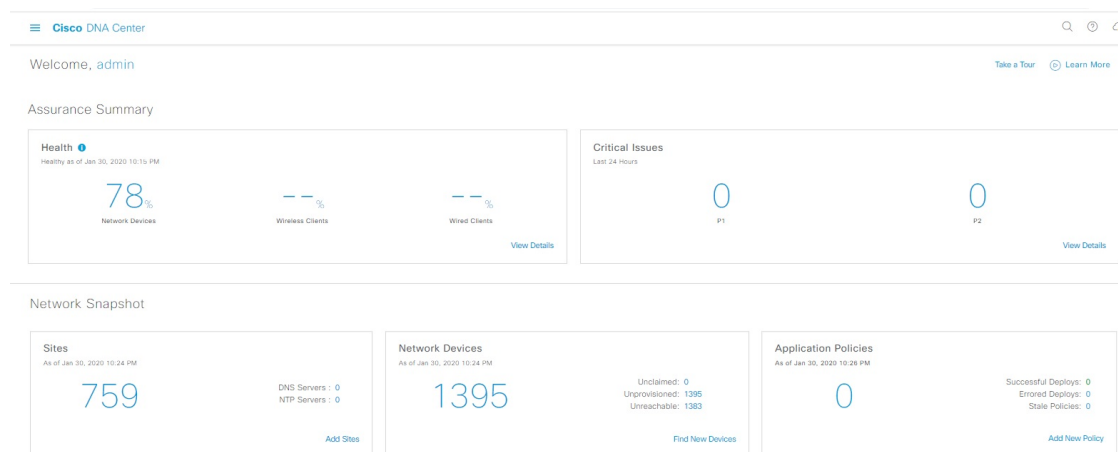
- **Licensed Devices:** Provides the number of devices that have a Cisco DNA Center license along with the number of switches, routers, and access points. Clicking **Manage Licenses** takes you to the **License Management** window.

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 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.

Welcome, admin Get Started Take a Tour Learn More

In order to gather Assurance data and calculate your network health, we'll need to discover or import your network devices.

[Import](#) [Discover](#)

Network Snapshot

+ Add Sites	<b>Network Devices</b> As of December 19, 2018 4:31 PM 0 Unclaimed : 0 Unprovisioned : 0 Unreachable : 0 <a href="#">Find New Devices</a>	<b>Network Profiles</b> As of Dec 19, 2018 4:31 PM 0 <a href="#">Manage Profiles</a>
+ Import Images/SMLUs	<b>DNA Licensed Devices</b> As of Dec 19, 2018 4:31 pm 0 Switches : 0 Routers : 0 Access Points : 0 <a href="#">Manage Licenses</a>	

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






We've discovered 10 devices in your network. [View Discovery](#)

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

Click the **Menu** icon (  $\equiv$ ) 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, and other items, anywhere they are stored in the Cisco DNA Center database.
	<p><b>Help</b></p> <ul style="list-style-type: none"> <li>• <b>About:</b> <ul style="list-style-type: none"> <li>Display the current Cisco DNA Center software version.</li> <li>Click <b>Release Notes</b> to launch the release notes in a separate browser tab.</li> <li>Click <b>Packages</b> to view the system and application package versions.</li> <li>Click <b>Serial number</b> to view the serial number of the Cisco DNA Center appliance.</li> </ul> </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>Notifications:</b> Displays event notifications and sets notification preferences. A red circle by the notification icon indicates that there are new notifications.
	<b>Interactive Help:</b> Opens a menu of interactive help flows that help you complete specific tasks from the GUI.




**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.

Cisco DNA Center allows you search for an IPv6 address. You can enter an entire IPv6 address or its abbreviated form.

For example, you can use the following search terms to search for `2001:0db8:85a3:0000:0000:8a2e:0370:7334`:

- `2001:0db8:85a3:0000:0000:8a2e:0370:7334` (using the full IPv6 address)

- `2001:db8:85a3:0:0:8a2e:0:7334` (truncating leading zeros)
- `2001:db8:85a3::8a2e:0:7334` (compressing consecutive zeros with a double colon)
- `2001:db8:85a3` (using a portion of the IPv6 address)

You can search for devices in Cisco DNA Center by entering their MAC addresses in any format (with a hyphen or colon).

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 center is the Cisco logo, consisting of a stylized signal icon above the word "CISCO". Below the logo, the text "Cisco DNA Center" is displayed in a large, blue, sans-serif font. Underneath that, the Japanese text "ネットワークの設計、自動化、保証" (Network design, automation, guarantee) is shown in a smaller, black font. The login form consists of two input fields: the first is labeled "ユーザ名\*" (Username\*) and the second is labeled "パスワード\*" (Password\*). Below the password field is a blue button with the white text "ログイン" (Login). A horizontal line is positioned below the button.

## 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 nonexisting 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 30](#)
- [Anonymize Data, on page 31](#)
- [Configure Authentication and Policy Servers, on page 32](#)
- [Configure Cisco AI Network Analytics Data Collection, on page 34](#)
- [Update the Machine Reasoning Knowledge Base, on page 37](#)
- [Cisco Accounts, on page 38](#)
- [Device Controllability, on page 42](#)
- [Cloud Access Keys, on page 44](#)
- [Integrity Verification, on page 45](#)
- [Configure an IP Address Manager, on page 47](#)
- [Configure Debugging Logs, on page 48](#)
- [Configure the Network Resync Interval, on page 50](#)
- [View Audit Logs, on page 50](#)
- [Activate High Availability, on page 52](#)
- [Configure Integration Settings, on page 52](#)
- [Set Up a Login Message, on page 53](#)
- [Configure the Proxy, on page 53](#)
- [Security for Cisco DNA Center, on page 54](#)
- [Configure the SFTP Server, on page 68](#)
- [Configure SNMP Properties, on page 68](#)
- [About Product Usage Telemetry Collection, on page 69](#)
- [Configure vManage Properties, on page 69](#)
- [Account Lockout, on page 70](#)
- [Password Expiry, on page 70](#)

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

**Note** All logging in Cisco DNA Center is enabled, by default.

- **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 and the integration status. 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 > 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 is 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 this step for the other appliances in your cluster, if necessary.
- 

### Delete Cisco IMC Settings



To delete the Cisco IMC connectivity settings that have been configured previously for a particular appliance, complete 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.
- Step 3** At the confirmation prompt, click **Ok**.
- 

## Subscribe to System Event Notifications

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 event notifications. See the "Work with Events" topic in the [Cisco DNA Center Platform User Guide](#) for a description of how to subscribe to these notifications. When completing this procedure, ensure that you select and subscribe to the following events in the **Platform > Developer Toolkit > Events** table:

- SYSTEM-CIMC
- SYSTEM-DISASTER-RECOVERY
- SYSTEM-EXTERNAL-CMX
- SYSTEM-EXTERNAL-IPAM
- SYSTEM-EXTERNAL-ISE-AAA-TRUST
- SYSTEM-EXTERNAL-ISE-PAN-ERS
- SYSTEM-EXTERNAL-ISE-PXGRID
- SYSTEM-EXTERNAL-ITSM
- SYSTEM-HARDWARE

## Event Notification Information

The following table lists the key information that Cisco DNA Center provides when it generates a system health notification message.

Domain	Subdomain	Tag	Instance	State	Message
System	CPU	CPU	<node-hostname>CPU1	Ok	Cisco DNA Center CPU-1 is working as expected on <node-hostname>
				NotOk	Cisco DNA Center CPU-1 has failed on <node-hostname>
				Disabled	Cisco DNA Center CPU-1 is disabled on <node-hostname>
	Memory	Memory	<node-hostname>DIMM_A1	Ok	Cisco DNA Center RAM DIMM_A1 is working as expected on <node-hostname>
				NotOk	Cisco DNA Center RAM DIMM_A1 has failed on <node-hostname>
	Disk	Disk	<node-hostname>Disk1	Ok	Cisco DNA Center Disk 2 is working as expected on <node-hostname>
				NotOk	Cisco DNA Center Disk 2 has failed on <node-hostname>
	RAID Controller	RAIDController	<node-hostname>Ctrl1	Ok	Cisco DNA Center RAID VD-2 is working as expected on <node-hostname>
				NotOk	Cisco DNA Center RAID VD-2 has degraded on <node-hostname>
				Disabled	Cisco DNA Center RAID VD-2 is offline on <node-hostname>
	Network Interfaces	NIC	<node-hostname>nic1	Ok	Cisco DNA Center network interfaces are working as expected
				NotOk	Cisco DNA Center: <x> network interfaces are missing for <node-hostname>: nic-1
PSU_FAN	PSU	<node-hostname>psu1	Ok	Cisco DNA Center power supply (PSU-1) is powered on and thermal condition is normal for <node-hostname>	
			NotOk	Cisco DNA Center power supply (PSU-2) is powered off and thermal condition is critical for <node-hostname>	

Domain	Subdomain	Tag	Instance	State	Message
	Disaster Recovery	DisasterRecovery	<disaster-recovery-name>	Ok	<ul style="list-style-type: none"> <li>Disaster recovery cluster is up</li> <li>Disaster recovery failover succeeded to &lt;site-name&gt;</li> </ul>
				Degraded	<ul style="list-style-type: none"> <li>Disaster recovery failover triggered from &lt;site-name&gt; to site-name</li> <li>Disaster recovery failed while failing over to &lt;site-name&gt;</li> <li>Disaster recovery standby cluster on &lt;site-name&gt; is down; cannot failover</li> <li>Disaster recovery witness is down; cannot failover</li> <li>Disaster recovery replication halted; recovery point objective will be impacted</li> <li>Disaster recovery pause failed</li> <li>Disaster recovery route advertisement failed</li> <li>Disaster recovery IPSec communication failed</li> </ul>
				NotOk	<ul style="list-style-type: none"> <li>Disaster recovery configuration failed</li> <li>Disaster recovery failed to rejoin the standby system</li> </ul>
Connectivity	ISE	ISE_ERS	<CiscoISEhostname>	Success	ISE AAA trust establishment succeeded for ISE server <ISE-server-details>
				Failed	ISE AAA trust establishment failed for ISE server <ISE-server-details>

Domain	Subdomain	Tag	Instance	State	Message
Integrations	IPAM	IPAM	<IPAM-hostname>	Ok	IPAM connection to Cisco DNA Center established. IPAM <IPAM-IP-address>.
				Critical	IPAM connection to Cisco DNA Center offline. IPAM <IPAM-IP-address>.
	ISE	ISE_AAA	<ISE-hostname>	Up	ISE AAA trust establishment succeeded for ISE server. ISE <ISE-IP-address>
				Down	ISE AAA trust establishment failed for ISE server. ISE <ISE-IP-address>
	CMX	CMX	<CMX-hostname>	serviceAvailable	CMX connection to Cisco DNA Center offline. CMX <CMX-IP-address>.
				serviceNotAvailable	CMX connection to Cisco DNA Center offline. CMX <CMX-IP-address>.
	ITSM	ITSM	<ITSM-hostname>	Up	ITSM connection to Cisco DNA Center offline. ITSM <ITSM-IP-address>.
				Down	ITSM connection to Cisco DNA Center offline. ITSM <ITSM-IP-address>.

## 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 Event Notifications, on page 20](#)

To view this page, click the **Menu** icon (☰) in the Cisco DNA Center GUI and choose **System > System Health**. Topology data is polled every 30 seconds. If any new data is received, the topology automatically updates to reflect this data.

Note the following:

- Cisco DNA Center now supports IPv6. When viewing a cluster on which IPv6 is enabled, the topology also displays the following information for that cluster's Enterprise virtual IP address:

- **Pre** field: 16-bit prefix
- **GID** field: 32-bit global ID
- **Subnet** field: 16-bit subnet value

The remainder of the cluster's Enterprise virtual IP address is used to label its topology icon.

- An IPv6-enabled cluster can only connect to and retrieve data from external systems that also support IPv6.

## Troubleshoot Appliance and External System Issues

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

## Troubleshoot External System Connectivity Issues

If Cisco DNA Center is currently unable to communicate with an external system, do the following to ping that system and troubleshoot why it cannot be reached.

### Before you begin

Do the following before you complete this procedure:

- Install the Machine Reasoning package. See "Download and Install Packages and Updates" in the [Cisco DNA Center Administrator Guide](#).
- Create a role that has write permission to the Machine Reasoning function and assign that role to the user that will complete this procedure. To access this parameter in the **Create a User Role** wizard, expand the **System** row in the **Define the Access** wizard page. For more information, see "Configure Role-Based Access Control" in the [Cisco DNA Center Administrator Guide](#).

- 
- Step 1** From the top-right portion of the **System Health** page, choose **Tools > Network Ping** to open the **Ping Device** page. The page lists all of the devices that Cisco DNA Center currently manages.



- Step 2** Click the radio button for any device whose reachability status is **Reachable** and then click the **Troubleshoot** link. The **Reasoner Inputs** pop-up window opens.
- Step 3** In the **Target IP Address** field, enter the IP address of the external system that cannot be reached.
- Step 4** Click **Run Machine Reasoning**.  
A dialog box is displayed after Cisco DNA Center has pinged the external system.
- Step 5** Click **View Details** to see whether the ping was successful.
- Step 6** If the ping failed, click the **View Relevant Activities** link to open the **Activity Details** slide-in pane and then click the **View Details** icon.  
The **Device Command Output** pop-up window opens, listing possible causes for the inability to reach the external system.

## 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 - xxx) State is Disabled	—	PowerSupply PSU1 (SerialNumber - xxx) 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	—	<ul style="list-style-type: none"> <li>A third-party IPAM provider is connected.</li> <li>There is no third-party IPAM provider connected.</li> <li>The third-party IPAM provider is currently synchronizing.</li> </ul>
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 <i>Cisco Identity Services Engine Administrator Guide</i> 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 <i>Cisco Identity Services Engine Administrator Guide</i> 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 <i>Cisco Digital Network Architecture Center Second Generation Appliance Installation Guide</i> for more information.</li> <li>3. Reestablish trust. See the "Enable PKI in Cisco ISE" topic in the <i>Cisco Identity Services Engine Administrator Guide</i> 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 <i>Cisco Identity Services Engine Administrator Guide</i> 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 <i>Cisco Identity Services Engine Administrator Guide</i> 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 <i>Cisco Identity Services Engine Administrator Guide</i> 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, Cisco DNA Center 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 must 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 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.
- 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, 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 HA 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 information.
- 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 do not interfere with the Cisco DNA Center and Cisco ISE pxGrid connection.
- You can change the RADIUS secret password. You provided the secret password when you configured Cisco ISE as a AAA server on the **System > Settings > External Services > Authentication and Policy Servers** page. To change the secret password, go 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.
- 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 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 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 certificate signed by your internal certificate authority (CA) 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 contain up to 128 characters.

**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 in to 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**.

- **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 several 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 Cisco ISE server is "FAILED" due to a password change, click **Retry**, and update the password to resynchronize the Cisco ISE connectivity.

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

- **Protocol**: **TACACS** and **RADIUS** (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. Cisco DNA Center supports only port 49 for TACACS; do not change the port number.
- **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 the preceding steps.

## 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 74](#).
- 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.eu1.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 **External Services** and choose **Cisco AI Analytics**.  
The **AI Network Analytics** window appears.

## 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](#) ⓘ

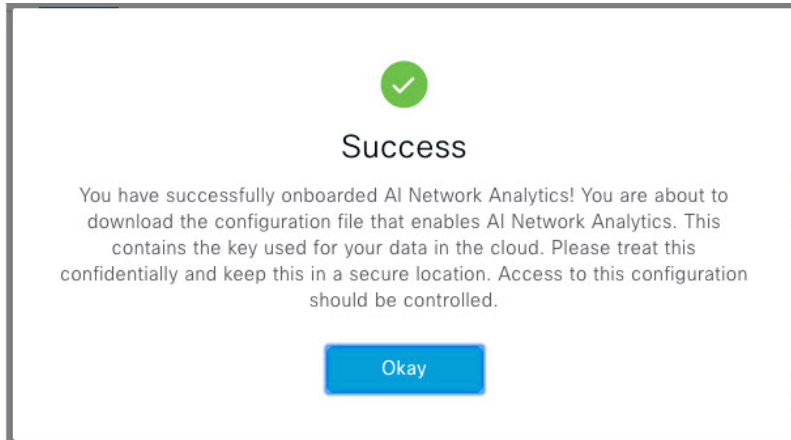
**Step 3** Do one of the following:

- 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.



- 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 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 **External Services** and choose **Cisco AI Analytics**.  
The **AI Network Analytics** window appears.
- Step 3** In the **Cloud Connection** area, click the button to off, such that  appears.
- 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 77](#).

---

**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 are configured for 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 44](#) for a description of how to re-enter 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 77](#).

- 
- 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 Cisco Smart Software Manager (SSM). Ensure that you have SUPER-ADMIN access permission to configure the different connection modes.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Settings > Cisco Accounts > SSM Connection Mode**.
- The following connection modes are available:
- **Direct**
  - **On-Prem CSSM**
  - **Smart Proxy**
- Step 2** Choose **Direct** to enable a direct connection to the Cisco SSM cloud.
- Step 3** If your organization is security sensitive, choose **On-Prem CSSM**. The on-prem option lets you access a subset of Cisco SSM functionality without using a direct internet connection to manage your licenses with the Cisco SSM cloud.
- Before you enable **On-Prem CSSM**, make sure that the satellite is deployed, up, and running in your network site.
  - Enter the details for the **On-Prem CSSM Host**, **Smart Account Name**, **Client Id**, and **Client Secret**.  
For information about how to retrieve the client ID and client secret, see the [Cisco Smart Software Manager On-Prem User Guide](#).
  - Click **Test Connection** to validate the CSSM connection.
  - Click **Save** and then **Confirm**.
- Caution** If there are any smart-enabled devices in your network that are already registered with CSSM, those devices are deregistered from the CSSM. After deregistration, devices go into Evaluation License mode, and network performance might degrade or an outage might occur. Therefore, we recommend that you perform this operation during a maintenance window.
- Step 4** Choose **Smart Proxy** to register your smart-enabled devices with the Cisco SSM cloud through Cisco DNA Center. With this mode, devices do not need a direct connection to the Cisco SSM cloud. Cisco DNA Center proxies the requests from the device to the 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

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure—you control what users can access. With Smart Licensing, you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more product activation keys (PAKs).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

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

For a more detailed overview on Cisco licensing, go to [cisco.com/go/licensingguide](https://cisco.com/go/licensingguide).

### Before you begin

- To enable Smart Licensing, you must configure Cisco Credentials (see [Configure Cisco Credentials, on page 38](#)) and upload Cisco DNA Center license conventions in Cisco SSM.
- Smart Licensing is not supported when the **System > Settings > Cisco Accounts > SSM Connection Mode** is **On-Prem CSSM**.

---

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

By default, **Smart User** and **Smart Domain** details are displayed.

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

**Step 3** Click **Register**.

**Step 4** After successful registration, click the **View Available Licenses** link to view the available 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 is pushed to the device, go to **Provision > Inventory** and from the **Focus** drop-down list, choose **Provision**. In the **Provision Status** column, click **See Details**.



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

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

- **Device Discovery**

- SNMP Credentials
- NETCONF Credentials

- **Adding Devices to Inventory**

Cisco TrustSec (CTS) Credentials



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

- **Assigning Devices to a Site**

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

Device controllability is enabled by default. If you do not want device controllability enabled, disable it manually. For more information, see [Configure Device Controllability, on page 44](#).

When device controllability is disabled, Cisco DNA Center does not configure any of the preceding credentials or features on devices while running discovery or when the devices are assigned to a site. However, the telemetry settings and related configuration are pushed when the device is provisioned or when the **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.

In earlier releases, the following IPDT commands were configured:

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

For each interface:

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

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

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

For each interface:

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

- **Device in Global Site:** When you successfully add, import, or discover a device, 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 Cisco DNA Center and check the **Configuration Clean-up** check box, the SNMP server, Syslog server, and NetFlow collector settings are removed from the device.
- **Device Moved from Site to Site:** If you move a device—for example, from Site A to Site B—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 the **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.



---

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

---

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

- 
- Step 1** 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 53](#).
- 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 74](#).

- 
- 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/cscrdtr/security/center/files/trust/Cisco\\_KnownGoodValues.tar](https://tools.cisco.com/cscrdtr/security/center/files/trust/Cisco_KnownGoodValues.tar)

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




---

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

---

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 77](#).

---

**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](https://tools.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](https://tools.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 77](#).

- 
- 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 77](#).
- 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**, **Log ID**, or **Description**.
- Step 6** Click **Subscribe** to subscribe the audit log events.
- A list of syslog servers appears.
- Step 7** Check the syslog server check box that you want to subscribe and click **Save**.
- Note** Uncheck the syslog server check box to unsubscribe the audit log events and click **Save**.
- Step 8** In the right pane, use the **Search** field to search for specific text in the log message.
- Step 9** 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.
- Step 10** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Activity > Work Items** tab to view in progress, completed, and failed work items.
- 

## Export Audit Logs to Syslog Servers

**Security Recommendation:** We strongly encourage you to export audit logs from Cisco DNA Center to a remote Syslog Server in your network, for more secure and easier log monitoring.

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

### Before you begin

You must configure the syslog servers in the **System > Settings > External Services > Destinations > Syslog** area.

---

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Activity > Audit Logs**.
- Step 2** Click **Subscribe**.
- Step 3** Select the syslog servers that you want to subscribe to and click **Save**.

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

---

## View Audit Logs in Syslog Server Using APIs

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

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

## 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.



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

---

### Before you begin

You have installed the Cisco DNA Center platform.

---

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

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

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

**Step 3** Click **Apply**.


---

## 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.



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

---

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 77](#).

**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 the Proxy Certificate, on page 57](#).

---

## 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 in a private internal network and behind a firewall that does not expose Cisco DNA Center to an untrusted network, such as the internet.
- If you have separate management and enterprise networks, connect Cisco DNA Center's management and enterprise interfaces to your management and enterprise networks, respectively. Doing so ensures network isolation between services used to administer and manage Cisco DNA Center and services used to communicate with and manage your network devices.
- If deploying Cisco DNA Center in a three-node cluster setup, verify that the cluster interfaces are connected in an isolated network.
- Replace the self-signed server certificate from Cisco DNA Center with the certificate signed by your internal certificate authority (CA).
- Upgrade Cisco DNA Center with critical upgrades, including security patches, as soon as possible after a patch announcement. For more information, see the [Cisco DNA Center Upgrade Guide](#).
- Restrict the remote URLs accessed by Cisco DNA Center using an HTTPS proxy server. Cisco DNA Center is configured to access the internet to download software updates, licenses, and device software, as well as provide up-to-date map information, user feedback, and so on. Providing internet connections for these purposes is a mandatory requirement. However, provide connections securely through an HTTPS proxy server.

- Restrict the ingress and egress management and enterprise network connections to and from Cisco DNA Center using a firewall, by only allowing known IP addresses and ranges and blocking network connections to unused ports.

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

**Security Recommendation:** We recommend that you upgrade the minimum TLS version to TLSv1.2 for incoming TLS connections to Cisco DNA Center.

Northbound REST API requests from the external network such as 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.

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

Cisco DNA Center provides a configuration option to downgrade the minimum TLS version and enable RC4-SHA, if your network devices under Cisco DNA Center control cannot support the existing minimum TLS version (TLSv1.1) or ciphers. For security reasons, however, we do not recommend that you downgrade Cisco DNA Center 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 the 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 77](#).
- 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 appears in the Cisco DNA Center GUI two months before 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 returns the imported proxy gateway certificate when requested by a proxy gateway. If you don't click the **Enable** button, the controller returns its own self-signed or imported CA certificate to the proxy gateway.

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

---

## 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 your internal CA. 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 your internal 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 your internal CA. Additionally, you must replace the self-signed certificate (installed in Cisco DNA Center by default) with a certificate that is signed by your internal 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 certificate signed by your internal certificate authority (CA), ensure that the certificate specifies all of the DNS names (including the Cisco DNA Center FQDN) 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 **Certificates** window in the GUI.

### Before you begin

You must obtain a valid X.509 certificate that is issued by your internal CA and the certificate must correspond to a private key in your possession.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Settings > Trust & Privacy > Certificates**.
- Step 2** In the **System** tab, view the current certificate data.

When you first view this window, the current certificate data that is displayed 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 **System** tab displays the following fields:

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

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

The following fields appear:

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

**Step 4** (Optional) Check the **Use system certificate for Disaster Recovery as well** check box if you want to use the same certificate for disaster recovery.

**Step 5** In the **Certificate** area, 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 6** 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 and Drop area.

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

After the upload succeeds, the system certificate is validated.

- For the **Private Key** field, import the private key by dragging and dropping the file into the Drag and Drop area.

**Note** Private keys must have a valid private key format extension (.key). The maximum file size for the private key is 10 MB.

After the upload succeeds, the private key is validated.

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

**Step 7** 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 and Drop area.

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

After the upload succeeds, the system certificate is validated.

- For the **Certificate** field, enter the passphrase for the certificate in the **Password** field.

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

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

**Step 8** Click **Save**.

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

**Step 9** Return to the **Certificates** window to view the updated certificate data. The information displayed in the **System** tab should have changed to reflect the new certificate name, issuer, and the certificate authority.

---

## Use an External SCEP Broker

You can use your own PKI broker and certificate service for devices and Cisco DNA Center. You can also enable and disable the use of an external device PKI or deprecate the settings between one or the other.

To upload an external PKI broker:

---

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

**Step 2** In the PKI Certificates window, click the **Use external SCEP broker** radio button.

**Step 3** Use one of the following options to upload an external certificate:

- Choose a file
- Drag and drop to upload

**Note** Only file types such as .pem, .crt, and .cer are accepted. The file size cannot exceed 10 MB.

**Step 4** Click **Upload**.

**Step 5** (Optional) If you want to perform auto enrollment, complete the following steps:

- a) Check the **Auto Enrollment** check box and enter the specified URL in the **Enrollment URL** field.
- b) Enter the subject in the **Subject Options** field.
- c) In the **Revocation Check** field, click the drop-down list and choose the appropriate revocation check option.
- d) Check the **Auto Renew** check box and enter an auto enrollment percentage.
- e) Click **Save**.

The external CA certificate is uploaded.

If you want to replace the uploaded external certificate, click **Replace Certificate** and enter the required details.

## Switch Back to an Internal PKI Certificate

After uploading an external certificate, if you want to switch back to the internal certificate, do the following:

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Settings > Trust & Privacy > PKI Certificates**.
- Step 2** In the PKI Certificates window, click the **Use Cisco DNA Center** radio button.
- Step 3** In the **Switching back to Internal PKI Certificate** alert, click **Apply**.  
The **Settings have been updated** message appears. For more information, see [Change the Role of the PKI Certificate from Root to Subordinate](#)

## 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 **Save**.
- 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).
  - **Sub CA Mode:** Enables a change from a root CA to a subordinate CA.
- Step 4** In the **CA Management** tab, check the **Sub CA Mode** check box.
- Step 5** Click **Next**.
- Step 6** Review the 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 63](#).
  - 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 77](#).

---

- 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 **Save**.

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

---

## About Product Usage Telemetry Collection

Cisco DNA Center collects product usage telemetry and provides data about the status and capabilities of the 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 is enabled by default. We recommend that you contact the 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** Choose the **Idle Session Timeout** value from the drop-down list.

**Step 5** Click **Save** to set the account lockout settings.

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

---

## Password Expiry

You can configure the password expiration policy to manage the 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 73
- [Download and Update System Updates](#), on page 73
- [Download and Install Packages and Updates](#), on page 74
- [Uninstall a Package](#), on page 75

## 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 77](#).

---

**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 77](#).

---

**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 77](#).

- 
- 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 77](#)
- [About User Roles, on page 77](#)
- [Create an Internal User, on page 78](#)
- [Edit a User, on page 78](#)
- [Delete a User, on page 79](#)
- [Reset a User Password, on page 79](#)
- [Change Your Own User Password, on page 80](#)
- [Reset a Forgotten Password, on page 80](#)
- [Configure Role-Based Access Control, on page 80](#)
- [Display Role-Based Access Control Statistics, on page 85](#)
- [Configure External Authentication, on page 85](#)
- [Two-Factor Authentication, on page 88](#)
- [Display External Users, on page 91](#)

## 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 an Internal User

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

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 77](#).

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Users & Roles > User Management**.
- Step 2** Click **Add**.
- Step 3** Enter a first name, last name, email address, and username for the new user.  
The email address must meet the requirements for the standard Apache EmailValidator class.
- Step 4** Under **Role List**, choose one of the following roles: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.
- Step 5** Enter a password and confirm it. The password must contain:
- At least eight characters
  - A character from at least three of the following categories:
    - Lowercase letter
    - Uppercase letter
    - Number
    - Special character
- Step 6** Click **Save**.
- 

## Edit a User

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

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 77](#).

- 
- 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 edit.
- Step 3** Click **Edit**.
- Step 4** Edit the first or last name or email address, if needed.
- Step 5** Under **Role List**, choose a new role, if needed: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.
- Step 6** Click **Save**.
- 

## Delete a User

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles, on page 77](#).

---

- 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 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 77](#).

---

- 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
  - 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.



### 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.

## Cisco DNA Center User Role Permissions

Table 4: Cisco DNA Center User Role Permissions

| Capability                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assurance                      | Assure consistent service levels with complete visibility across all aspects of your network.                                                                                                                                                                                                                                                                                                                                                                                      |
| Monitoring and Troubleshooting | Monitor and manage the health of your network with issue troubleshooting and remediation, proactive network monitoring, and insights driven by AI Network Analytics.<br>This role lets you: <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            | Configure and manage issues. Update network, client, and application health thresholds.<br>Note: You must have at least Read permission on Monitoring and Troubleshooting.                                                                                                                                                                                                                                                                                                         |
| Troubleshooting Tools          | Create and manage sensor tests. Schedule on-demand forensic packet captures (Intelligent Capture) for troubleshooting clients.<br>Note: You must have at least Read permission on Monitoring and Troubleshooting.                                                                                                                                                                                                                                                                  |
| Network Analytics              | Manage network analytics-related components.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Data Access                    | Enable access to query engine APIs.<br>Note: Do not set the permission to Deny, because all applications will fail.                                                                                                                                                                                                                                                                                                                                                                |
| Network Design                 | 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      | <ul style="list-style-type: none"> <li>• Update network settings such as global device credentials, authentication and policy servers, certificates, trustpool, cloud access keys, Stealthwatch, Umbrella, and data anonymization.</li> <li>• Export the device inventory and its credentials.</li> </ul> <p><b>Note</b> To complete this task, you must have Read permissions on Network Settings.</p>                                                                            |
| Image Repository               | Manage software images and facilitate upgrades and updates on physical and virtual network entities.                                                                                                                                                                                                                                                                                                                                                                               |

| Capability               | Description                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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         | 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.<br><br>Note: To create SSIDs, you must have Write permission on Network Settings.                                                                                                                                    |
| Network Settings         | Common site-wide network settings such as AAA, NTP, DHCP, DNS, Syslog, SNMP, and Telemetry. Users with this role can add an SFTP server and modify the Network Resync Interval in System Settings.<br><br>Note: To create wireless profiles, you must have Write permission on Network Profiles.                                                                                                                                |
| Virtual Network          | 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.                                                                                                                                                                                                                                                                                                                                                       |
| Compliance               | Manage compliance provisioning.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Image Update             | Upgrade a software image on devices after a complete upgrade lifecycle.                                                                                                                                                                                                                                                                                                                                                         |
| Inventory Management     | Discover, add, replace, or delete devices on your network while managing device attributes and configuration properties.<br><br>Note: To replace a device, you must have Write permission on <b>Network Provision &gt; PnP</b> .                                                                                                                                                                                                |
| License                  | Unified view of your software and network assets relative to license usage and compliance.                                                                                                                                                                                                                                                                                                                                      |
| Network Telemetry        | Enable or disable the collection of application telemetry from devices. Configure the telemetry settings associated with the assigned site. Configure other settings like wireless service assurance and controller certificates.<br><br>Note: To enable or disable network telemetry, you must have Write permission on <b>Provision</b> .                                                                                     |
| 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.<br><br>Note: To provision devices in sites that have network profiles attached, you must have at least Read permission on <b>Network Profiles</b> . |
| <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 the wide-area Bonjour service across your network to enable policy-based service discovery.                                                                                                                                                                                                                                                                                                                              |


| Capability              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stealthwatch            | <p>Configure network elements to send data to Cisco Stealthwatch to detect and mitigate threats, even in encrypted traffic.</p> <p>To provision Stealthwatch, you must have Write permission 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>                                                                |
| 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 permission 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 permission on <b>Advanced Network Settings</b>.</p> |
| <b>Platform</b>         | 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>                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Security</b>         | 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.                                                                                                                                                                                                                                                                                                                                                                                                         |

| Capability        | Description                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System            | Centralized administration of Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.                                                                                                                                                                                                                                      |
| Machine Reasoning | Configure automatic updates to the machine reasoning knowledge base to rapidly identify security vulnerabilities and improve automated issue analysis.                                                                                                                                                                                                                           |
| System Management | Manage core system functionality and connectivity settings. Manage user roles and configure external authentication.<br><br>This role includes Cisco Credentials, Integrity Verification, Proxy Config, Device EULA, HA, Integration Settings, Disaster Recovery, Debugging Logs, Telemetry Collection, System EULA, IPAM, vManage Servers, Backup & Restore, and Data Platform. |
| 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.                                                                                                                                                                                                                                               |
| Scheduler         | Integrated with other back-end services, scheduler lets you schedule tasks such as deploy policies, provision network devices, or upgrade.                                                                                                                                                                                                                                       |
| 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.

---

## 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 77](#).
- You must configure at least one authentication server.



**Note** The external authentication fallback behavior has changed in this Cisco DNA Center release. In releases earlier than 2.1.x, when external authentication is enabled, Cisco DNA Center falls back to local users if the AAA server is unreachable or the AAA server rejects an unknown username. In the current release, Cisco DNA Center does not fall back to local users if the AAA server is unreachable or the AAA server rejects an unknown username.

To enable external authentication fallback, SSH to the Cisco DNA Center instance and enter the following CLI command:

```
magctl rbac external_auth_fallback enable
```

**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**.

- In the **AAA Attribute** field, leave the default value of **Cisco-AVPair** or enter the new AAA attribute value.
- 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. 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.

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

| Name                          | Description                                                                                                                                                                                                                                                            |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Password</b>               | Password for the Cisco ISE CLI username.                                                                                                                                                                                                                               |
| <b>FQDN</b>                   | 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:<br><br><i>hostname.domainname.com</i><br><br>For example, the FQDN for a Cisco ISE server might be ise.cisco.com. |
| <b>Subscriber Name</b>        | A unique text string—for example, <code>acme</code> —that is used during Cisco DNA Center-to-Cisco ISE integration to set up a new pxGrid client in Cisco ISE.                                                                                                         |
| <b>SSH Key</b>                | Diffie-Hellman-Group14-SHA1 SSH key used to connect and authenticate with Cisco ISE.                                                                                                                                                                                   |
| <b>Virtual IP Address(es)</b> | 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                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Protocol</b>            | TACACS or RADIUS.                                                                                                                                                                                                                                                                            |
| <b>Authentication Port</b> | 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>                                                                     |
| <b>Accounting Port</b>     | 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> |
| <b>Retries</b>             | Number of times that Cisco DNA Center can attempt to connect with Cisco ISE.                                                                                                                                                                                                                 |
| <b>Timeout</b>             | Length of time that Cisco DNA Center waits for Cisco ISE to respond. The maximum timeout value is 60 seconds.                                                                                                                                                                                |

- e) Click **Update**.

# Two-Factor Authentication

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

The 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:

- a) Click **Add**.
- b) 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`
- c) 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.

---

## 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 93
- [Integration with Cisco Smart Accounts](#), on page 96
- [Set Up License Manager](#), on page 97
- [Visualize License Usage and Expiration](#), on page 98
- [View License Details](#), on page 99
- [Change License Level](#), on page 99
- [Export License Information](#), on page 100
- [Auto Registration of Smart License-Enabled Devices](#), on page 101
- [Day 0 Configuration for Smart License-Enabled Devices](#), on page 101
- [Apply Specific License Reservation or Permanent License Reservation to Devices](#), on page 102
- [Cancel SLR or PLR Applied to Devices](#), on page 104
- [Install the Authorization Code and Enable the High Security License](#), on page 104
- [Upload Resource Utilization Details to CSSM](#), on page 105
- [Change Device Throughput](#), on page 105
- [Transfer Licenses Between Virtual Accounts](#), on page 106
- [Manage Customer Tags to Smart License-Enabled Devices](#), on page 106
- [Modify License Policy](#), on page 107

## 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** window contains tabs with the following information:

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

- **All License:** The **License Summary** shows the total licenses purchased from Cisco Smart Software Management (CSSM), number of licenses that are about to expire, and out-of-compliance details for all types of licenses for all Cisco devices.
- **Reporting and Compliance:** The **License Summary** shows the total licenses purchased from CSSM, number of licenses that are about to expire, and out-of-compliance details for all types of licenses for all Cisco devices. The **Smart License Readiness** shows the steps to take before devices can be updated to the simplified model. The **Smart License Compliance** card allows you to launch the **Smart License Update** workflow.
- **Notifications:** Shows notifications such as CSSM Connectivity, Connection Mode, Device App Over Usage, Upload Usage Report, and so on.

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



**Note** Not all controls are available in every tab.


**Table 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 choose <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 99</a> . |
| <b>Change Virtual Account</b>                                            | Select one or more licenses and choose <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 choose <b>Actions &gt; Manage Smart License &gt; Register</b> to register the Smart License-enabled devices.                                                                                                                                                          |
| <b>Manage Smart License &gt; Deregister</b>                              | Select one or more Smart License-enabled devices and choose <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), then choose <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.<br>You can update the SLR applied to a wireless device or switches with a wireless controller package.<br>Choose the device for which you want to update SLR, then choose <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 choose <b>Actions &gt; Manage License Reservation &gt; Cancel/Return License Reservation</b> to cancel or return the SLR or PLR applied to the device.                                                                                                                                               |

| Control                                                            | Description                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Manage License Reservation &gt; Factory License Reservation</b> | Choose the device and choose <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>License Usage</b>                                               | Click <b>License Usage</b> to see the license utilization percentage for all types of licenses.                                                                                                                                                                                             |
| <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 100</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 display in each page of the table.                                                                                                                                                                                                                    |

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



**Note** Not all columns are used in every tab. 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 99</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.                                                                                                                                            |

| Column                                         | Description                                                                           |
|------------------------------------------------|---------------------------------------------------------------------------------------|
| 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 99</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.                                                                                                                   |
| 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. You can add multiple Cisco Smart Accounts.



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

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

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

If you already have a Cisco Smart Account, you can use 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

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

## 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 multiple Smart Accounts, choose 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.com Credentials**.
- Step 3** Under **Cisco.com Credentials**, enter the username and password for your cisco.com account.
- Step 4** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Settings > Smart Account**.
- Step 5** Under **Smart Account**, click **Add** and enter the username and password for your Smart Account.
- Step 6** Click **Save**.
- Step 7** If you have multiple Smart Accounts, click **Add** and enter your additional accounts.

- Step 8** If you have multiple Smart Accounts, choose one account to be the default. The License Manager uses the default account for visualization and licensing operations. To change the default Smart Account:
- Click **Change** next to the selected Smart Account name.
  - Change the active Smart Account and choose a Smart Account to be the default.
  - Click **Apply**.  
After changing the default account, it takes several minutes to retrieve the data from CSSM and display it on the License Manager Overview and All License windows.
- Step 9** To edit a Smart Account, click the three dots in the Actions column and choose **Edit**.
- Step 10** To delete a nondefault Smart Account, click the three dots in the Actions column and choose **Delete**.
- Step 11** To access your Smart Account using a virtual or subordinate Smart Account name and password, under **Link Your Smart Account**, choose:
- **Use Cisco.com user ID** if your cisco.com and Smart Account credentials are the same.
  - **Use different credentials** if your cisco.com and Smart Account credentials are different, and then enter your Smart Account credentials.
- Step 12** Click **View all virtual accounts** to view all virtual Smart License Accounts.

---

### What to do next

Register the 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**, **All Licenses**, or **Reporting and Compliance**.
- The **License Usage** pie chart at the top of the window displays the aggregate number of purchased licenses and the number of licenses currently in use for the device category you selected. The graphs also indicate the proportion of Essentials versus Advantage licenses within each total.
- Under the graphs, the **License Usage** table shows subtotals for used and unused licenses, listed alphabetically by product family name.
- Step 3** To see detailed comparisons for a particular product family, click the name of the product family in the **Device Series** column.
- Cisco DNA Center displays details about the product family you selected.





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

## View 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 graph displays 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 can enter filter criteria in multiple fields. When you click **Apply**, the table displays only the rows displaying information that matches your filter criteria.
- If you want to view the devices that belong to a particular site, navigate to the site in the left pane, and click the site. The devices are filtered accordingly. A site marker indicating the site hierarchy is displayed at the top of the page.
- **Find:** Click in the **Find** field and enter the text you want to find in any of the table columns. When you press **Enter**, the table scrolls to the first row with text that matches your entry in the **Find** field.
  - **Customize:** Click  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 find the device you want, click the **Device Name** link in the row for that device.
- Cisco DNA Center displays the **License Details** window with complete license details and license history for the device you selected. **Actions** displays actions that can be performed on the device or its licenses.
- When you are finished, click  to close the **License Details** 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 99](#) 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 filename 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 > Smart Account**.
- Step 3** Click **License**.
- Step 4** Check the **Auto register smart license enabled devices** check box.
- Step 5** Choose a virtual account.
- Step 6** Click **Apply**.
- 

## Day 0 Configuration for Smart License-Enabled Devices

Devices that are already added to 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 Devices and Cisco DNA Center Are Connected to CSSM, on page 102](#).

To enable SLR or PLR when the device and Cisco DNA Center do not have connectivity to CSSM, see [Enable SLR/PLR When the Devices and Cisco DNA Center Are Not Connected to CSSM, on page 103](#).

## Enable SLR/PLR When the Devices 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 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** Obtain the authorization code for each device from CSSM and update it in the CSV file. See [Generate the Authorization Code from CSSM](#).
- Step 7** Click the **Upload CSV** link.
- Step 8** Click the **Select a file from your computer** link to select the saved CSV file.
- Step 9** Click **Continue**.
- Step 10** Choose a virtual account from which you want to reserve licenses and click **Continue**. SLR or PLR is applied to the selected devices.
- You can now view the updated status of the devices under **Reservation Status** on the **All Licenses** 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.

---

## Install the Authorization Code and Enable the High Security License

You can install the authorization code and enable the High Security (HSEC) license in a single workflow or in separate workflows, as required.

### Before you begin

Ensure that the Cisco IOS-XE software that is currently running on the device is 17.3.2 or later.

---

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > License Manager**.
  - Step 2** Click the **Reporting and Compliance** tab.
  - Step 3** Click **Smart License Compliance** card.
  - Step 4** In the **Smart License Update** window, click **Let's Do It**.  
To skip this window in the future, check **Don't show this to me again**.
  - Step 5** In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.
  - Step 6** Click **Next**.
  - Step 7** In the **Choose Sites and Devices** window, choose the devices on which you want to install the authorization code and click **Next**.
  - Step 8** In the Policy Settings window, review the CSSM policies and click **Next**.
  - Step 9** In the **Choose Device Features** window, do the following:
    - a) Choose the devices.
    - b) From the **Auth Codes** drop-down list, choose **Install**.
    - c) From the **HSEC** drop-down list, choose **Enable**.
    - d) Click **Next**.
  - Step 10** In the **Feature Summary** window, click **Next**.
  - Step 11** In the **Installing Device Features** window, view the authorization code and HSEC installation status and click **Next**.
-



# Upload Resource Utilization Details to CSSM

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

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > License Manager**.
- Step 2** Click the **Reporting and Compliance** tab.
- Step 3** Click the **Smart License Compliance** card.
- Step 4** In the **Smart License Update** window, click **Let's Do It**.  
To skip this window in the future, check **Don't show this to me again**.
- Step 5** In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.
- Step 6** Click **Next**.
- Step 7** In the **Choose Sites and Devices** window, choose the devices from which you want to retrieve the resource utilization details and click **Next**.
- Step 8** To upload the resource utilization details instantly, click **Next** in the **Reporting Policy** window. To schedule the reporting frequency, do the following:  
a) Under **Policy Settings**, enter an interval value.  
b) Click **Save**.
- Step 9** In the **Sync Data with Cisco** window, click **Next**.
- Step 10** The **Summary** window shows the status of operations that are performed in this workflow. Click **Finish** to complete this workflow.  
Cisco DNA Center sends an acknowledgment to the devices after successful synchronization of data with CSSM.
- 

# Change Device Throughput

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

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > License Manager**.
- Step 2** Click the **Reporting and Compliance** tab.  
The Reporting and Compliance window displays a table listing all your Smart License-enabled devices and their licenses.
- Step 3** Choose a device for which you want to change throughput.
- Step 4** Click **More Actions** and choose **Change Throughput**.
- Step 5** In the **Choose Throughput** window, choose the throughput value and click **Next**.
- Step 6** In the **Apply Throughput** window, click **Next**.
- Step 7** Click the **Recent Tasks** link to launch the **Recent Tasks** window.  
You can view the **Change Throughput** task status in the **Recent Task** window.
-

## Transfer Licenses Between Virtual Accounts

You can transfer licenses between virtual accounts.

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > License Manager**.  
The License Manager window displays a table listing all your discovered devices and their licenses.
- Step 2** Click the down arrow next to **Device View** and choose **License View**.
- Step 3** Choose the licenses that you want to transfer and click **Transfer Licenses**.
- Step 4** In the **Transfer Licenses** window, choose the virtual account.
- Step 5** Enter the **Transfer License Count** for each of the chosen licenses and click **Transfer**.
- Step 6** Click the **Recent Tasks** link to launch the **Recent Tasks** window.  
You can view the **License Transfer** task status in the **Recent Task** window.
- 

## Manage Customer Tags to Smart License-Enabled Devices

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

- 
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools > License Manager**.
- Step 2** Click the **Reporting and Compliance** tab.  
The Reporting and Compliance window displays a table listing all Smart License-enabled devices and their licenses.
- Step 3** Choose the devices on which you want to add customer tags.
- Step 4** Click **More Actions** and choose **Manage Free Form Fields** to add, update, or delete customer tags.
- Step 5** To add or update customer tags, do the following in the **Free Form Fields** window:  
a) Enter the customer tags.  
b) Click **Save**.
- Step 6** To delete customer tags, do the following in the **Free Form Fields** window:  
a) Click the delete icon for the customer tags that you want to delete.  
b) Click **Save**.  
c) In the **Warning** window, click **Continue**.
- Step 7** Click the **Recent Tasks** link to launch the **Recent Tasks** window.  
You can view the **Manage Customer Tags** task status in the **Recent Task** window.
-

# Modify License Policy

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

---

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

**Step 2** Click **Reporting and Compliance** tab.

**Step 3** In the **Smart License** table, click **Modify Policy**.

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

**Step 4** Under **Policy Settings**, click **Modify**.

**Step 5** In the **Change Reporting Interval** window, enter the reporting interval value.

**Step 6** Click **Save**.

---





## CHAPTER 7

# Backup and Restore

---

- [About Backup and Restore, on page 109](#)
- [Backup Server Requirements, on page 110](#)
- [Backup Storage Requirements, on page 111](#)
- [Example of NFS Server Configuration—Ubuntu, on page 112](#)
- [Example of NFS Server Configuration—CentOS, on page 113](#)
- [Configure Firewall Rules to Allow NFS, on page 114](#)
- [Configure Backup Servers, on page 115](#)
- [Back Up Data Now, on page 116](#)
- [Schedule Data Backups, on page 117](#)
- [Restore Data from Backups, on page 118](#)

## 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.

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 110](#).

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.



---

**Important**

After a backup and restore of Cisco DNA Center, you need to access the **Integration Settings** page and update (if necessary) the **Callback URL Host Name** or **IP Address**. For more information, see [Configure Integration Settings](#).

---

## Backup Server Requirements

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

- RedHat Enterprise (or CentOS) 7 or later
- Ubuntu 16.04 (or Mint, etc) or later

### Server Requirements for Automation Data Backup

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

- Must use SSH (port22)/remote sync (rsync). Cisco DNA Center does not support using FTP (port 21) when performing a backup.
- The Linux rsync utility must be installed.

- The backup user must own the destination folder for the backup or have read-write permissions for the user's group. For example, assuming the backup user is *backup* and the user's group is *staff*, 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 be a Linux-based NFS server that meets the following requirements:

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



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

## Backup Storage Requirements

Cisco DNA Center stores backup copies of Assurance data on an external NFS device and automation data on an external remote sync (rsync) target location. You must allocate enough external storage for your backups to cover the required retention. We recommend the following storage.

| Appliance     | NFS Storage (14 Days Incremental) | Rsync Storage (Daily Full) |
|---------------|-----------------------------------|----------------------------|
| DN2-HW-APL    | 1.7 TB                            | 50 GB                      |
| DN2-HW-APL-L  | 3 TB                              | 100 GB                     |
| DN2-HW-APL-XL | 8.4 TB                            | 300 GB                     |

Additional notes:

- The preceding table assumes fully loaded appliance configurations that support the maximum number of access points and network devices for each appliance.
- Only unique data is backed up to NFS. Therefore, single- and three-node HA configurations create backups of approximately equal sizes.
- NFS storage is the only available destination type for Assurance data backups.
- NFS backups are incremental after the first full backup. The preceding table assumes that the first day you run an Assurance data backup, a full backup is generated. Then, each subsequent day generates an incremental backup.
- Rsync storage is the only available destination type for automation data backups.
- The rsync backup sizing is estimated for one daily backup. If you want to retain backups for additional days, multiply the required storage by the additional number of days. For example, if you have a DN2-HW-APL appliance and you want to store five copies of automation data backups generated once each day, the total storage required is  $5 * 50 \text{ GB} = 250 \text{ GB}$ .

## Example of NFS Server Configuration—Ubuntu

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** Enter 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** Enter 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** Enter 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** Enter 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** Enter 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** Enter 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** Enter 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
```

---

## Example of NFS Server Configuration—CentOS

The following procedure shows an example NFS server configuration for CentOS.

---

**Step 1** Enter the `sudo yum check-update` command to access and update the Yellowdog Updater Modified (YUM) for the NFS server.

For example, enter a command similar to the following:

```
$ sudo yum check-update
```

**Step 2** Enter the `sudo yum install` command to install the advanced packaging tool for NFS.

For example, enter a command similar to the following:

```
$ sudo yum install -y nfs-utils
```

**Step 3** Enable and start the NFS server.

```
$ sudo systemctl enable nfs-server
```

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

**Step 4** Enter 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 <your_NFS_directory>
```

**Step 5** Enter the `sudo chown nfsnobody` command to change the ownership of the group.

For example, enter a command similar to the following:

```
$ sudo chown nfsnobody:nfsnobody /var/nfsshare
```

**Step 6** Enter 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 7** Enter 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 8** Enter 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
```

---

## Configure Firewall Rules to Allow NFS

By default, firewall is disabled on Debian/Ubuntu distributions but enabled on RedHat/CentOS distributions. Check whether firewall is enabled on Debian/Ubuntu distributions and if it is, add firewall rules.

### Configure Firewall Rules—Debian/Ubuntu

For **Debian/Ubuntu**, do the following:

---

**Step 1** Enter the following command to check whether firewall is enabled or disabled:

```
$ sudo ufw status
```

If firewall is disabled, the output shows:

```
Status: inactive
```

If firewall is enabled, the output shows:

```
Status: active
```

**Step 2** If firewall is enabled, set the static port for the mountd process to allow for easy firewall rule creation. To set the static port for mountd, change the following line to add `--port 32767` to `/etc/default/nfs-kernel-server`:

```
RPCMOUNTDOPTS="--manage-gids --port 32767"
```

**Step 3** Enter the following commands to add firewall rules to allow NFS:

```
sudo ufw allow portmapper
sudo ufw allow nfs
sudo ufw allow mountd
```

---

### Configure Firewall Rules—RedHat/CentOS

For **RedHat/CentOS**, do the following:

---

**Step 1** Add the mountd port to services and to `nfs.conf`.

**Note** RedHat/CentOS-based distributions use a different port for mountd than Debian-based distributions. RedHat/CentOS distributions use port **20048** for mountd in the `/etc/service` file.

Add the following lines to `/etc/nfs.conf` if they don't exist:

```
[mountd]
manage-gids = 1
port = 20048
```

**Step 2** Enter the following command to restart the NFS services and firewall:

```
sudo systemctl restart nfs-server rpcbind nfs-mountd
```

**Step 3** Enter the following commands to add firewall rules to allow NFS:

```
sudo firewall-cmd --permanent --add-service={nfs, rpc-bind, mountd}
sudo firewall-cmd --reload
```

## Configure Backup Servers

If you plan to back up automation data only, you need to configure the Cisco DNA Center Core System server. If you plan to back up both 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 77](#).
- The server that you plan to use for data backups must meet the requirements described in [Backup Server Requirements, on page 110](#).

**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.                                                                                                                                                                                                                                                                                              |
| Encryption Passphrase | Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials.<br><br>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 77](#).
- Backup servers meet the requirements described in [Backup Server Requirements, on page 110](#).
- Backup servers have been configured in Cisco DNA Center. For information, see [Configure Backup Servers, on page 115](#).

**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 Settings** and see [Configure Backup Servers, on page 115](#).

**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 automation and Assurance data.

- Click **Cisco DNA Center (without Assurance data)** to back up only 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 77](#).
- Backup servers meet the requirements described in [Backup Server Requirements, on page 110](#).
- Backup servers have been configured in Cisco DNA Center. For information, see [Configure Backup Servers, on page 115](#).

---

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

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

**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 automation and Assurance data.
- Click **Cisco DNA Center (without Assurance data)** to back up 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**.
  - If multiple clusters share the same Cisco AI Network Analytics configuration and are active at the same time, restoring a backup that includes the AI Network Analytics configuration on a different Cisco DNA Center cluster might result in data inconsistency and service disruption.

Therefore, the AI Network Analytics configuration must be active on a single cluster. To uninstall the AI Network Analytics package from any inactive cluster, choose **System > Software Updates > Installed Apps > AI Network Analytics > Uninstall**.

---

### 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 77](#).
- 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.

---







## CHAPTER 8

# Implement Disaster Recovery

- [Overview, on page 121](#)
- [Prerequisites, on page 125](#)
- [Add the Disaster Recovery Certificate, on page 128](#)
- [Configure the Witness Site, on page 130](#)
- [Configure Disaster Recovery, on page 131](#)
- [Failovers: An Overview, on page 141](#)
- [Pause Your Disaster Recovery System, on page 144](#)
- [Rejoin Your System, on page 146](#)
- [Backup and Restore Considerations, on page 148](#)
- [Disaster Recovery Event Notifications, on page 148](#)
- [Troubleshoot Your Disaster Recovery System, on page 150](#)

## Overview

Disaster recovery adds another layer of redundancy to safeguard against network downtime. It responds to a cluster failure by handing off network management duties to a connected cluster (referred to as a site going forward). Cisco DNA Center's disaster recovery implementation consists of three components: the main site, the recovery site, and the witness site. At any given time, the main and recovery sites are operating in either the active or standby role. The active site manages your network while the standby site maintains a continuously updated copy of the active site's data and managed services. Whenever an active site goes down, Cisco DNA Center automatically initiates a failover, completing the tasks necessary to designate the former standby site as the new active site.

Refer to the topics in this chapter for a description of how to set up and use disaster recovery in your production environment.

## Key Terms

The following terms are key for understanding Cisco DNA Center's disaster recovery implementation:

- **Main site:** The first site you configure when setting up your disaster recovery system. By default, it operates as the active site that manages your network. For information on how to configure the sites in your system, see [Configure Disaster Recovery, on page 131](#).
- **Recovery site:** The second site you configure when setting up your disaster recovery system. By default, it acts as your system's standby site.

- **Witness site:** The third site you configure when setting up your disaster recovery system. This site, which resides on a virtual machine or separate server, is not involved with the replication of data or managed services. Its role is to give the current active site the quorum it needs to carry out disaster recovery tasks. In the event that a site fails, this prevents the split brain scenario from taking place. This scenario can occur in a two-member system when the sites cannot communicate with each other. Each site believes that it should become active, creating two active sites. Cisco DNA Center uses the witness site to arbitrate between the active and standby sites, allowing only one active site at any given time. For a description of witness site requirements, see [Prerequisites, on page 125](#).
- **Register:** To add a site to a disaster recovery system, you must first register it with the system by providing information such as your main site's VIP. When registering your recovery or witness site, you will also need to provide the token that is generated when you register your main site. For more information, see [Configure Disaster Recovery, on page 131](#).
- **Configure Active:** The process of establishing a site as the active site, which involves tasks such as exposing the appropriate managed service ports.
- **Active site:** The site that is currently managing your network. Cisco DNA Center continuously replicates its data to your standby site.
- **Configure Standby:** The process of establishing a site as the standby site, which involves tasks such as configuring the replication of the active site's data and disabling the services which manage the network on the standby site.
- **Standby Ready:** When an isolated site meets the prerequisites to become a standby site, Cisco DNA Center moves it to this state. To establish this site as your system's standby site, click **Rejoin** in the **Action** area.
- **Standby site:** The site that maintains an up-to-date copy of your active site's data and managed services. In the event that your active site goes down, your system initiates a failover and your standby site takes over as the active site.



---

**Note** After a failover, Assurance restarts and processes a fresh set of data on the new active site. Historical Assurance data from the former active site is not migrated over.

---

- **Failover:** Cisco DNA Center supports two types of failover:
  - **System-triggered:** As soon as Cisco DNA Center recognizes that your active site has gone down, it automatically carries out the tasks required to establish your standby site as the new active site. You can monitor these tasks from the [Monitor the Event Timeline](#).
  - **Manual:** You can initiate a manual failover to designate the current standby site as the new active site. For more information, see [Initiate a Manual Failover, on page 141](#).
- **Isolate:** During a failover, the former active site is separated from the disaster recovery system. Cisco DNA Center suspends its services and stops advertising its virtual IP address (VIP). From here, Cisco DNA Center completes the tasks necessary to establish the former standby site as the new active site.
- **Pause:** Temporarily suspend your disaster recovery system in order to separate the sites that make up your system and stop data and service replication. For more information, see [Pause Your Disaster Recovery System, on page 144](#).

- **Rejoin:** From the **Disaster Recovery > Monitoring** tab, click this button in the **Action** area in order to add a Standby Ready or Paused site back into a disaster recovery system as the new standby site (after a failover has taken place). You would also click this button in order to restart a disaster recovery system that is currently paused.
- **Activate DR:** User-initiated operation that creates your system's active and standby sites. This operation entails setting up intracluster communication, verifying that the sites meet disaster recovery prerequisites, and replicating data between the two sites.
- **Deregister:** Click this button in the **Action** area to remove the three sites you have configured for your disaster recovery system. You must do so in order to make changes to any of the site settings you have entered previously.
- **Retry:** In the **Action** area, click this button in order to reinitiate any action that failed previously.

## Data Replication Overview

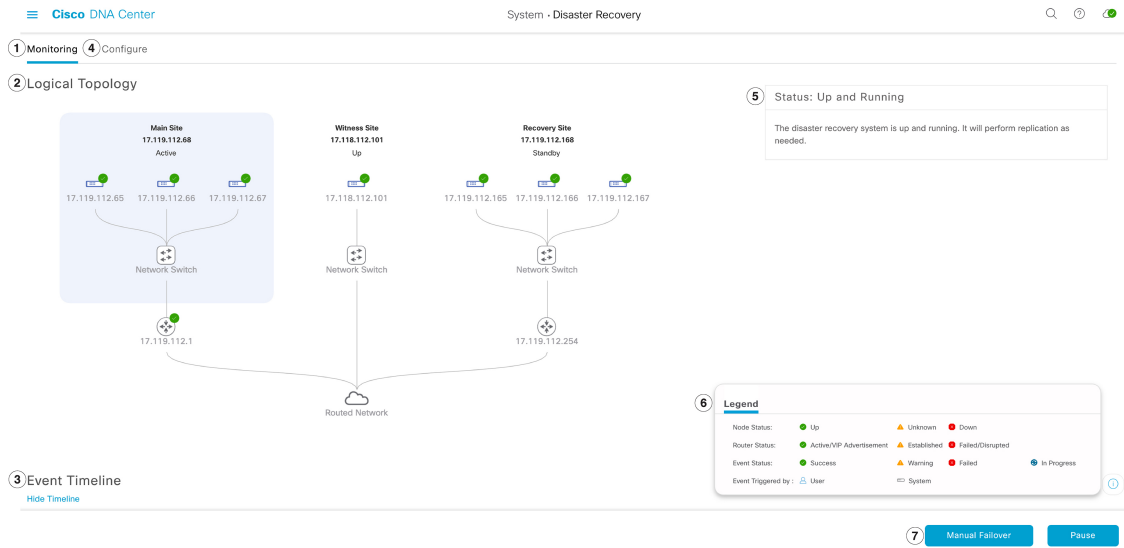
The data replication process syncs data between your disaster recovery system's main site and recovery site. Its duration will depend on a few factors: the amount of data that needs to be replicated, your network's effective bandwidth, and the amount of latency that exists between the main and recovery sites. When disaster recovery is active for your Cisco DNA Center deployment, data replication will *not* impact any operations or application use on the current active site (which is managing your network).

Either a full or incremental replication of data takes place, depending on which of the following scenarios is applicable:

- **After initial activation:** After the initial configuration and activation of your disaster recovery system, the recovery site does not have any data. In this scenario, a full replication of data between the main and recovery sites happens.
- **After a failover:** Whenever the current active site fails, the disaster recovery system triggers a failover. In this scenario, a full data replication between the main and recovery sites occurs after the failed site rejoins the system.
- **During normal operation:** This is the scenario that will typically apply to your system. During its day-to-day operation, changes that take place on the current active site are continuously synced with the current standby site.

## Navigate the Disaster Recovery GUI

The following table describes the components that make up Cisco DNA Center's disaster recovery GUI and their function.



| Callout | Description                                                                                                                                                                                                                                                                                                                                      |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | <p><b>Monitoring</b> tab: Click to do the following:</p> <ul style="list-style-type: none"> <li>• View a topology of the sites that make up your system.</li> <li>• Determine the current status of your system.</li> <li>• Perform disaster recovery tasks.</li> <li>• View a listing of the tasks that have been completed to date.</li> </ul> |
| 2       | <p><b>Logical Topology</b>: Displays a topology of your system that indicates the current status of your sites and their members. To view a description of the possible site states, see <a href="#">System and Site States, on page 137</a>.</p>                                                                                                |
| 3       | <p><b>Event Timeline</b>: Lists every disaster recovery task that is currently in progress or has been completed for your system. For more information, see <a href="#">Monitor the Event Timeline, on page 136</a>.</p>                                                                                                                         |
| 4       | <p><b>Configure</b> tab: Click to enter the settings necessary to establish a connection between your disaster recovery system's sites. See <a href="#">Configure Disaster Recovery, on page 131</a> for more information.</p>                                                                                                                   |
| 5       | <p><b>Status</b> area: Indicates the current status of your system. To view a description of the possible system states, see <a href="#">System and Site States, on page 137</a>.</p>                                                                                                                                                            |
| 6       | <p><b>Legend</b>: Indicates what the topology icons represent. To view the legend, click ⓘ in the bottom right corner of the <b>Disaster Recovery</b> page.</p>                                                                                                                                                                                  |
| 7       | <p><b>Action</b> area: Displays the disaster recovery tasks that are currently available for you to initiate. The tasks you can choose from vary, depending on whether you have configured your sites and your system's status.</p>                                                                                                              |

# Prerequisites

Before you enable disaster recovery in your production environment, ensure that the following prerequisites have been met.



## Important

If you plan to upgrade to the latest Cisco DNA Center 2.2.1.x release, you will need to complete a few steps in order to ensure that disaster recovery works properly after the upgrade. See [Configure Disaster Recovery After an Upgrade, on page 127](#) for more information.

## General Prerequisites

- You have allocated three systems to disaster recovery. Cisco DNA Center supports the following setups:
  - **Three-node setup:** One node functions as your main site, a second node serves as your recovery site, and a third system (residing on a virtual machine) acts as your witness site.
  - **Seven-node setup:** One three-node cluster functions as your main site, a second three-node cluster serves as your recovery site, and a third system (residing on a virtual machine) acts as your witness site.
- You have configured a VIP for the Enterprise port interface on your Cisco DNA Center appliances. This is required because disaster recovery uses the Enterprise network for intrasite communication. In the [Cisco DNA Center Second-Generation Appliance Installation Guide](#), refer to the following:
  - For more information about the Enterprise port, see the "Interface Cable Connections" topic.
  - For more information about Enterprise port configuration, see either the "Configure the Primary Node Using the Maglev Wizard" or "Configure the Primary Node Using the Expert Configuration Wizard" topic.
- You have assigned a super-admin user to carry out disaster recovery tasks. Only users with this privilege level can access this functionality.
- You have confirmed that the links connecting the following sites are one GB links with 200 ms RTT latency (at most):
  - Main and recovery sites
  - Main and witness sites
  - Recovery and witness sites
- You have generated a third-party certificate and installed this certificate on both the main and recovery sites. Otherwise, site registration will fail.



**Note** Cisco DNA Center copies this certificate to the witness site automatically during the registration process.

Ensure that all of the IP addresses and fully qualified domain names (**FQDN**) that these sites use are included in these certificates. For a description of how to generate third-party certificates, see [Generate a Certificate Request Using Open SSL](#) in the *Cisco DNA Center Security Best Practices Guide*.

### Main and Recovery Site Prerequisites

- Both your main and recovery site must consist of the same number of nodes. Cisco DNA Center will not allow you to register and activate a disaster recovery system that does not meet this requirement.
- Both your main and recovery site must consist of Cisco DNA Center appliances that have the same number of cores. This means that one site cannot consist of 56-core second-generation appliances while the other site consists of 112-core appliances. The following table lists the appliances that support disaster recovery and their corresponding Cisco part number:

|                                                                                                                                                            |                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Second-generation Cisco DNA Center appliance, which is based on either the Cisco UCS C220 M5 small form-factor (SFF) chassis or Cisco UCS C480 M5 chassis. | 56-core appliance: Cisco part number DN2-HW-APL-L               |
|                                                                                                                                                            | 56-core promotional appliance: Cisco part number DN2-HW-APL-L-U |
|                                                                                                                                                            | 112-core appliance: Cisco part number DN2-HW-APL-XL             |
|                                                                                                                                                            | 112-core promotional appliance: DN2-HW-APL-XL-U                 |

- You have configured and enabled high availability (HA) on both your main and recovery site. Otherwise, the registration of these sites will fail. For more information, see the latest [Cisco DNA Center High Availability guide](#).



**Note** This is applicable to seven-node setups only.

- If you want to use Border Gateway Protocol (BGP) to advertise your system's virtual IP address routes, you need to configure your system's Enterprise virtual IP address on each of the main and recovery site's neighbor routers. The configuration you need to enter will look similar to one the following examples:

#### Interior BGP (iBGP) Configuration Example

```
router bgp 64555
  bgp router-id 10.30.197.57
  neighbor 172.25.119.175 remote-as 64555
  neighbor 172.25.119.175 update-source 10.30.197.57
  neighbor 172.25.119.175 next-hop-self
```

where:

- 64555 is the neighbor router's local and remote AS number.
- 10.30.197.57 is the neighbor router's IP address.
- 172.25.119.175 is your system's Enterprise virtual IP address.

#### Exterior BGP (eBGP) Configuration Example

```
router bgp 62121
  bgp router-id 10.30.197.57
```

```
neighbor 172.25.119.175 remote-as 64555
neighbor 172.25.119.175 update-source 10.30.197.57
neighbor 172.25.119.175 next-hop-self
neighbor 172.25.119.175 ebgp-multihop 255
```

where:

- 62121 is the neighbor router's local AS number.
  - 64555 is the neighbor router's remote AS number.
  - 10.30.197.57 is the neighbor router's IP address.
  - 172.25.119.175 is your system's Enterprise virtual IP address.
- If you enable BGP route advertisement (as described in the previous bullet), we recommend that you filter routes towards Cisco DNA Center in order to improve its performance. To do so, enter the following configuration:

```
neighbor system's-Enterprise-virtual-IP-address route-map DENYALL out
!
ip prefix-list deny-all seq 5 deny 0.0.0.0/0 le 32
!
route-map DENYALL permit 10
match ip address prefix-list deny-all
```

#### Witness Site Prerequisites

- You have confirmed that the virtual machine that hosts your witness site is running (at a minimum) VMware ESXi hypervisor version 6.0 or later with a 2.1-GHz core and two virtual CPUs, 4 GB of RAM, and 10 GB of hard drive space.
- You have set up your witness site in a different location than your main and recovery sites and confirmed that it is reachable from both of these sites.
- You have configured an NTP server that is accessible by the witness site. You must synchronize this NTP server with the NTP servers that are used by the main and recovery sites.

## Configure Disaster Recovery After an Upgrade

To successfully configure disaster recovery after upgrading your system to the latest Cisco DNA Center 2.2.1.x version, complete the steps that are applicable to your situation:

### Scenario 1

In this scenario, the first Cisco DNA Center version installed on your appliances was a version previous to 2.1.x. Now you want to upgrade to the latest 2.2.1.x version from 2.1.x. Complete the following steps to ensure that disaster recovery functions properly after the upgrade:

**Step 1** On your appliances, upgrade from your current Cisco DNA Center version to the latest 2.2.1.x version (see the [Cisco DNA Center Upgrade Guide](#)).

**Step 2** Back up your data (see [Back Up Data Now, on page 116](#)).

Ensure that your backup file resides on a remote server, as the next step will completely erase the data on your appliances and virtual machine.

## Scenario 2

- Step 3** Install the latest Cisco DNA Center 2.2.1.x ISO image onto your appliances (see the "Reimage the Appliance" topic in the *Cisco DNA Center Second-Generation Appliance Installation Guide*).
- Step 4** Restore the data from your backup file (see [Restore Data from Backups](#), on page 118).
- Step 5** Proceed with the configuration of your disaster recovery system.
- 

## Scenario 2

In this scenario, the first Cisco DNA Center version installed on your appliances was an earlier 2.1.x version and now you want to upgrade to the latest 2.2.1.x version. Also, disaster recovery is enabled and operational on these appliances. Complete the following steps:

---

- Step 1** [Place Your System on Pause](#), on page 144.
- Step 2** Upgrade the appliances at your main and recovery sites to the latest 2.2.1.x version. In the *Cisco DNA Center Upgrade Guide*, see the "Upgrade to Cisco DNA Center 2.2.1.x" chapter.
- Step 3** [Replace the Current Witness Site](#), on page 135.
- Step 4** [Rejoin Your System](#), on page 146.
- 

## Scenario 3

In this scenario, the first Cisco DNA Center version installed on your appliances was an earlier 2.1.x version and now you want to upgrade to the latest 2.2.1.x version. Unlike Scenario 2, disaster recovery has not been configured on these appliances. Complete the following steps:

---

- Step 1** [Configure the Witness Site](#), on page 130.
- Step 2** [Configure Disaster Recovery](#), on page 131.
- 

## Add the Disaster Recovery Certificate

Cisco DNA Center supports the import and storage of an X.509 certificate and private key into Cisco DNA Center. The disaster recovery certificate is used for intracluster communications.

You must obtain a valid X.509 certificate that is issued by your internal CA and the certificate must correspond to a private key in your possession.



**Note** If you want your disaster recovery system to use the same certificate that Cisco DNA Center uses, you can skip this procedure. When you configure the certificate, make sure that you check the **Use system certificate for Disaster Recovery as well** check box (see [Update the Cisco DNA Center Server Certificate](#), on page 59).

---



---

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

**Step 2** In the **Add Certificate** area, 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 3** If you chose **PEM**, perform the following tasks:

- For the **Certificate** field, import the **PEM** file by dragging and dropping the file into the Drag and Drop area.

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

After the upload succeeds, the system certificate is validated.

- For the **Private Key** field, import the private key by dragging and dropping the file into the Drag and Drop area.

**Note** Private keys must have a valid private key format extension (.key). The maximum file size for the private key is 10 MB.

After the upload succeeds, the private key is validated.

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

**Step 4** If you chose **PKCS**, perform the following tasks:

- For the **Certificate** field, import the **PKCS** file by dragging and dropping the file into the Drag and Drop area.

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

After the upload succeeds, the system certificate is validated.

- For the **Certificate** field, enter the passphrase for the certificate in the Password field.

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

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

**Step 5** Click **Save**.

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

---

# Configure the Witness Site

Complete the following procedure to configure the virtual machine that will serve as the witness site for your disaster recovery system.

- 
- Step 1** Download the OVF package that's specific to the Cisco DNA Center version that the witness site is running:
- Open <https://software.cisco.com/download/home/286316341/type>.  
**Note** You need a Cisco.com account to access this URL. See the following page for a description of how to create an account: <https://www.cisco.com/c/en/us/about/help/registration-benefits-help.html>
  - In the **Select a Software Type** area, click the Cisco DNA Center software link.  
The **Software Download** page updates, listing the software that's available for the latest Cisco DNA Center release.
  - Do one of the following:
    - If the OVF package (\*.ova) you need is already listed, click its **Download** icon.
    - Enter the relevant version number in the **Search** field, click its link in the navigation pane, and then click the **Download** icon for that version's OVF package.
- Step 2** Copy this package to a local machine running VMware vSphere 6.0 or 6.5.
- Step 3** From the vSphere client, choose **File > Deploy OVF Template**.
- Step 4** Complete the **Deploy OVF Template** wizard:
- Do the following in the wizard's **Source** screen:
    - Click **Browse**.
    - Navigate to the witness site's OVF package (.ova).
    - Click **Open**.
    - In the **Deploy from a file or URL** field, verify that the package's path is displayed and then click **Next >**.  
The wizard's **OVF Template Details** screen opens.
  - Click **Next >**.
  - Do the following in the wizard's **Name and Location** screen:
    - In the **Name** field, enter the name you want to set for the package.
    - In the **Inventory Location** field, select the folder that you want the package to reside in.
    - Click **Next >**.The wizard's **Host/Cluster** screen opens.
  - Click the host or cluster on which you want to run the deployed template and then click **Next >**.  
The wizard's **Storage** screen opens.
  - Click the storage drive that the virtual machine files will reside on and then click **Next >**.

The wizard's **Disk Format** screen opens.

- f) Click the **Thick Provision** radio button and then click **Next >**.
- g) Do the following in the wizard's **Network Mapping** screen and then click **Next >**:
  1. Click the IP address that is listed in the **Destination Networks** column.
  2. In the resulting drop-down list, choose the network that the deployed template should use.

The wizard's **Ready to Complete** screen opens, displaying all of the settings that you have entered.

- h) Check the **Power on after deployment** check box and then click **Finish**.
- i) When the **Deployment Completed Successfully** dialog box appears, click **Close**.

### Step 5

Enter the network settings for your witness site:

- a) Open a console to the virtual machine you just created by doing one of the following:
  - Right-click the virtual machine from the vSphere Client list and choose **Open Console**.
  - Click the **Open Console** icon in the vSphere Client menu.

The **Witness User Configuration** window appears.

- b) Enter and confirm the desired password for the admin user (*maglev*), then press **N** to proceed.
- c) Enter the following settings, then press **N** to proceed:
  - Its IP address
  - The netmask associated with the virtual machine's IP address
  - The IP address of your default gateway
  - **(Optional)** The IP address of the preferred DNS server
- d) Enter one or more NTP server addresses or hostnames (separated by spaces), then press **S** to submit your settings and begin the configuration of the witness site.

At least one NTP address or hostname is required.

- e) Verify that configuration has completed by using SSH port 2222 to log in to the IP address you configured for the witness site.

---


## Configure Disaster Recovery

To configure your disaster recovery system for use, complete the tasks described in the following procedure.



**Note** When configuring your system, you have a couple of options:

- You can specify a virtual IP address that uses Border Gateway Protocol (BGP) route advertising.
  - You can choose to not configure a virtual IP address. If you choose this option, you must enable device controllability so that a site's virtual IP address can be reconfigured after a failover occurs.
-

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default.

**Step 2** Register your main site:

**Note** At any point before Step 2d, you can click **Reset** to clear all of the settings that you have entered. You will then need to repeat Step 2 and enter the correct settings before you register the main site.

a) Click the **Configure** tab.

The **Main Site** radio button should already be selected.

b) Enter the following information in the **Setting up this cluster** area:

- **Main Site VIP:** The virtual IP address that manages traffic between the active site's cluster nodes and your Enterprise network. Choose the Enterprise virtual IP address for the main site from the drop-down list.
- **Recovery Site VIP:** The Enterprise virtual IP address that manages traffic between the recovery site's cluster nodes and your Enterprise network.
- **Witness Site IP:** The IP address that manages traffic between the witness site's virtual machine and your Enterprise network.

**Important** Ensure that the addresses you enter are currently reachable. Otherwise, the registration of your system's sites will fail.

c) Enter the following information in the **Additional Protocols** area:

- **Routing Protocol:** Specify whether you want to use BGP to advertise your system's virtual IP address routes.
- **Border Gateway Protocol Type:** If you clicked the **Border Gateway Protocol (BGP)** radio button, specify whether your BGP peers will establish exterior (**Exterior BGP (eBGP)**) or interior (**Interior BGP (iBGP)**) sessions with one another.
- **Enterprise VIP for Disaster Recovery:** When configured, this floating virtual IP address automatically moves to and operates on the site that is currently acting as your network's active site. This address manages traffic between your disaster recovery system and your Enterprise network.

**Note** You must enter a value for this field if you selected the **Border Gateway Protocol (BGP)** option.

- **Main Site Router Settings:** If you selected the **Border Gateway Protocol (BGP)** option, enter the IP address of your main site's remote router, as well as its local and remote autonomous system (AS) numbers. Click the **Add (+)** icon if you want to configure additional remote routers.

**Note** When the **iBGP** option is selected, Cisco DNA Center will automatically set the local AS number to the value you enter as the remote AS number.

- **Recovery Site Router Settings:** If you selected the **Border Gateway Protocol (BGP)** option, enter the IP address of your recovery site's remote router, as well as its local and remote AS numbers. Click the **Add (+)** icon if you want to configure additional remote routers.

**Note** When the **iBGP** option is selected, Cisco DNA Center will automatically set the local AS number to the value you enter as the remote AS number.

- **(Optional) Management VIP for Disaster Recovery:** When configured, this floating virtual IP address automatically moves to and operates on the site that is currently acting as your network's active site. This address manages traffic between your disaster recovery system and your Management network.

**Note** If you configure a Management virtual IP address and selected the **Border Gateway Protocol (BGP)** option, you must enter the appropriate remote router information (like you did for the Enterprise virtual IP address).

- d) From the **Action** area, click **Register**.

The **Disaster Recovery Registration** dialog opens.

- e) Click **Continue**.

The token that your recovery and witness sites need to use in order to register with your main site is generated.

**Step 3** In the **Supplement** area, click **Copy Token**.

**Step 4** Register your recovery site:

**Note** At any point before Step 4d, you can click **Reset** to clear all of the settings that you have entered. You will then need to repeat Step 4 and enter the correct settings before you register the recovery site.

- a) From the **Supplement** area, right-click the **Recovery Site** link and open the resulting page in a new browser tab.  
b) If necessary, enter the appropriate username and password to log in to your recovery site.

The **Disaster Recovery** page's **Configure** tab opens, with the **Recovery Site** radio button already selected.

**Note** If the Enterprise VIP you configured in Step 2c is not reachable from a browser, update the URL that is provided by replacing the Enterprise VIP with your recovery site's Management VIP and open the resulting URL.

- c) Enter the following information:

- **Main Site VIP:** The virtual IP address that manages traffic between the active site's cluster nodes and your Enterprise network.
- **Recovery Site VIP:** The virtual IP address that manages traffic between the recovery site's cluster nodes and your Enterprise network. Choose the recovery site's Enterprise virtual IP address from the drop-down list.
- The registration token you generated in Step 2.
- The username and password configured for the your active site's super-admin user.

- d) From the **Action** area, click **Register**.

The **Disaster Recovery Registration** dialog opens.

- e) Click **Continue**.

The topology updates the status for the main and recovery sites after they have been connected.

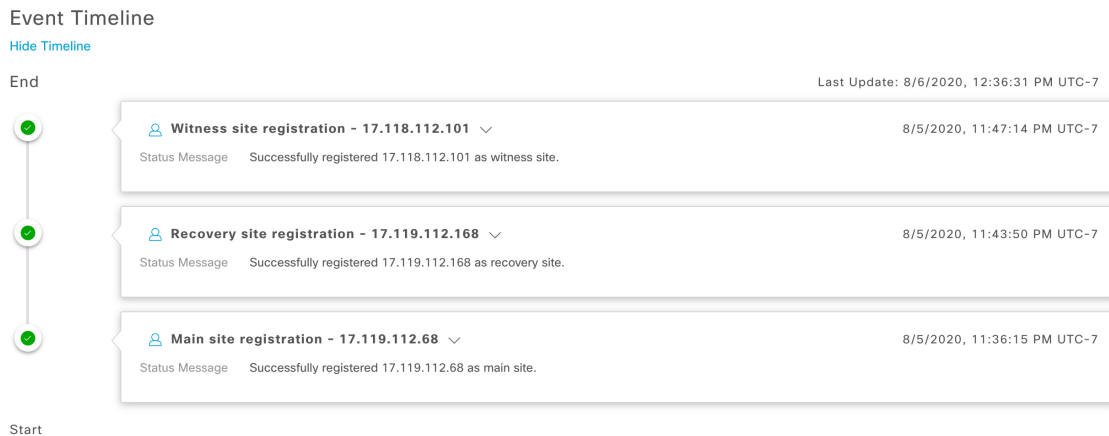
**Step 5** Register your witness site:

- a) Return to the main site's browser tab.  
b) From the **Supplement** area, click **Copy Witness Login Cmmd**.  
c) Open an SSH console to the witness site, paste the command you just copied, and then run it to log in.  
d) When prompted, enter the default (maglev) user's password.

- e) Return to the **Supplement** area and click **Copy Witness Register Cmmd**.
- f) In the SSH console, paste the command you just copied.
- g) Replace `<main_admin_user>` with the super-admin user's username and then run the command.
- h) When prompted, enter the super-admin user's password.

**Step 6** Verify that your main, recovery, and witness sites have been registered successfully:

- a) Return to the main site's browser tab and click **Monitoring** to view the Disaster Recovery **Monitoring** tab.
- b) In the **Logical Topology** area, confirm that the three sites are displayed and their status is **Registered**.
- c) In the **Event Timeline** area, confirm that the registration of each site is listed as an event and that each task completed successfully.



**Step 7** In the **Action** area, click **Activate**.

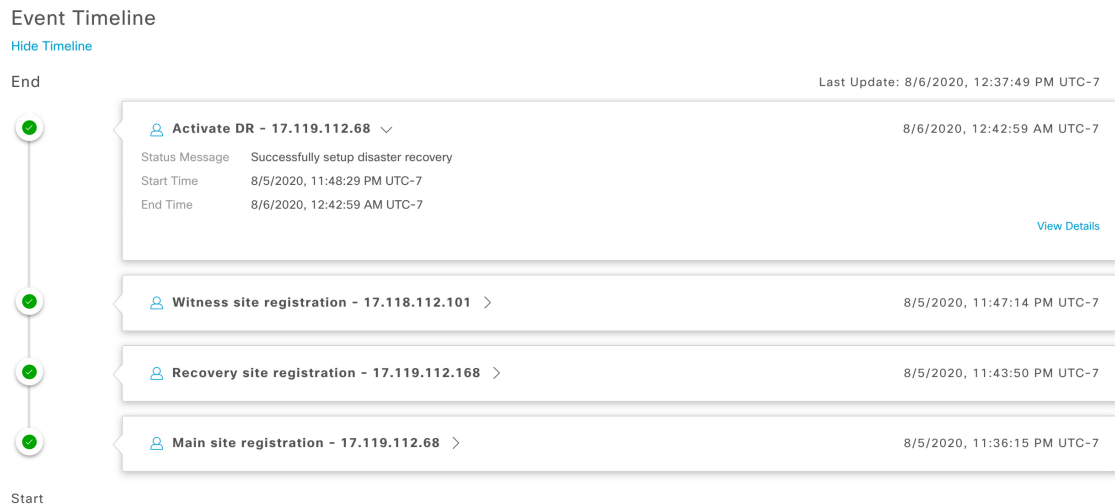
A dialog appears, indicating that all of the data that currently resides in your recovery site will be erased.

**Step 8** To begin the configuration of your disaster recovery system and the replication of your main site's data to the recovery site, click **Continue**.

**Note** The activation process may take some time to complete. View the Event Timeline in order to monitor its progress.

**Step 9** After Cisco DNA Center has completed the necessary tasks, verify that your system is operational:

- a. View its topology and confirm that the following status is displayed for your respective sites:
  - Main site: **Active**
  - Recovery site: **Standby**
  - Witness site: **Up**
- b. View the Event Timeline and confirm that the **Activate DR** task completed successfully.



- c. Verify that your sites are reachable by pinging them from the main site.

## Replace the Current Witness Site

Complete the following procedure if you need to upgrade or replace your current witness site.

- Step 1** Log in to the current witness site:
- Open an SSH console to the witness site and run the `ssh -p 2222 maglev@witness-site's-IP-address` command.
  - Enter the default (maglev) user's password.
- Step 2** Run the `witness reset` command.
- Step 3** Delete the current witness site's virtual machine.
- Step 4** Install the new witness site's virtual machine, as described in [Configure the Witness Site, on page 130](#).
- Step 5** Log in to the new witness site:
- Open an SSH console to the witness site and run the `ssh -p 2222 maglev@witness-site's-IP-address` command.
  - Enter the default (maglev) user's password.
- Step 6** Run the `witness reconnect` command.

## Deregister Your System

After your disaster recovery system has been activated, you may need to update the settings that you entered for a particular site. If you find yourself in this situation, complete the following procedure. Before you proceed, note that the settings that are currently set for all of the sites in your system will be cleared.

- Step 1** From the **Action** area, click **Pause DR** to suspend the operation of your system.

See [Place Your System on Pause, on page 144](#) for more information.


**Step 2** From the **Action** area, click **Deregister**.

Cisco DNA Center deletes all of the settings that you configured previously for your system's sites.

**Step 3** Complete the tasks described in [Configure Disaster Recovery, on page 131](#) in order to enter the appropriate settings for your sites, reregister them, and reactivate your system.



## Monitor the Event Timeline

From the Event Timeline, you can track the progress of disaster recovery tasks that are currently running and confirm when these tasks have completed. To view the timeline, do the following:

1. In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default.

2. Scroll to the bottom of the page.

Every task that is in progress or has completed for your system is listed here (in descending order based on their completion timestamp), starting with the most recent task. Cisco DNA Center indicates whether each task was initiated by the system () or a user ().

### Event Timeline

[Hide Timeline](#)

End

Last Update: 8/6/2020, 12:39:04 PM UTC-7



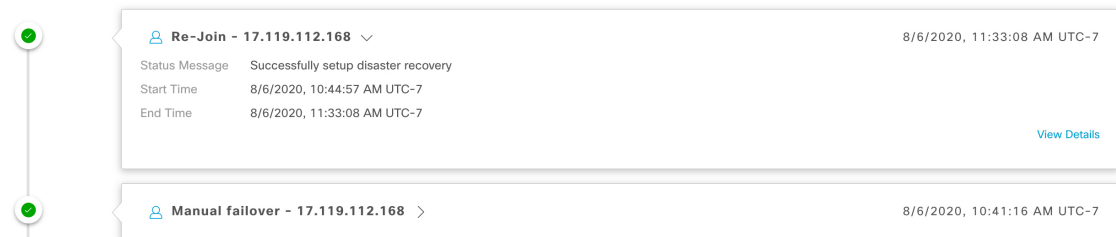
Say you want to monitor the restoration of your system after it was paused. Cisco DNA Center updates the Event Timeline as each task in the restoration process is started and then completed. To view a summary of what took place during a particular task, click >.

### Event Timeline

[Hide Timeline](#)

End

Last Update: 8/6/2020, 12:42:01 PM UTC-7





If the **View Details** link is displayed for a task, click it to view a listing of the relevant subtasks that were completed.

#### Event Timeline

[Hide Timeline](#)

End

Last Update: 8/6/2020, 12:42:39 PM UTC-7

The screenshot shows an event timeline for a 'Re-Join' task on host 17.119.112.168. The main task is 'Re-Join - 17.119.112.168' with a status message 'Successfully setup disaster recovery'. It has a start time of 8/6/2020, 10:44:57 AM UTC-7 and an end time of 8/6/2020, 11:33:08 AM UTC-7. Below it are two subtasks: 'Configure active - 17.119.112.68' (start: 8/6/2020, 10:50:12 AM UTC-7) and 'Configure standby - 17.119.112.168' (start: 8/6/2020, 11:33:05 AM UTC-7). A 'Manual failover' task is also visible at the bottom.

As with tasks, you can click > to view summary information for a particular subtask.

#### Event Timeline

[Hide Timeline](#)

End

Last Update: 8/6/2020, 12:43:53 PM UTC-7

This screenshot shows the 'Configure active' subtask expanded. The main task is 'Re-Join - 17.119.112.168' with a status message 'Successfully setup disaster recovery'. The expanded subtask is 'Configure active - 17.119.112.68' with a status message 'Successfully configured active system'. It has a start time of 8/6/2020, 10:45:06 AM UTC-7 and an end time of 8/6/2020, 10:50:12 AM UTC-7. Below it are five sub-subtasks: 'Starting bgp advertisement.', 'Configuring Global DR VIPs.', 'Configure standby to active services.', 'Add other cluster metadata.', and 'Save cluster metadata.', each with its own start and end times.

See [Troubleshoot Your Disaster Recovery System, on page 150](#) for a description of the issues you may encounter while monitoring the Event Timeline and how to remedy them.

## System and Site States

The following tables explain the various states you may see for your system in the Status area or your sites in the Topology.

Table 10: Disaster Recovery System States

| State                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Unconfigured</b>                     | Newly installed system. Disaster recovery has not been configured yet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Registered</b>                       | The active, standby, and witness sites have been registered and all registration validation checks have completed successfully. The three sites can communicate with one another.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Configuring</b>                      | This state can indicate any of the following situations: <ul style="list-style-type: none"> <li>• <b>Activate DR</b> was clicked in the <b>Action</b> area, which initiates a number of workflows in both the active and standby sites. If any of these workflows fail, this site reverts back to the <b>Registered</b> state.</li> <li>• The tasks that run prior to the configuration of your system's active and standby sites have completed successfully.</li> </ul>                                                                                        |
| <b>Up</b>                               | This state can indicate any of the following situations: <ul style="list-style-type: none"> <li>• Disaster recovery has been configured and system-triggered failover is available.</li> <li>• Disaster recovery has been configured. However, system-triggered failover is not available because either the witness site has not been configured or the witness site is down.</li> <li>• The standby system is unavailable and data replication is not taking place.</li> <li>• Either a system-triggered or manual failover completed successfully.</li> </ul> |
| <b>Up (with no Failover)</b>            | The system enters this state when either: <ul style="list-style-type: none"> <li>• The active and standby sites lose connectivity with the witness site.</li> <li>• The active and witness sites lose connectivity with the standby site.</li> </ul>                                                                                                                                                                                                                                                                                                             |
| <b>Down</b>                             | The disaster recovery system detected that the active site is down and initiated a failover, but the failover failed. When your system is in this state, resolve the issue and then initiate a manual failover.                                                                                                                                                                                                                                                                                                                                                  |
| <b>Failover in progress</b>             | After detecting that the active site is down, the disaster recovery system triggered a failover.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Deregistering</b>                    | Deregistration is in progress. After this process completes, all registration information and related network settings are reset.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Deregistered</b>                     | The main, recovery, and witness sites have been deregistered from your disaster recovery system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Pausing Disaster Recovery System</b> | The disaster recovery system is temporarily being paused for maintenance or other activities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Disaster Recovery System Paused</b>  | The disaster recovery system has been paused. The main and recovery sites are currently operating as two standalone clusters that are not replicating data between each other. To restart the system and resume data replication, click <b>Rejoin</b> .                                                                                                                                                                                                                                                                                                          |
| <b>Pausing Disaster Recovery Failed</b> | Errors occurred while pausing your disaster recovery system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| State                      | Description                                                                                                                                                                                                    |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User intervention required | Both the main and recovery sites went offline and then restarted. However, the disaster recovery system remains in a disconnected state. Pause and then restart your system to see if that resolves the issue. |

Table 11: Active Site States

| State                 | Description                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unconfigured          | Newly installed site. Disaster recovery information is not available yet.                                                                                                                                                                   |
| Registered            | This site was designated as the active site. Also, the validation checks and registration have completed successfully.                                                                                                                      |
| Configuring Active    | The workflows that run before a site is configured as the active site are in progress.                                                                                                                                                      |
| Active                | The workflows that run before a site is configured as either the active or standby site have completed successfully.                                                                                                                        |
| Failed to Configure   | Unable to complete the workflows that run before a site is configured as the active site.                                                                                                                                                   |
| Active                | This site was successfully configured as the active site.                                                                                                                                                                                   |
| Isolating             | Indicates that the isolation of this site from the disaster recovery system is in progress. This is triggered after you initiate a manual failover and the site that was previously acting as the active site comes back online.            |
| Isolated              | This site was successfully isolated from the disaster recovery system.                                                                                                                                                                      |
| Isolate Failed        | Unable to isolate this site from the disaster recovery system.                                                                                                                                                                              |
| Down                  | Either the automated health monitor recognizes that the witness system is down or the system has not provided a health update within the configured threshold time.                                                                         |
| Pausing Active        | The active site is temporarily being paused for maintenance or other activities.                                                                                                                                                            |
| Active Paused         | The active site has been paused. The active and standby sites are currently operating as two standalone clusters that are not replicating data between each other. To restart the system and resume data replication, click <b>Rejoin</b> . |
| Pausing Active Failed | Errors occurred while pausing your active site.                                                                                                                                                                                             |

Table 12: Standby Site States

| State               | Description                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------|
| Unconfigured        | Newly installed site. Disaster recovery information is not available yet.                           |
| Registered          | This site was designated as the standby site and the validation checks have completed successfully. |
| Configuring Standby | The workflows that run before a site is configured as the standby site are in progress.             |

| State                         | Description                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Standby</b>                | The workflows that run before a site is configured as the standby site have completed successfully.                                                                                                                                          |
| <b>Failed to Configure</b>    | Unable to complete the workflows that run before a site is configured as the standby site.                                                                                                                                                   |
| <b>Passive</b>                | This site was successfully configured as the standby site.                                                                                                                                                                                   |
| <b>Activating passive</b>     | Indicates that a system-triggered or manual failover is in progress, which will convert your standby site into the new active site.                                                                                                          |
| <b>Failover success</b>       | A system-triggered or manual failover completed successfully and the disaster recovery system is ready to operate.                                                                                                                           |
| <b>Failover failed</b>        | A system-triggered or manual failover did not complete successfully.                                                                                                                                                                         |
| <b>Standby ready</b>          | The site previously acting as the active site is ready to be configured as the new standby site.                                                                                                                                             |
| <b>Down</b>                   | Either the automated health monitor recognizes that the witness system is down or the system has not provided a health update within the configured threshold time.                                                                          |
| <b>Pausing Standby</b>        | The standby site is temporarily being paused for maintenance or other activities.                                                                                                                                                            |
| <b>Standby Paused</b>         | The standby site has been paused. The active and standby sites are currently operating as two standalone clusters that are not replicating data between each other. To restart the system and resume data replication, click <b>Rejoin</b> . |
| <b>Pausing Standby Failed</b> | Errors occurred while pausing your standby site.                                                                                                                                                                                             |

Table 13: Witness Site States

| State                                        | Description                                                                                                                                                             |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Unconfigured</b>                          | Newly installed site. Disaster recovery information is not available yet.                                                                                               |
| <b>Registered</b>                            | This site has been designated as the witness site and the validation checks have completed successfully.                                                                |
| <b>Up</b>                                    | Configuration of the witness site has completed successfully.                                                                                                           |
| <b>Down</b>                                  | Either the automated health monitor recognizes that the witness site is down or the witness site has not provided a health update within the configured threshold time. |
| <b>Up and Replicating</b>                    | The disaster recovery system is up and running. Replication is in progress.                                                                                             |
| <b>Up (Manual failover)</b>                  | The disaster recovery system is running without the quorum that the witness site provides. System-triggered failover is not currently available.                        |
| <b>Failover in progress</b>                  | Failover is in progress. After resolving any issues on the new standby site (if any), click <b>Rejoin</b> after failover completes.                                     |
| <b>Failover in progress (User initiated)</b> | A manually-initiated failover is in progress. The witness site is not currently reachable.                                                                              |

| State                             | Description                                                                                                                                                               |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Up (No failover)                  | The configuration and activation of the disaster recovery system have been completed. However, the witness site is not reachable, so failover is not currently available. |
| Down (User intervention required) | Failover did not complete successfully. The witness system is not reachable. Pause and then restart your system to see if that resolves the issue.                        |

## Failovers: An Overview

A failover takes place when your disaster recovery system's standby site takes over the responsibilities of the former active site and becomes the new active site. Cisco DNA Center supports two types of failover:

- **System-triggered:** Occurs when your system's active site experiences an issue that brings it offline (such as a hardware failure or network outage). When Cisco DNA Center recognizes that the active site has not been able to communicate with the rest of the Enterprise network (as well as the standby and witness sites) for seven minutes, it completes the tasks necessary for your standby site to assume its role so that network operations can continue without interruption.
- **Manual:** Occurs when a super-admin user instructs Cisco DNA Center to swap the roles that are currently held by your system's active and standby sites. You would typically do this before you update the Cisco DNA Center software that is installed on a site's appliances or perform routine site maintenance.

After either type of failover has taken place and the former active site has come back online, your disaster recovery system automatically moves the site to the **Standby Ready** state. To establish this site as the new standby site, click **Rejoin** in the **Action** area of the **Monitoring** tab.

## Initiate a Manual Failover

When you manually initiate a failover, you instruct Cisco DNA Center to swap the roles that are currently assigned to your disaster recovery system's main and recovery site. This is handy if you know that the current active site is experiencing issues and you want to proactively designate the standby site as the new active site. Complete the following procedure to initiate a manual failover.

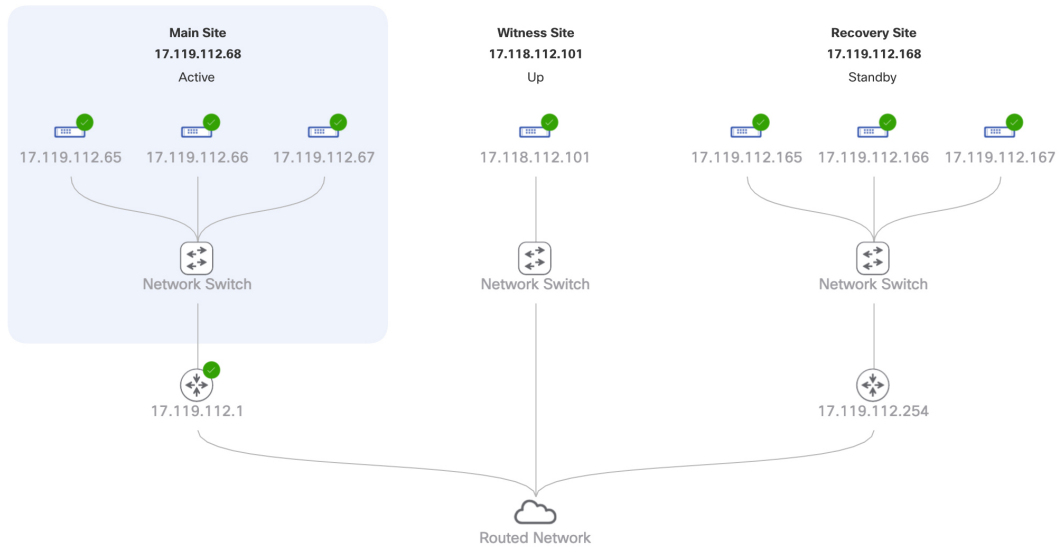


**Note** You cannot initiate a manual failover from your witness site. You can only do so from the current active site.

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology. In the following example, the user is logged in to the current active site.

## Logical Topology



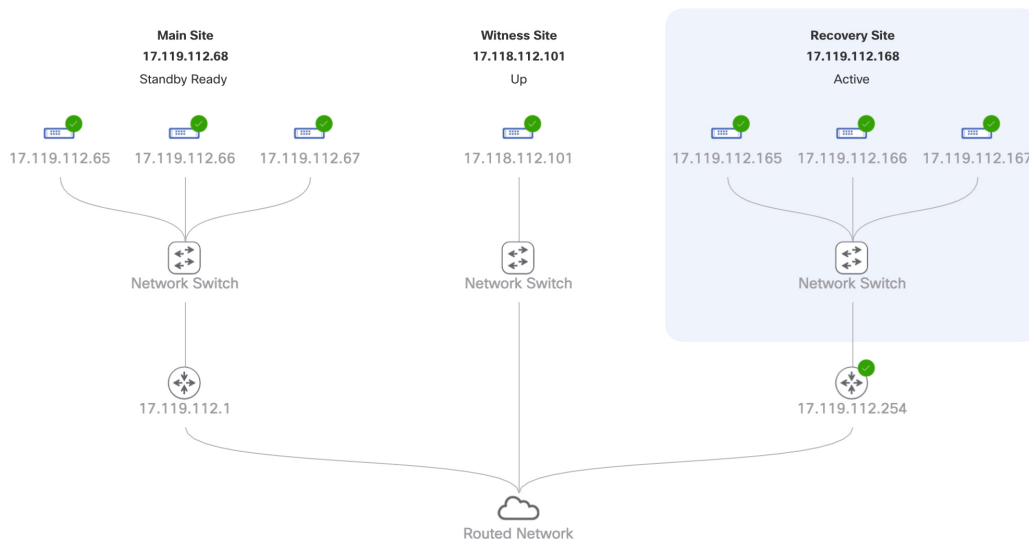
**Step 2** In the **Action** area, click **Manual Failover**.

The **Disaster Recovery Manual Failover** dialog opens, indicating that the standby site will assume the **Active** role.

**Step 3** Click **Continue** to proceed.

A message appears in the bottom right corner of the page, indicating that the failover process has started. The site previously acting as the active site is isolated from the system and enters the **Standby Ready** state.

## Logical Topology



At this point, the main and recovery sites are not connected and data replication is not taking place. If the former active site is experiencing issues, now is a good time to resolve those issues.

A subsequent failover (initiated by either the system or a user) cannot take place until you add the former active site back to your disaster recovery system.

**Step 4** Reconnect the main and recovery sites and reconfigure your disaster recovery system:

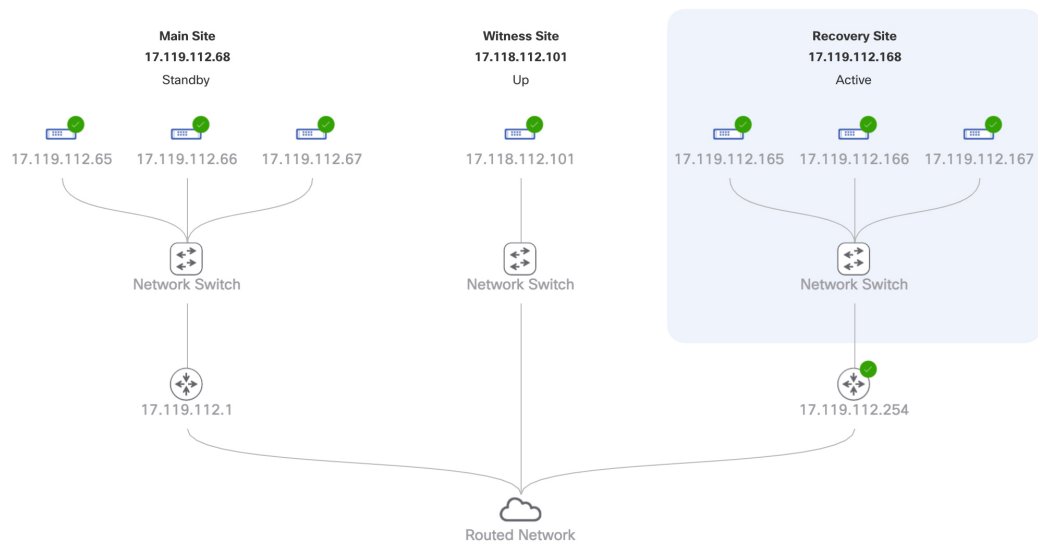
- a. Log in to your recovery site.
- b. In the **Action** area, click **Rejoin**.

A dialog opens, indicating that data on the standby site will be erased.

**Step 5** Click **Continue** to proceed and restart data replication.

After Cisco DNA Center completes the relevant workflows, the manual failover completes. The main site, which was currently serving as the active site, is now the standby site.

Logical Topology



**Step 6** Confirm that your disaster recovery system is operational again:

- a. In the top right corner of the **Monitoring** tab, verify that its status is listed as **Up and Running**.
- b. In the Event Timeline, verify that the **Rejoin** task completed successfully.

## Event Timeline

[Hide Timeline](#)

End

Last Update: 8/6/2020, 3:28:55 PM UTC-7

The event timeline displays three successful operations for IP address 17.119.112.168:

- Re-Join - 17.119.112.168** (8/6/2020, 3:27:11 PM UTC-7): Status Message: Successfully setup disaster recovery. Start Time: 8/6/2020, 1:14:04 PM UTC-7. End Time: 8/6/2020, 3:27:11 PM UTC-7.
- Configure active - 17.119.112.168** (8/6/2020, 1:21:34 PM UTC-7): Status Message: Successfully configured active system. Start Time: 8/6/2020, 1:14:09 PM UTC-7. End Time: 8/6/2020, 1:21:34 PM UTC-7.
- Configure standby - 17.119.112.68** (8/6/2020, 3:27:10 PM UTC-7): Status Message: Successfully configured standby system. Start Time: 8/6/2020, 1:14:05 PM UTC-7. End Time: 8/6/2020, 3:27:10 PM UTC-7.

## Pause Your Disaster Recovery System

By pausing your main and recovery sites, you are effectively breaking up your disaster recovery system. The sites will no longer be connected and instead will act as standalone clusters. You would want to pause your system to temporarily disable the replication of data from the active site to the standby site if you plan to break up your system for an extended period of time. You would also pause your system if you need to perform any administrative tasks, such as installing additional packages. By pausing your disaster recovery system, you can protect Cisco DNA Center from known network disruptions or disable disaster recovery without deleting your system's settings.

### Place Your System on Pause

To temporarily pause your disaster recovery system, which you would typically do before performing maintenance on a system component, complete the following procedure:

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (  $\equiv$ ) and choose **System > Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology.

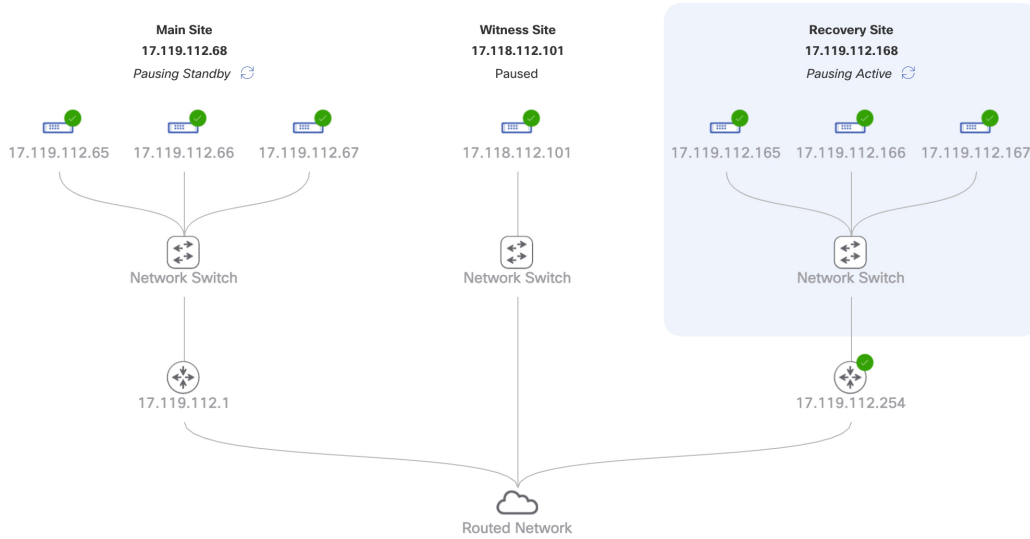
**Step 2** In the **Action** area, click **Pause DR**.

**Step 3** In the resulting dialog, click **Continue** to proceed.

A message appears in the bottom right corner of the page, indicating that the process to pause your system has started. To pause your system, Cisco DNA Center disables data and service replication. It also reinstates the services that were suspended on your recovery site. As this is taking place, the status for your main and recovery sites is set to **Pausing** in the topology.

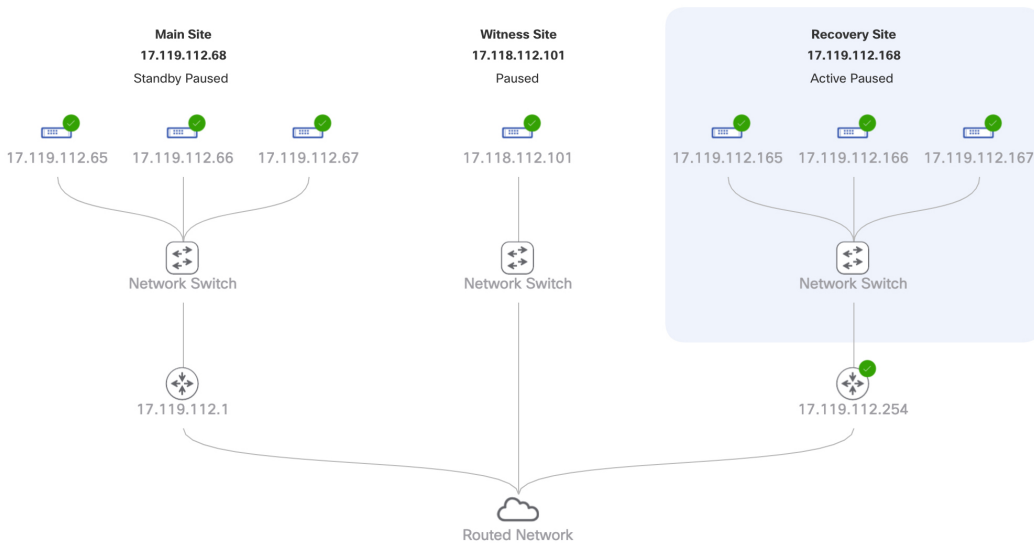


Logical Topology



After Cisco DNA Center completes the necessary tasks, the topology updates and sets the status for your main, recovery, and witness sites as **Paused**.

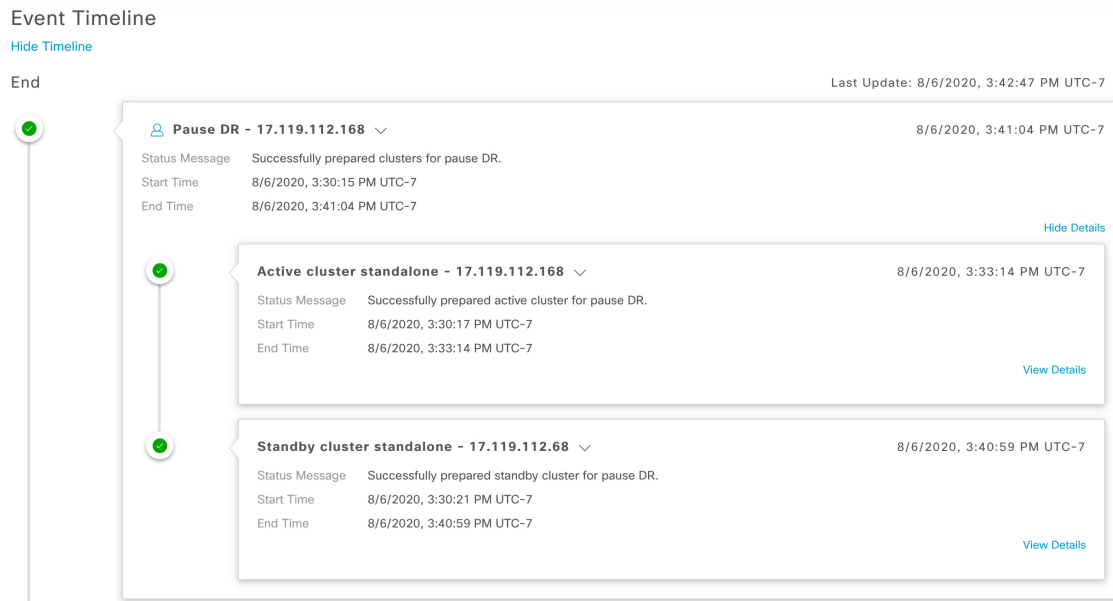
Logical Topology



**Step 4**


Confirm that your disaster recovery system has been paused:

- a. In the top right corner of the **Monitoring** tab, verify that its status is listed as **Disaster Recovery System Paused**.
- b. In the Event Timeline, verify that the **Pause DR** task completed successfully.



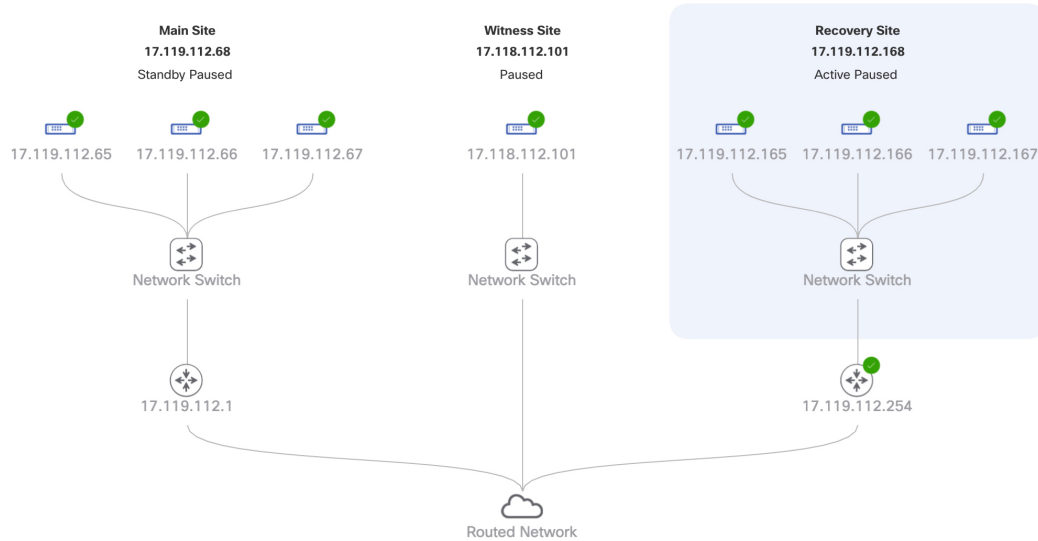
## Rejoin Your System

Complete the following procedure in order to restart a disaster recovery system that is currently on pause.

**Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology.

Logical Topology



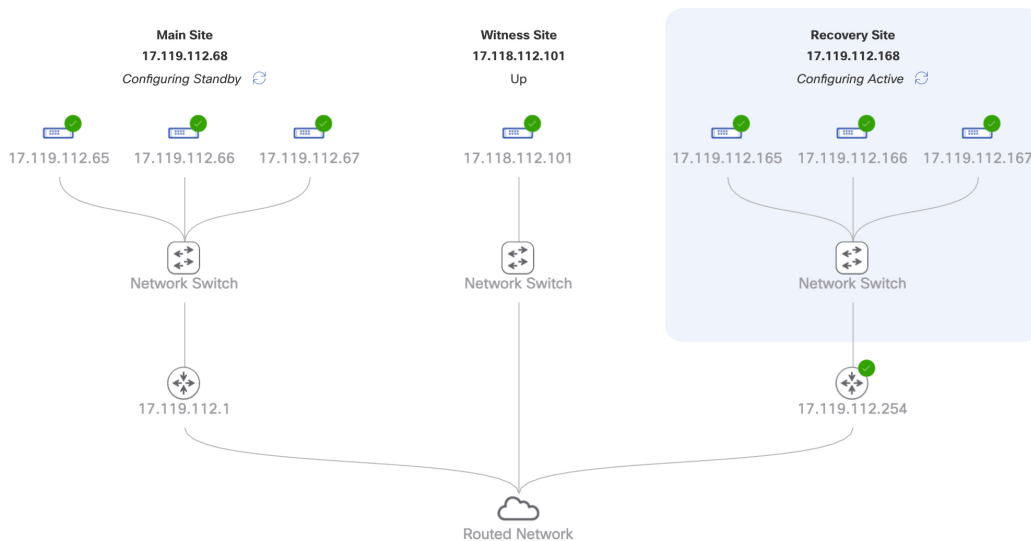
**Step 2** In the **Action** area, click **Rejoin**.

A dialog opens, indicating that all of the data on your standby site will be erased.

**Step 3** Click **Continue** to proceed.

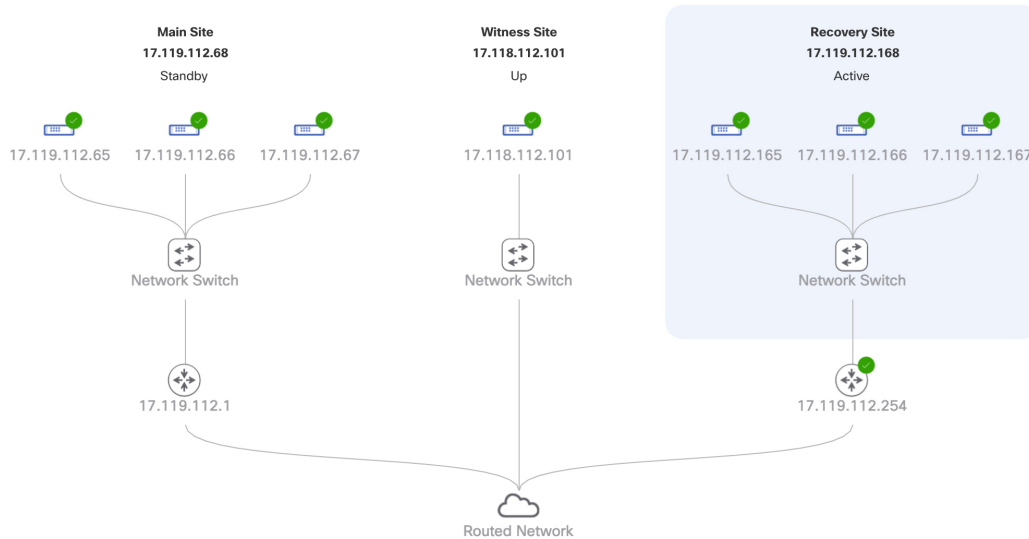
A message appears in the bottom right corner of the page, indicating that the process to reconnect your main, recovery, and witness sites has started. As this is taking place, the status for your main and recovery sites is set to **Configuring** in the topology.

Logical Topology



After Cisco DNA Center completes the necessary tasks, the topology updates the status for your main, recovery, and witness sites.

## Logical Topology



- Step 4** Confirm that your disaster recovery system is operational again by verifying that its status is listed as **Up and Running** in the top right corner of the **Monitoring** tab.

## Backup and Restore Considerations

Keep the following points in mind when backing up and restoring your disaster recovery system:

- A backup can only be scheduled from your system's active site.
- You cannot restore a backup file when disaster recovery is enabled. You must first pause your system temporarily. See [Place Your System on Pause, on page 144](#) for more information.
- You should only restore a backup file on the site that was the active site prior to pausing your system. After you restore the backup file, you then need to rejoin your system's sites. Doing so will reinstate disaster recovery and initiate the replication of the active site's data to the standby site. See [Rejoin Your System, on page 146](#) for more information.
- You can only restore a backup file on cluster nodes that have the same Cisco DNA Center version installed as the other nodes in your system.

For more information on backing up and restoring your disaster recovery system, see [Backup and Restore, on page 109](#).

## Disaster Recovery Event Notifications

You can configure Cisco DNA Center to send a notification whenever a disaster recovery event takes place. See the "Work with Events" topic in the [Cisco DNA Center Platform User Guide](#) for a description of how to configure and subscribe to these notifications. When completing this procedure, ensure that you select and

subscribe to the SYSTEM-DISASTER-RECOVERY event in the **Platform > Developer Toolkit > Events** table.

After you subscribe, Cisco DNA Center sends a notification indicating that the IPsec session is down because the system's certificate has expired. Do the following to update this certificate:

1. [Place Your System on Pause, on page 144.](#)
2. On both your main and recovery site, replace the current system certificate. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Settings > Trust & Privacy > Certificates > System**.
3. [Rejoin Your System, on page 146.](#)

## Supported Events

The following table lists the disaster recovery events that Cisco DNA Center generates notifications for when they take place.

| System Health Status | Event                                                                                                          | Notification                                     |
|----------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| OK                   | The disaster recovery system is operational.                                                                   | Activate DR (Disaster Recovery Setup Successful) |
| OK                   | Failover to either the main or recovery site has completed successfully.                                       | Failover Successful                              |
| Degraded             | Failover to either the main or recovery site has failed.                                                       | Failover Failed                                  |
| Degraded             | Automated failover is not available because the standby site is currently down.                                | Standby Cluster Down                             |
| Degraded             | Automated failover is not available because the witness site is currently down.                                | Witness Cluster Down                             |
| Degraded             | Unable to place the disaster recovery system on pause.                                                         | Pause Failure                                    |
| Degraded             | BGP route advertisement failed.                                                                                | BGP Failure                                      |
| Degraded             | The IPsec tunnel connecting your system's sites is operational.                                                | IPsec Up                                         |
| Degraded             | The IPsec tunnel connecting your system's sites is currently down.                                             | IPsec Down                                       |
| NotOk                | Disaster recovery system configuration failed.                                                                 | Activate DR Failure                              |
| NotOk                | The site that is currently in the <b>Standby Ready</b> state is unable to rejoin the disaster recovery system. | Activate DR Failure                              |

# Troubleshoot Your Disaster Recovery System

The following table describe the issues that your disaster recovery system may present and how to deal with them.

**Table 14: Disaster Recovery System Issues**

| Error Code | Message                                                                             | Solution                                                                                                                                                                                                                                                                                                                                               |
|------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SODR10007  | Token does not match.                                                               | The token provided during recovery site registration does not match the token generated during main site registration. From the main site's <b>Disaster Recovery &gt; Configuration</b> tab, click <b>Copy Token</b> to ensure that you copy the correct token.                                                                                        |
| SODR10048  | Packages ( <i>package names</i> ) are mandatory and not installed on the main site. | Install the listed packages before registering the system.                                                                                                                                                                                                                                                                                             |
| SODR10056  | Invalid credentials.                                                                | Confirm that you entered the correct credentials for the main site during recovery and witness site registration.                                                                                                                                                                                                                                      |
| SODR10062  | () site is trying to () with invalid IP address. Expected is (); actual is ().      | The main site IP address provided during recovery and witness site registration is different from the IP address that was provided during main site registration.                                                                                                                                                                                      |
| SODR10067  | Unable to connect to ( <i>recovery or witness site</i> ).                           | Verify that the main site is up.                                                                                                                                                                                                                                                                                                                       |
| SODR10072  | All the nodes are not up for ( <i>main or recovery site</i> ).                      | Check whether all three of the site's nodes are up.                                                                                                                                                                                                                                                                                                    |
| SODR10076  | High availability should be enabled on ( <i>main or recovery</i> ) site cluster.    | Enable high availability (HA): <ol style="list-style-type: none"> <li>1. Log in to the site you need to enable HA on.</li> <li>2. In the Cisco DNA Center GUI, click the <b>Menu</b> icon (☰) and choose <b>System &gt; Settings &gt; System Configuration &gt; High Availability</b>.</li> <li>3. Click <b>Activate High Availability</b>.</li> </ol> |

| Error Code | Message                                                                            | Solution                                                                                                                                                                                                      |
|------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SODR10100  | <i>(Main or recovery)</i> site has no third party certificate.                     | Replace the default certificate that Cisco DNA Center is currently using with a third-party certificate. See <a href="#">Update the Cisco DNA Center Server Certificate, on page 59</a> for more information. |
| SODR10118  | Appliance mismatch between main () and recovery ().                                | Different appliances are used by the main and recovery sites. To successfully register disaster recovery, both sites must use the same 56 or 112 core appliance.                                              |
| SODR10121  | Failed to advertise BGP.<br>Reason: ().                                            | See <a href="#">Troubleshoot BGP Route Advertisement Issues, on page 156</a> for more information.                                                                                                            |
| SODR10122  | Failed to stop BGP advertisement. Reason: ().                                      | See <a href="#">Troubleshoot BGP Route Advertisement Issues, on page 156</a> for more information.                                                                                                            |
| SODR10123  | Failed to establish secure connection between main () and () ().                   | No solution is available for this issue. Please contact Cisco TAC for support.                                                                                                                                |
| SODR10124  | Cannot ping VIP: <i>(main, recovery, or witness site's VIP or IP address)</i> .    | Do the following: <ul style="list-style-type: none"> <li>• Verify that the address specified is correct.</li> <li>• Check whether the address is reachable from the other addresses.</li> </ul>               |
| SODR10129  | Unable to reach main site. ()                                                      | Check whether the Enterprise virtual IP address configured for the main site is reachable from the recovery and witness sites.                                                                                |
| SODR10132  | Unable to check IP addresses are on the same interface.<br>Retry the operation. () | Retry the operation you just attempted.                                                                                                                                                                       |

| Error Code | Message                                                                                                                                                                                                                                   | Solution                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SODR10133  | The disaster recovery enterprise VIP () and the IP addresses () are not configured or reachable via the same interface. Check the gateway or static routes configuration.                                                                 | Communication between a disaster recovery system's sites relies on the Enterprise network. The main and recovery site's Enterprise virtual IP address, as well as the witness site's IP address, need to be reachable via the Enterprise interface.<br><br>This error indicates that the IP address/virtual IP address configured for one or multiple sites uses an interface other than the Enterprise interface for communication. |
| SODR10134  | The disaster recovery management VIP (VIP address) and the IPs (IP addresses) are configured/reachable via same interface. It should be configured/reachable via management interface. Check the gateway or static routes' configuration. | The disaster recovery system's Management virtual IP address needs to be configured on the Management interface. This error indicates that the virtual IP address is currently configured on an interface where the Management cluster's virtual IP address has not been configured.<br><br>Add a /32 static route to the Management virtual IP address that's configured on the Management interface.                               |
| SODR10136  | Certificates required to establish IPsec session not found.                                                                                                                                                                               | From the <b>System Certificate</b> page ( <b>System &gt; Settings &gt; Trust &amp; Privacy &gt; Certificates &gt; System</b> ), try uploading the third-party certificate again and then retry registration. If the problem persists, contact Cisco TAC for assistance.                                                                                                                                                              |
| SODR10138  | Self-signed certificate is not allowed. Upload a third-party certificate and retry.                                                                                                                                                       | —                                                                                                                                                                                                                                                                                                                                                                                                                                    |



| Error Code | Message                                                                                                                                                     | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SODR10139  | Disaster recovery requires first non-wildcard DNS name to be same in main and recovery. {} in {} site certificate is not same as {} in {} site certificate. | <p>The third-party certificate installed on your main and recovery sites has different DNS names specified for your disaster recovery system. Generate a third-party certificate that specifies a DNS name for your system and upload this certificate to both sites.</p> <p><b>Note</b> Ensure that the DNS name does <i>not</i> use a wildcard.</p>                                                                                            |
| SODR10140  | Disaster recovery requires at least one non-wildcard DNS name. No DNS name found in certificate.                                                            | <p>The third-party certificate installed on your main and recovery sites does not specify a DNS name for your disaster recovery system. Cisco DNA Center uses this name to configure the IPsec tunnel that connects your system's sites. Generate a third-party certificate that specifies a DNS name for your system and upload this certificate to both sites.</p> <p><b>Note</b> Ensure that the DNS name does <i>not</i> use a wildcard.</p> |
| —          | —                                                                                                                                                           | <p>When all three of your system's sites are not connected due to network partitioning or another condition, Cisco DNA Center sets the status of the sites to <b>Isolated</b>. Contact Cisco TAC for help with completing the appropriate recovery procedure.</p>                                                                                                                                                                                |

| Error Code | Message                                                                                                         | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —          | External postgres services does not exists to check service endpoints.                                          | <p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Log in to the site that the error occurred on.</li> <li>2. Run the following commands: <ul style="list-style-type: none"> <li>• <b>Kubectl get sep -A</b></li> <li>• <b>kubectl get svc -A   grep external</b></li> </ul> </li> <li>3. In the resulting output, search for <code>external-postgres</code>.</li> <li>4. If present, run the following command: <b>kubectl delete sep external-postgres -n fusion</b></li> <li>5. Retry the operation that failed previously.</li> </ol> |
| —          | Cannot ping VIP: (VIP address).                                                                                 | Verify that the Enterprise VIP address configured for your system is reachable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| —          | VIP drop-down list is empty.                                                                                    | Confirm that your system's VIP addresses and intracluster link are configured properly.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| —          | Cannot perform (disaster recovery operation) due to ongoing workflow: BACKUP. Please try again at a later time. | A disaster recovery operation was triggered while a scheduled backup was running. Retry the operation after the backup finishes.                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Error Code | Message                                                                              | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —          | The GUI indicates that the standby site is still down after it has come back online. | <p>If the standby site goes down and Cisco DNA Center's first attempt to isolate it from your disaster recovery system fails, it may not automatically initiate a second attempt. When this happens, the GUI will indicate that the site is down, even if it is operational again. In addition, you will not be able to restart your system as the standby site is stuck in maintenance mode.</p> <p>To restore the standby site, do the following:</p> <ol style="list-style-type: none"> <li>1. In an SSH client, log in to the standby site.</li> <li>2. Run the <b>maglev maintenance disable</b> command to take the site out of maintenance mode.</li> <li>3. Log in to Cisco DNA Center.</li> <li>4. In the GUI, click the <b>Menu</b> icon (☰) and choose <b>System &gt; Disaster Recovery</b>.<br/>The <b>Monitoring</b> tab is selected, by default.</li> <li>5. In the <b>Action</b> area, click <b>Rejoin</b> in order to restart your disaster recovery system.</li> </ol> |
| —          | Multiple services exists for MongoDB to check node-port label.                       | <p>For debugging, the MongoDB node port is exposed as a service. Run the following commands to identify this port and hide it:</p> <ul style="list-style-type: none"> <li>• <b>kubectl get svc --all-namespaces   grep mongodb</b></li> <li>• <b>magctl service unexpose mongodb &lt;port-number&gt;</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Error Code | Message                                                        | Solution                                                                                                                                                                                                                                                                                                                            |
|------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ---        | Multiple services exist for Postgres to check node-port label. | <p>For debugging, the Postgres node port is exposed as a service. Run the following commands to identify this port and hide it:</p> <ul style="list-style-type: none"> <li>• <code>kubectrl get svc --all-namespaces   grep postgres</code></li> <li>• <code>magctl service unexpose postgres &lt;port-number&gt;</code></li> </ul> |

## Troubleshoot BGP Route Advertisement Issues

If you receive a BGP route advertisement error, complete the following procedure in order to troubleshoot the cause.

### Step 1

From the Cisco DNA Center cluster, validate the BGP session's status:

- a) In the Event Timeline, confirm whether the **Starting BGP advertisement** task completed successfully (**Activate DR > View Details > Configure active**).

If the task failed, do the following before proceeding to Step 1b:

1. Check whether the neighbor router indicated in the error message is up.
2. Confirm whether the neighbor router has connectivity with Cisco DNA Center. If it doesn't, restore connectivity and then retry activating the new disaster recovery system or restarting an existing system that was paused.

- b) In the Cisco DNA Center GUI, view the disaster recovery system's Logical Topology and determine whether the neighbor router is currently active.

If it's down, check whether the Cisco DNA Center cluster is configured as a BGP neighbor from the router's perspective. If it's not, configure the cluster as a neighbor and then retry activating the new disaster recovery system or restarting an existing system that was paused.

- c) Check the status of the BGP session between Cisco DNA Center and its neighbor router by running the following command:

```
etcdctl get /maglev/config/network_advertisement/bgp/address1_address2 | jq
```

where:

- *address1* is the Cisco DNA Center cluster's virtual IP address.
- *address2* is the neighbor router's IP address.

If **Established** is listed in the **state** field, this indicates that the session is active and functioning properly.

- d) Run the following commands to view the bgpd and bgpmanager log files:

- `sudo vim /var/log/quagga/bgpd.log`

- **magctl service logs -rf bgpmanager | lql**

When viewing the log files, look for error messages. If you can't find any, this indicates that the BGP session is functioning properly.

- e) Check the status of the BGP session between Cisco DNA Center and its neighbor router by running the following command: **echo admin-password| sudo VTYSH\_PAGER=more -S -i vtysh -c 'show ip bgp summary'**

In the command output, look for the neighbor router's IP address. At the end of the same line, confirm that the router's connection state is listed as **0**. If this is the case, this indicates that the BGP session is active and functioning properly.

**Step 2**

From the neighbor router indicated in the error message, validate the BGP session's status:

- a) Run the **show ip bgp summary** command.
- b) In the command output, look for the Cisco DNA Center cluster's virtual IP address. At the end of the same line, confirm that the cluster's connection state is listed as **0**. If this is the case, this indicates that the BGP session is active and functioning properly.
- c) Run the **show ip route** command.
- d) View the command's output and confirm whether the disaster recovery system's Enterprise virtual IP address is being advertised.

For example, say your system's Enterprise virtual IP address is 10.30.50.101. If this is the first IP address that you see in the output, this confirms that it is being advertised.

---

