Cisco DNA Center Administrator Guide, Release 2.3.4

First Published: 2022-09-21

Last Modified: 2024-03-08

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

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 standards documentation, or language that is used by a referenced third-party product.

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)

© 2022–2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **New and Changed Information** 1

CHAPTER 2 **Configure System Settings** 3

About System Settings 4

User Profile Roles and Permissions 4

Use the System 360 4

View the Services in System 360 6

Monitor System Health 7

Establish Cisco IMC Connectivity 7

Delete Cisco IMC Settings 9

Subscribe to System Event Notifications 9

Event Notification Information 10

System Health Scale Numbers 16

View the System Topology 16

Troubleshoot Appliance and External System Issues 17

Troubleshoot External System Connectivity Issues 18

Use the Validation Tool 18

Use the System Analyzer Tool 23

System Topology Notifications 26

Disk Utilization Event Notifications 28

Suggested Actions 28

Cisco DNA Center and Cisco ISE Integration 32

Anonymize Data 34

Configure Authentication and Policy Servers 35

Configure Cisco AI Network Analytics 38

Client Certificate Renewal 40

Disable Cisco AI Network Analytics 40
Update the Machine Reasoning Knowledge Base 41
Cisco Accounts 42
Configure Cisco Credentials 42
Clear Cisco Credentials 42
Configure Connection Mode 43
Register Plug and Play 44
Create PnP Event Notifications 45
Configure Smart Account 45
Smart Licensing 46
Device Controllability 47
Configure Device Controllability 49
Accept the License Agreement 49
Configure SNMP Properties 49
Enable ICMP Ping 50
Configure an Image Distribution Server 50
Enable PnP Device Authorization 51
Configure Device Prompts 52
Create Custom Prompts 52
Configure Device Configuration Backup Settings 53
Configure an External Server for Archiving the Device Configuration 53
Cloud Access Keys 54
Integrity Verification 55
Upload the KGV File 55
Configure an IP Address Manager 57
Configure Webex Integration 58
Configure an MS Teams Integration 59
Configure ThousandEyes Integration 59
Configure Debugging Logs 59
Configure the Network Resync Interval 61
View Audit Logs 61
Export Audit Logs to Syslog Servers 62
View Tasks 63
Activate High Availability 63

Configure Integration Settings 64
Set Up a Login Message 64
Configure the Proxy 65
Security Recommendations 65
Change the Minimum TLS Version and Enable RC4-SHA (Not Secure) 66
Configure the Proxy Certificate 68
Upload an SSL Intercept Proxy Certificate 70
Certificate and Private Key Support 70
Certificate Chain Support 71
Update the Cisco DNA Center Server Certificate 72
Use an External SCEP Broker 74
Switch Back to an Internal PKI Certificate 75
Export the Cisco DNA Center PKI Certificate 75
Certificate Management 75
Manage Device Certificates 75
Configure the Device Certificate Lifetime 76
Change the Role of the PKI Certificate from Root to Subordinate 76
Provision a Rollover Subordinate CA Certificate 79
Configure the Device Certificate Trustpoint 80
Renew Certificates 80
Configure Trustpool 81
About Restricted Shell 82
About Product Usage Telemetry Collection 83
Configure vManage Properties 83
Account Lockout 84
Password Expiry 84
IP Access Control 85
Configure IP Access Control 85
Enable IP Access Control 85
Add an IP Address to the IP Access List 85
Delete an IP Address from the IP Access List 86
Disable IP Access Control 87

CHAPTER 3 **Manage Applications** 89

Application Management 89
Download and Install the Latest System Version 89
Download and Install a Previous System Version 90
Download and Install Application Updates 91
Package Download and Upgrade Event Notifications 91
Uninstall an Application 92

CHAPTER 4 Manage Users 93
About User Profiles 93
About User Roles 93
Create an Internal User 94
Edit a User 94
Delete a User 95
Reset a User Password 95
Change Your Own User Password 96
Change Your Own User Password Without Admin Permission 96
Reset a Forgotten Password 96
Configure Role-Based Access Control 97
Cisco DNA Center User Role Permissions 98
Display Role-Based Access Control Statistics 102
Configure External Authentication 103
Two-Factor Authentication 105
Prerequisites for Two-Factor Authentication 105
Two-Factor Authentication Workflow 106
Configure Two-Factor Authentication 106
Enable Two-Factor Authentication Using RADIUS 107
Enable Two-Factor Authentication Using TACACS+ 108
Log In Using Two-Factor Authentication 108
Display External Users 109

CHAPTER 5 Manage Licenses 111
License Manager Overview 111
Integration with Cisco Smart Accounts 115
Set Up License Manager 115

Visualize License Usage and Expiration 116
View Historical Trends for License Consumption 117
View License Details 118
Change License Level 119
Export License Information 120
Auto Registration of Smart License-Enabled Devices 120
Day 0 Configuration for Smart License-Enabled Devices 120
Apply Specific License Reservation or Permanent License Reservation to Devices 121
Enable SLR/PLR When the Devices and Cisco DNA Center Are Connected to CSSM 121
Enable SLR/PLR When the Devices and Cisco DNA Center Are Not Connected to CSSM 122
Generate the Authorization Code from CSSM 123
Cancel SLR or PLR Applied to Devices 123
Install the Authorization Code and Enable the High Security License 123
Disable High Security License 124
Upload Resource Utilization Details to CSSM 125
Change Device Throughput 126
Transfer Licenses Between Virtual Accounts 126
Manage Customer Tags to Smart License-Enabled Devices 126
Modify License Policy 127

CHAPTER 6 **Backup and Restore 129**
About Backup and Restore 129
Backup and Restore Event Notifications 130
Backup Server Requirements 131
Backup Server Directory Layout 133
Backup Storage Requirements 134
Example of NFS Server Configuration—Ubuntu 134
Example of NFS Server Configuration—CentOS 135
Configure Firewall Rules to Allow NFS 136
Configure Firewall Rules—Debian/Ubuntu 136
Configure Firewall Rules—RedHat/CentOS 137
Configure Backup Servers 137
Back Up Data Now 138
Schedule Data Backups 140

Restore Data from Backups 141

CHAPTER 7 **Implement Disaster Recovery** 143

Overview 143

Key Terms 143

Data Replication Overview 145

Navigate the Disaster Recovery GUI 146

View Disaster Recovery System Status 147

Prerequisites 148

Configure Disaster Recovery on an Upgraded Cisco DNA Center Appliance 152

Add the Disaster Recovery Certificate 152

Install the Witness Site 153

Configure Disaster Recovery 155

Replace the Current Witness Site 163

Deregister Your System 164

Monitor the Event Timeline 164

System and Site States 166

Upgrade a Disaster Recovery System 170

Failovers: An Overview 170

Initiate a Manual Failover 171

Pause Your Disaster Recovery System 174

Place Your System on Pause 174

Rejoin Your System 176

Disaster Recovery System Considerations 178

Backup and Restore Considerations 178

Node or Cluster Replacement Considerations 179

Reconfiguration Considerations 179

HA Considerations 179

Site Failure Considerations 180

Certificate Replacement Considerations 180

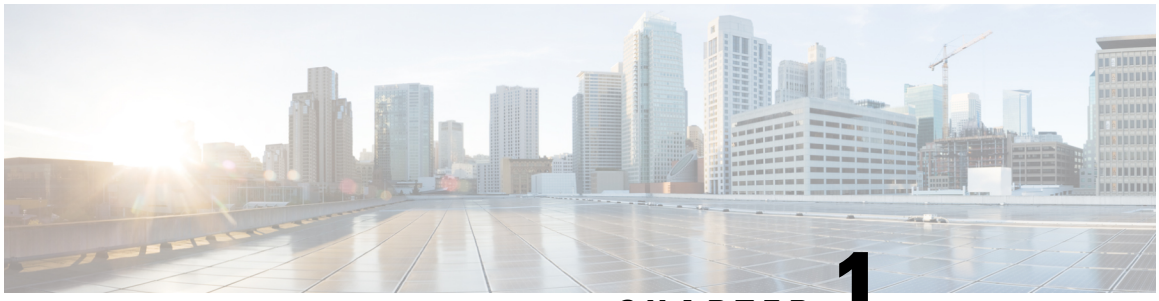
Disaster Recovery Event Notifications 180

Supported Events 180

Troubleshoot Your Disaster Recovery System 182

Two-Site Failure Scenarios 186

Troubleshoot BGP Route Advertisement Issues 190



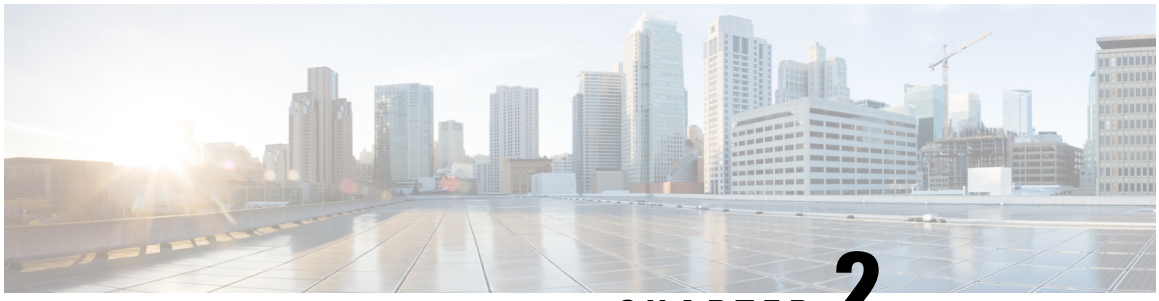
CHAPTER 1

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 2.3.4

Feature	Description
Restricted Shell	For added security, access to the root shell is disabled starting in this release of Cisco DNA Center. With restricted shell, users can't access the underlying operating system and file system, which reduces operational risk. Restricted shell is enabled for security purposes. However, if you want to access the root shell temporarily, you must contact the Cisco TAC for assistance. See About Restricted Shell, on page 82.
Configure an MS Teams Integration	You can now configure integration with Microsoft Teams. Once the integration is enabled, Cisco DNA Center provides call quality metrics information for Application 360 and Client 360 dashboards. See Configure an MS Teams Integration, on page 59.
Device Certificate	The **Device Certificate** window now contains a **Device Name** column, which lets you filter certificates by device name. See Manage Device Certificates, on page 75.



CHAPTER 2

Configure System Settings

- About System Settings, on page 4
- User Profile Roles and Permissions, on page 4
- Use the System 360, on page 4
- View the Services in System 360, on page 6
- Monitor System Health, on page 7
- Cisco DNA Center and Cisco ISE Integration, on page 32
- Anonymize Data, on page 34
- Configure Authentication and Policy Servers, on page 35
- Configure Cisco AI Network Analytics, on page 38
- Update the Machine Reasoning Knowledge Base, on page 41
- Cisco Accounts, on page 42
- Device Controllability, on page 47
- Configure SNMP Properties, on page 49
- Enable ICMP Ping, on page 50
- Configure an Image Distribution Server, on page 50
- Enable PnP Device Authorization, on page 51
- Configure Device Prompts, on page 52
- Configure Device Configuration Backup Settings, on page 53
- Configure an External Server for Archiving the Device Configuration, on page 53
- Cloud Access Keys, on page 54
- Integrity Verification, on page 55
- Configure an IP Address Manager, on page 57
- Configure Webex Integration, on page 58
- Configure an MS Teams Integration, on page 59
- Configure ThousandEyes Integration, on page 59
- Configure Debugging Logs, on page 59
- Configure the Network Resync Interval, on page 61
- View Audit Logs, on page 61
- View Tasks, on page 63
- Activate High Availability, on page 63
- Configure Integration Settings, on page 64
- Set Up a Login Message, on page 64
- Configure the Proxy, on page 65

- Security Recommendations, on page 65
- About Product Usage Telemetry Collection, on page 83
- Configure vManage Properties, on page 83
- Account Lockout, on page 84
- Password Expiry, on page 84
- IP Access Control, on page 85

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.
- Any changes to the IP address, static route, DNS server, or **maglev** user password must be done from the CLI with the `sudo maglev-config update` command.

User Profile Roles and Permissions

Cisco DNA Center supports role-based access control (RBAC). The roles assigned to a user profile define the capabilities that a user has permission to perform. Cisco DNA Center has three main default user roles:

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

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

If you're unable to perform an action in Cisco DNA Center, the reason might be that your user profile is assigned a role that doesn't permit it. For more information, check with your system administrator or see Configure Role-Based Access Control, on page 97.

Use the System 360

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

Step 1 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.

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 Click the menu icon (☰) and choose **System** > **System 360**.

Step 2 In the **System 360** tab, under 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 your cursor 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 must 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.

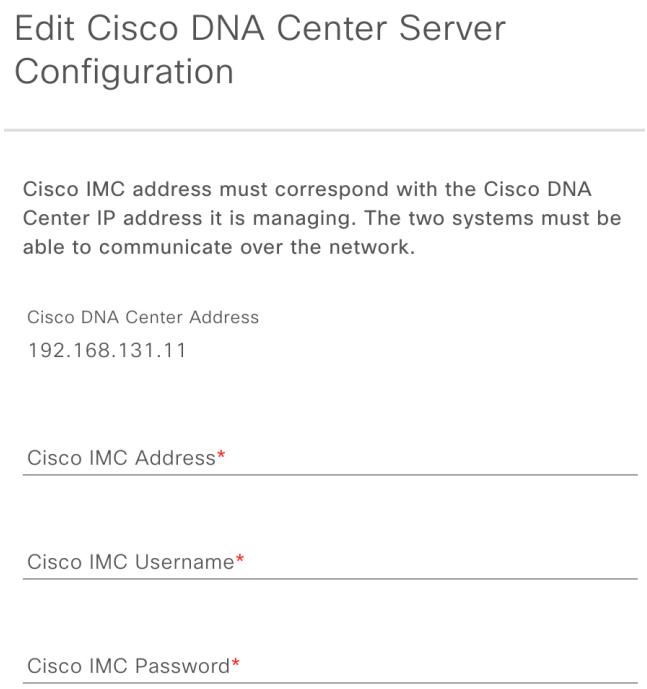
Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **System Configuration** > **System Health**.

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 Click the menu icon ( ) and choose **System** > **Settings** > **System Configuration** > **System Health**.

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

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

Subscribe to System Event Notifications

Information about 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. The rules engine then processes these raw events and converts them into system event notifications that are displayed in the System Health topology. By completing the procedure described in the "Work with Event Notifications" topic of the Cisco DNA Center Platform User Guide, you can also receive these notifications in one of the available formats. When completing this procedure, select and subscribe to the following events:

- Certificate expiration events:
  - SYSTEM-CERTIFICATE
  - SYSTEM-NODE-CERTIFICATE
- Connected external systems events:
  - SYSTEM-EXTERNAL-CMX
  - SYSTEM-EXTERNAL-IPAM
  - SYSTEM-EXTERNAL-ISE-AAA-TRUST
  - SYSTEM-EXTERNAL-ISE-PAN-ERS
  - SYSTEM-EXTERNAL-ISE-PXGRID
  - SYSTEM-EXTERNAL-ITSM
- Disaster recovery system events: SYSTEM-DISASTER-RECOVERY
- General system events:

- SYSTEM-CIMC
- SYSTEM-CONFIGURATION
- SYSTEM-HARDWARE
- SYSTEM-MANAGED-SERVICES

Note For managed services, the probe interval (the time it takes for Cisco DNA Center to delete stale events from its database) is 60 minutes. When managed services have been down and become active again, it takes this long for the System Health GUI to reflect that the services have been restored.

- SYSTEM-SCALE-LIMITS

Event Notification Information

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

Subdomain	Tag	Instance	State	Message
Domain: System				
CPU	CPU	<*node-hostname*>:CPU-1	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*>

Subdomain	Tag	Instance	State	Message
RAID Controller	RAIDController	<*node-hostname*>:Controller-1	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*>:nic-1	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*>:psu-1	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*>

Subdomain	Tag	Instance	State	Message
Disaster Recovery	DisasterRecovery	<*disaster-recovery-hostname*>	Ok	• Disaster recovery cluster is up • Disaster recovery failover succeeded to <*site-name*>
			Degraded	• Disaster recovery failover triggered from <*site-name*> to *site-name* • Disaster recovery failed while failing over to <*site-name*> • Disaster recovery standby cluster on <*site-name*> is down; cannot failover • Disaster recovery witness is down; cannot failover • Disaster recovery replication halted; recovery point objective will be impacted • Disaster recovery pause failed • Disaster recovery route advertisement failed • Disaster recovery IPSec communication failed
			NotOk	• Disaster recovery configuration failed • Disaster recovery failed to rejoin the standby system
Platform Services	ManagedServices	<hostname>:<name>	OK	Managed Service <*service-name*> is Running
			NOTOK	Managed Service <*service-name*> is Interrupted

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

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

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

Subdomain	Tag	Instance	State	Message
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*>.

System Health Scale Numbers

The following versions of the second-generation Cisco DNA Center appliance are available:

- 44-core appliance: Cisco part number DN2-HW-APL
- 44-core promotional appliance: Cisco part number DN2-HW-APL-U
- 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: Cisco part number DN2-HW-APL-XL-U

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

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

Note

- 1,000,000 notifications are maintained in the audit log for every appliance (regardless of type) and are stored for one year.
- To view the current appliance scale numbers, see the *Cisco DNA Center Data Sheet*.
- System Health isn't supported on Cisco DNA Center clusters consisting of three 44-core appliances.

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. 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 7
- Subscribe to System Event Notifications, on page 9

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.
- Whenever a connected appliance or external system has a certificate installed that is set to expire, the topology does the following:
  - If a certificate is set to expire within 90 days, the topology displays a warning.
  - If a certificate is set to expire within 30 days, the topology displays an error to bring your attention to the issue.
- System Health runs a hardware compliance check regularly and indicates whenever a connected appliance or external system does not meet the minimum configuration requirements. For example, System Health updates the topology to indicate when the **Write Through** cache write policy is not set for a connected virtual drive.
- If disaster recovery is operational in your production environment, System Health now provides hardware information for the appliances at both the main and recovery site. Previously, hardware information was provided only for main site appliances.

Troubleshoot Appliance and External System Issues

When viewing the System Health topology, the minor issue icon (⚠) and major issue icon (⛔) indicate network components that require attention. To begin troubleshooting the issue that a component is experiencing, place your cursor over its topology icon to open a pop-up window that displays 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 completes this procedure. To access this parameter in the **Create a User Role** wizard, expand the **System** row in the **Define the Access** page. For more information, see "Configure Role-Based Access Control" in the *Cisco DNA Center Administrator Guide*.

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

The window lists all the devices that 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.

Use the Validation Tool

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

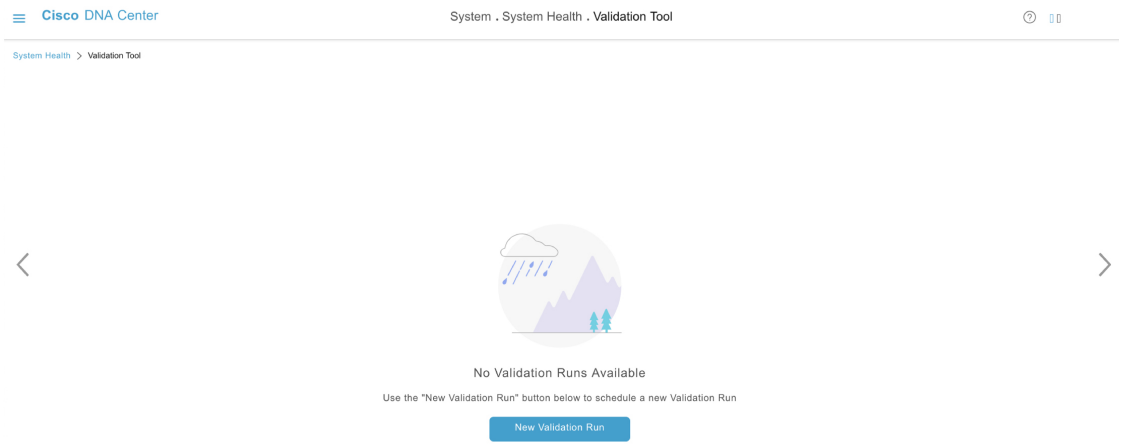
- The ability to connect to ciscoconnectdna.com (to download system and package updates).
- The presence of expiring certificates.
- The current health of appliance hardware and back-end services.
- The network components that have exceeded a scale number threshold.

To access the validation tool, do the following:

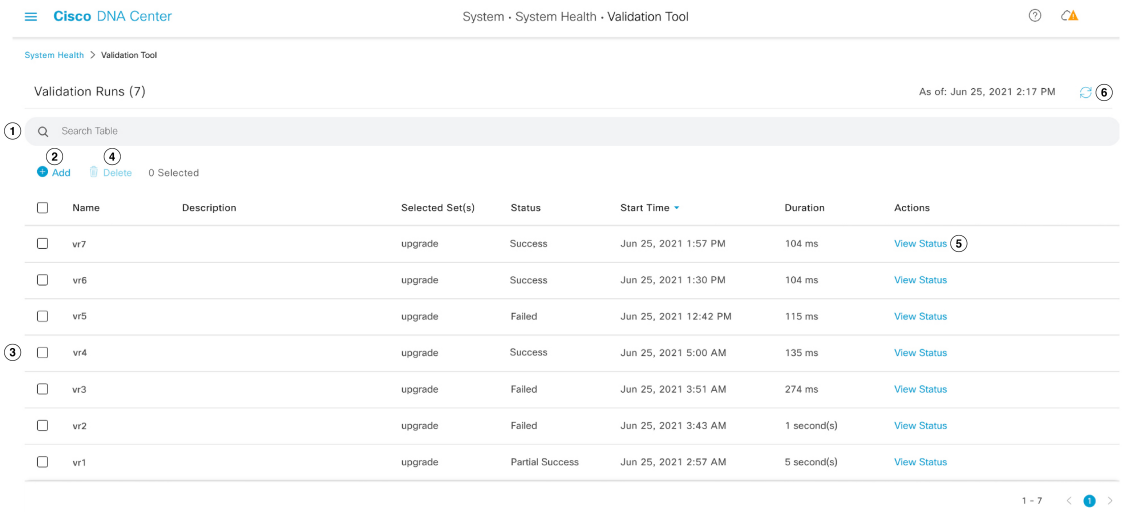
1. Click the menu icon ( ) and choose **System** > **System Health** to open the **System Health** page.
2. From the **Tools** drop-down menu, choose **Validation Tool**.

Navigate the Validation Tool Page

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



If Cisco DNA Center has validation run information, the page looks like this:



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

Callout	Description
1	**Search Table** field: Enter a search string to filter the validation runs that are listed on this page.
2	**Add** button: Click to open the **New Validation Run** slide-in pane and enter the required settings for a new run. For more information, see Start a Validation Run, on page 20.
3	**Validation Runs** table: Lists the validation runs that completed previously. For each run, the table provides information such as its name, applicable validation set, and completion status. Note the following points: • By default, the runs are ordered by start time, with the most recent run listed first. • A duration of zero is listed for any run that's currently in progress.
4	**Delete** button: With the check box for a validation run checked, click to delete the run. Then click **Ok** in the **Warning** dialog box to confirm deletion. **Note** You cannot delete a run that is in progress.
5	**View Status** link: Click to view the details for a particular run. For more information, see View Validation Run Details, on page 21.
6	**Refresh** button: Click to refresh the information that is displayed on this page.

Start a Validation Run

To start a validation run, complete the following steps.

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

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

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

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

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

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

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

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

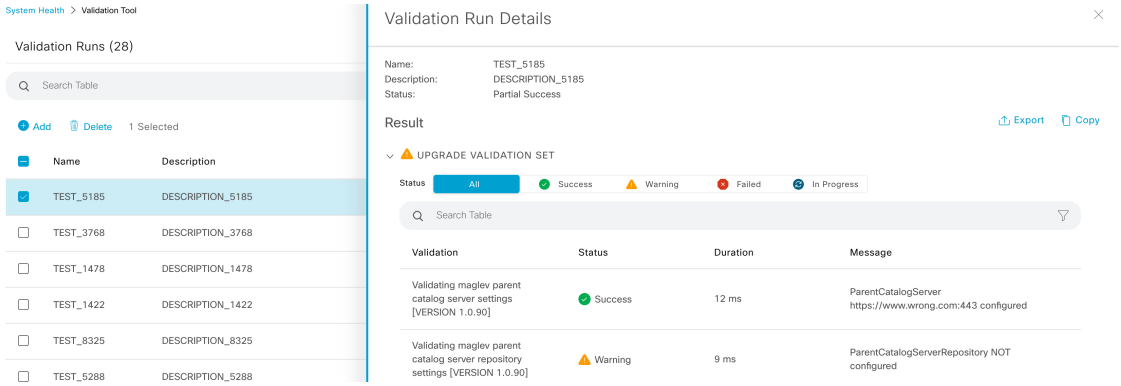
Step 4 In the **Validation Set(s) Selection** area, check the check box for the validation sets you want to run.

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

Step 5 Click **Run**.

View Validation Run Details

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



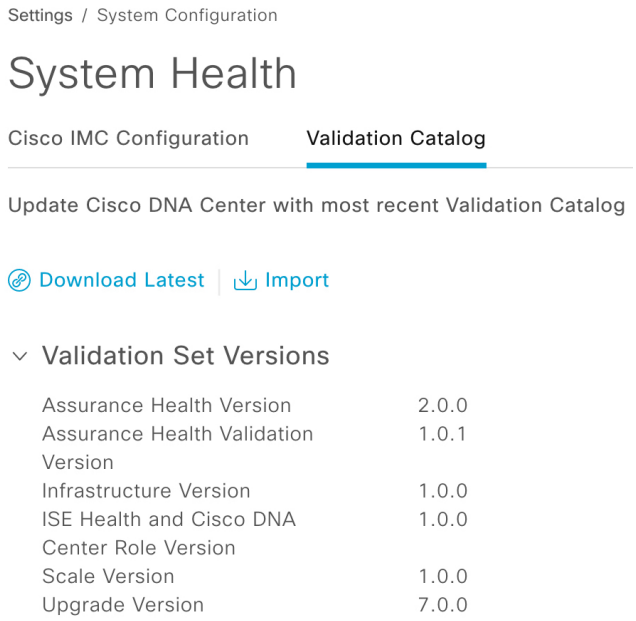
From here, you can also do the following:

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

Update the Validation Set

Validation sets should be updated whenever you upgrade Cisco DNA Center. In case you need to update validation sets manually, do the following:

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **System Configuration** > **System Health**.

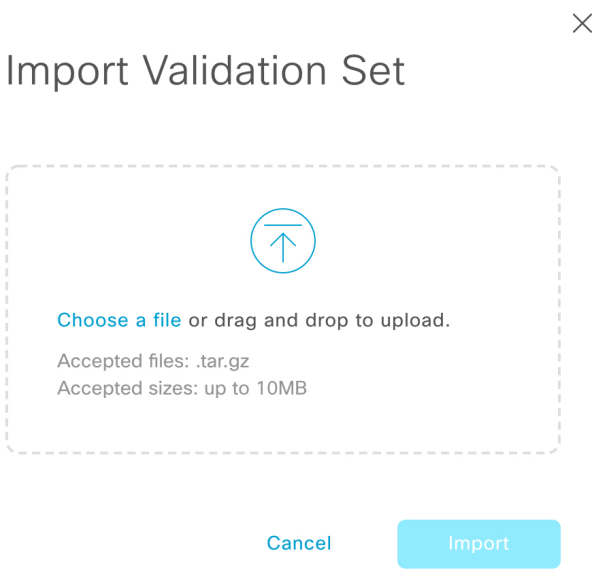


Step 2 Click the **Validation Catalog** tab.

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

Step 4 Import the validation set to Cisco DNA Center:

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



b) Do one of the following:

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

c) Click **Import**.

Use the System Analyzer Tool

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

1. Click the menu icon (☰) and choose **System** > **System Health**.

   The **System Health** window opens.

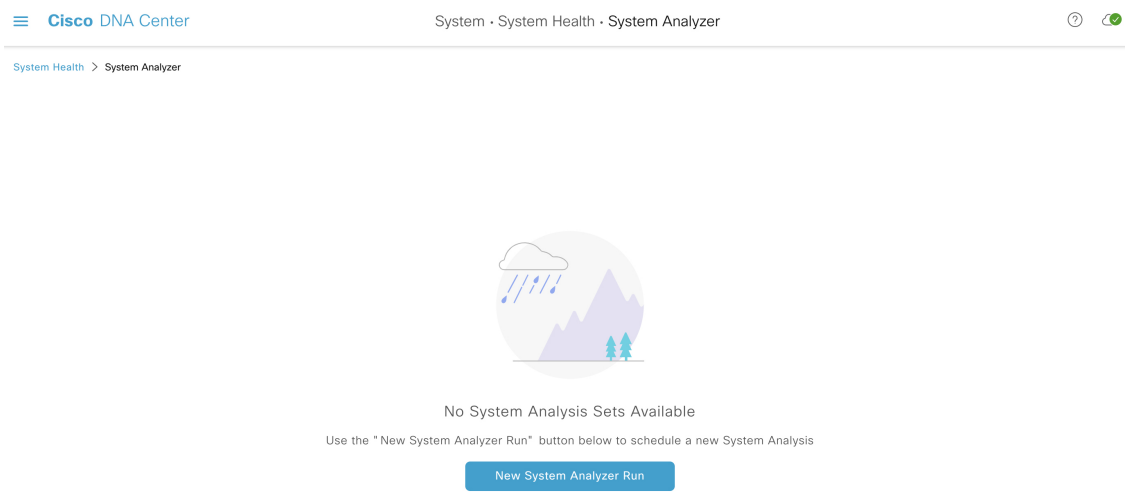
2. From the **Tools** drop-down list, choose **System Analyzer**.

Before you use this tool, note the following points:

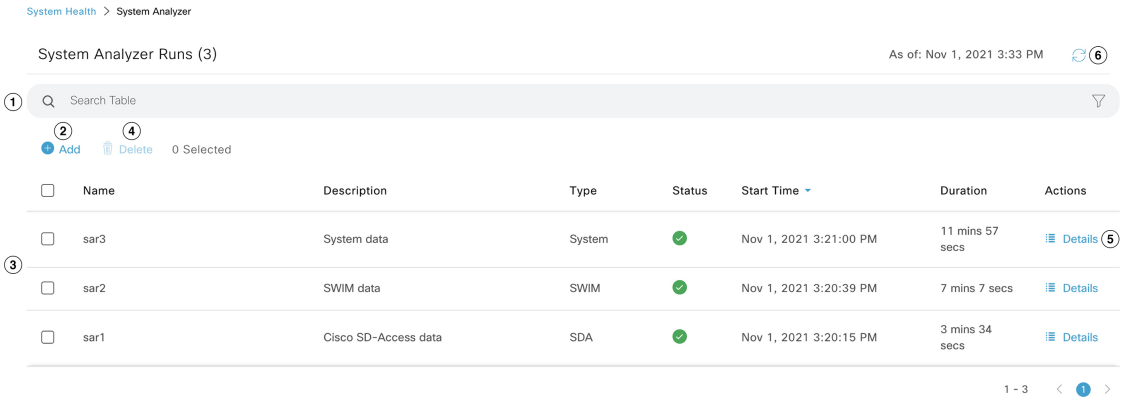
- Only admin users can start system analysis runs, download the resulting log files, and delete completed runs. All users can open and view the **System Analysis Details** slide-in pane for a selected run.
- The System Analyzer tool requires 5 GB of disk space on Cisco DNA Center's GlusterFS filesystem.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

Navigate the System Analyzer Page

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



If Cisco DNA Center has run information, the page looks like this:



The following table describes the components that make up the **System Analyzer** page and their function when run information is available.

Callout	Description
1	**Search Table** field: Enter a search string to filter the runs that are listed on this page.
2	**Add** button: Click to open the **New System Analyzer Run** slide-in pane and enter the required settings for a run. See Start a System Analyzer Run, on page 25 for more information.
3	**System Analyzer Runs** table: Lists the runs that are currently in progress or have completed previously. For each run, the table provides information such as its name, the relevant Cisco DNA Center component, and the amount of time it took to complete the run. Note the following points: • By default, the runs are ordered by start time, with the most recent run listed first. • A duration of zero is listed for any run that's currently in-progress.
4	**Delete** button: With the check box for a run checked, click **Delete** to remove it. **Note** You cannot delete a run that is in progress.

Callout	Description
5	**Details** link: Click to view the details for a particular run. For more information, see View System Analyzer Run Details, on page 25.
6	**Refresh** button: Click to refresh the information that's displayed on this page.

Start a System Analyzer Run

Complete the following procedure to start a System Analyzer run.

Step 1 Do one of the following in the **System Analyzer** page, depending on whether the **System Analyzer Runs** table is displayed:

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

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

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

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

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

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

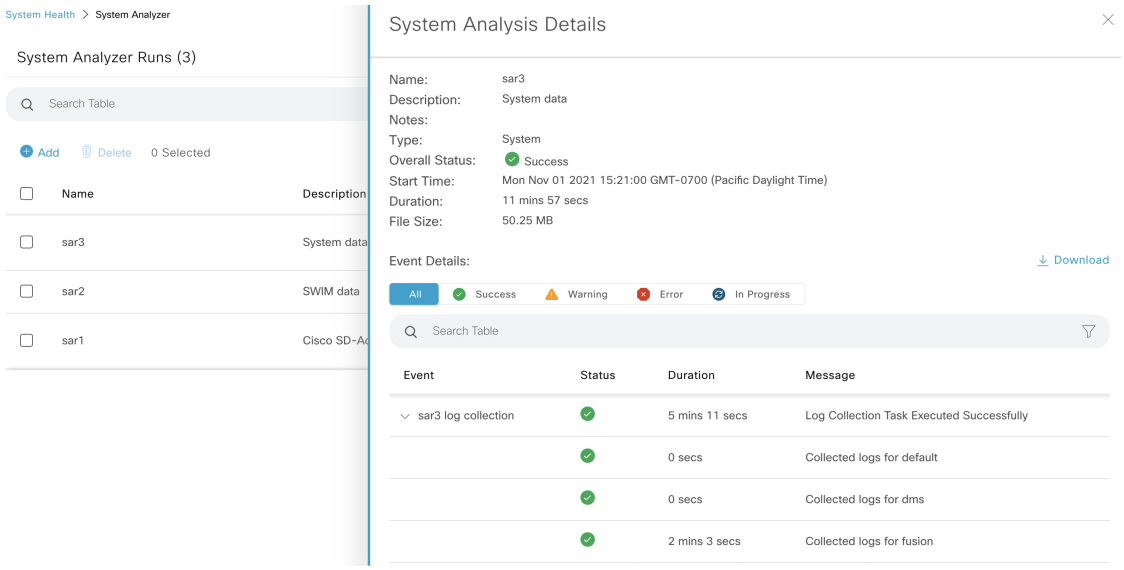
Step 4 (Optional) In the **Notes** field, enter any additional information (up to a maximum of 250 characters) you want to provide for the run.

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

Step 6 Click **Run**.

View System Analyzer Run Details

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



From here, you can also do the following:

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

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

System Topology Notifications

The following tables list the various notifications that are displayed in the system topology of the **System Health** page 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 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

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

Table 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	—	• A third-party IPAM provider is connected. • There is no third-party IPAM provider connected. • The third-party IPAM provider is currently synchronizing.
Cisco ISE—External RESTful Services (ERS)	—	ISE PAN ERS connection: ISE ERS API call unauthorized	ISE PAN ERS connection: ERS reachability with ISE - Success
Cisco ISE—Trust	—	ISE AAA Trust Establishment: Trust Establishment Error	ISE AAA Trust Establishment: Successfully established trust and discovered PSNs from PAN

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

Disk Utilization Event Notifications

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

Note the following points regarding disk utilization monitoring:

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

Suggested Actions

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

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

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

Component	Subcomponent	Issue	Suggested Actions
Cisco Connected Mobile Experiences (CMX) server IP address management (IPAM) server IT service management (ITSM) server	Reachability	Unable to establish connectivity with the server.	Check whether the server in question is currently down.
	Authentication	Unable to log in to the server.	Confirm that the correct login credentials are configured in 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		
	Networking	Interfaces are missing.	1. Connect to Cisco IMC. 2. If the PID is UCSC-C220-M4, UCSC-C220-M4S, or DN1-HW-APL, complete the following steps: a. From the main menu, choose **Compute** > **BIOS** > **Configure BIOS**. b. Click the **Advanced** tab. c. Expand **LOM and PCIe Slots Configuration**. d. Enable the disabled mLOMs and reboot the host. 3. For all other PIDs, replace the faulty component.

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

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 an 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.
- You must have Admin-level access in Cisco ISE.
- Disable password expiry for the Admin user in Cisco ISE. Alternatively, make sure that you update the password before it expires. For more information, see the *Cisco Identity Services Engine Administrator Guide*.
- When the Cisco ISE certificate changes, 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 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 under **System** > **Settings** > **External Services** > **Authentication and Policy Servers**. To change the secret password, choose **Design** > **Network Settings** > **Network** and click the **Change Shared Secret** link. This causes Cisco ISE to use the new secret password when connecting to network devices managed by Cisco DNA Center.
- In distributed Cisco ISE clusters, each node performs only certain functions, such as PAN (Admin), MnT (Monitoring and Troubleshooting), or PSN (Policy Service). It is possible to have only Admin certificate usage on PAN nodes, and only EAP Authentication certificate usage on PSN nodes. However, this configuration prevents Cisco DNA Center and Cisco ISE integration for pxGrid. Therefore, we recommend that you enable EAP Authentication certificate usage on the Cisco ISE primary PAN node.
- Cisco DNA Center supports certificate revocation checks via CRL Distribution Point (CDP) and Online Certificate Status Protocol (OCSP). During integration, Cisco DNA Center receives the Cisco ISE admin certificate over port 9060 and verifies its validity based on the CDP and OCSP URLs inside that Cisco ISE admin certificate. If both CDP (which contains a list of CRLs) and OCSP are configured, Cisco DNA Center uses OCSP to verify the revocation status of the certificate and falls back to CDP if the OCSP URL is not accessible. If there are multiple CRLs present in CDP, Cisco DNA Center contacts the next CRL if the first CRL is not reachable. However, due to a JDK PKI Oracle bug, the system does not check for all CRL entries.

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

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

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

Note Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Cisco DNA Center releases earlier than 2.2.1.x do not support more than two pxGrid nodes.

  - If you have a distributed Cisco ISE deployment:
    - You must integrate Cisco DNA Center with the primary policy administration node (PAN), and enable ERS on the PAN.

Note We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the PSNs.

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

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

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

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

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

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**.

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

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

- **Server IP Address**: IP address of the AAA server.
- **Shared Secret**: Key for device authentications. The shared secret can contain up to 100 characters.

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

- **Server IP Address**: IP address of the Cisco ISE server.
- **Shared Secret**: Key for device authentications.
- **Username**: Username that is used to log in to Cisco ISE via HTTPS.
- **Password**: Password for the Cisco ISE HTTPS username.

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

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

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

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

hostname.domainname.com

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

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

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

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

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

  When you enable this option, ensure that:

  - The Cisco DNA Center certificate is generated by the same Certificate Authority (CA) as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).
  - The Certificate Extended Key Use (EKU) field includes "Client Authentication."

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

  Attention If you do not enable 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 UDP port is 1812.
- **Accounting Port**: Port used to relay important events to the AAA server. The default UDP port is 1813.
- **Port**: The default TACACS port is 49.
- **Retries**: Number of times that Cisco DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
- **Timeout**: The time period for which the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

Note After the required information is provided, Cisco ISE is integrated with 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** window and **System 360** window:

Cisco ISE server registration phase:

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

pxGrid subscriptions registration phase:

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

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

Step 6 Click **Add**.

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

Configure Cisco AI Network Analytics

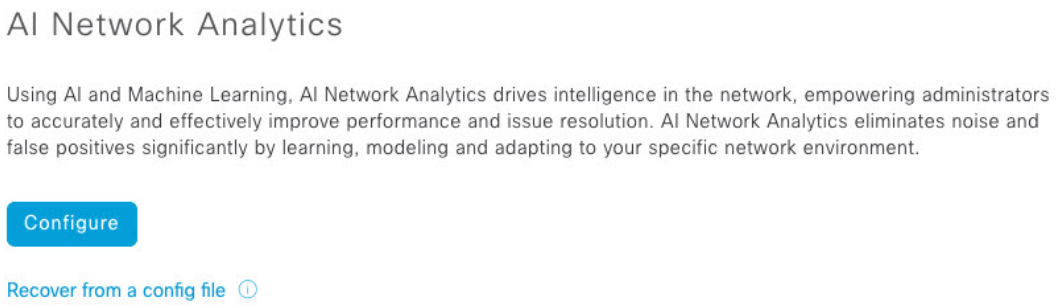
Use this procedure to enable the Cisco AI Analytics features to exports network event data from network devices as well as inventory, site hierarchy, and topology data to the Cisco AI Cloud.

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 the latest version of the AI Network Analytics application is installed. See Download and Install Application Updates, on page 91.
- Make sure that your network or HTTP proxy is configured to allow outbound HTTPS (TCP 443) access to the following cloud hosts:
  - **api.use1.prd.kairos.ciscolabs.com** (US East Region)
  - **api.euc1.prd.kairos.ciscolabs.com** (EU Central Region)

Step 1 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 Do one of the following:

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

     The Restore AI Network Analytics window appears.
  2. Drag-and-drop the configuration files in the area provided or choose the files from your file system.
  3. Click **Restore**.

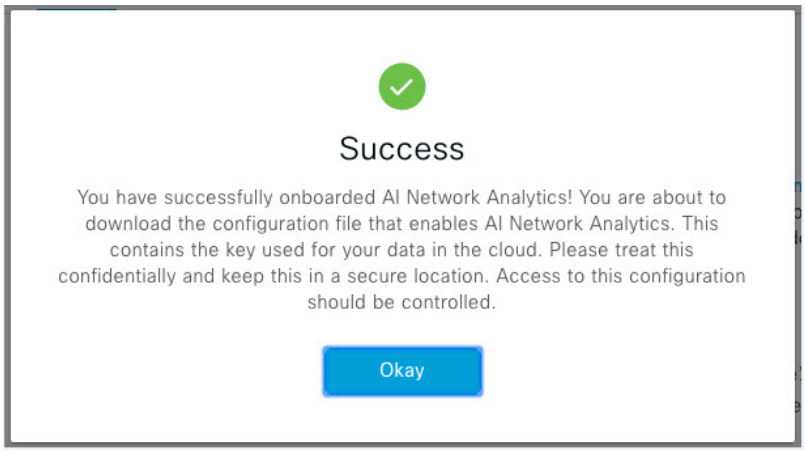
     Cisco AI Network Analytics might take a few minutes to restore, and then the **Success** dialog box appears.

- If this is the first time you are configuring Cisco AI Network Analytics, do the following:
  1. Click **Configure**.
  2. 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**.
  3. Click **Next**.

     The terms and conditions window appears.
  4. 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 **Enable AI Network Analytics** toggle button displays ☑.

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

Client Certificate Renewal

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

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

Disable Cisco AI Network Analytics

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

Step 1 Click the menu icon (☰) and choose **System** > **Settings**.

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

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

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

Step 4 Click **Update**.

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

Step 6 (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 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.
- **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY**: Integrates Cisco DNA Center with CX Cloud that allows you to perform an automated config. This integration provides enhanced vulnerability detection on devices directly from security advisories tool on Cisco DNA Center.

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

You can perform an automatic update only if 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.

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

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

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

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 93.

Step 1 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 49 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 93.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Cisco Accounts** > **Cisco.com Credentials**.

Step 2 Click **Clear**.

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

Configure Connection Mode

Connection mode manages the connections between smart-enabled devices in your network that interact with 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 Click the menu icon (☰) and choose **System** > **Settings** > **Cisco Accounts** > **SSM Connection Mode**.

The following connection modes are available:

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

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

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

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

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

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

Do not use a space or an underscore in the Smart Account name.

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

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

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

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

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

g) In the **Resync Devices** dialog box, do the following:

- Enter the **Smart Account**.
- Enter the **Virtual Account**.

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

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

Step 4 Choose **Smart proxy** to register your smart-enabled devices with the Cisco SSM cloud through 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.

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

Register Plug and Play

You can register 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 Click the menu icon (☰) and choose **System** > **Settings** > **Cisco Accounts** > **PnP Connect**.

A table of PnP connected profiles is displayed.

Step 2 Click **Register** to register a virtual account.

Step 3 In the **Register Virtual Account** window, the Smart Account you configured is displayed in the **Select Smart Account** drop-down list. You can select an account from the **Select Virtual Account** drop-down list.

Step 4 Click the required **IP** or **FQDN** radio button.

Step 5 Enter the IP address or FQDN (Fully Qualified Domain Name) of the controller.

Step 6 Enter the profile name. A profile is created for the selected virtual account with the configuration you provided.

Step 7 Check the **Use as Default Controller Profile** check box to register this Cisco DNA Center controller as the default controller in the Cisco PnP Connect cloud portal.

Step 8 Click **Register**.

Create PnP Event Notifications

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

Ensure that you create event notifications to the following PnP events:

Event Name	Event ID	Description
Add device failed	NETWORK-TASK_FAILURE-3-008	Device(s) are not added through single or bulk import. An error occurs when adding devices through single or bulk import.
Add device successful	NETWORK-TASK_COMPLETE-4-007	Device(s) are added through single or bulk import successfully.
Device in error state	NETWORK-ERROR_1-002	Device goes to **Error** state.
Device in provisioned state	NETWORK-INFO_4-003	Device goes to **Provisioned** state.
Device stuck in onboarding state	NETWORK-TASK_PROGRESS-2-006	Device is stuck in onboarding state for more than 15 minutes.
Device waiting to be claimed	NETWORK-INFO_2-001	Device reaches **Unclaimed** state and is ready to be provisioned.
Smart Account sync failed	NETWORK-TASK_FAILURE-1-005	Smart Account sync is failed for some devices.
Smart Account sync successful	NETWORK-TASK_COMPLETE-4-004	Smart Account sync is successful for some devices.

Configure Smart Account

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

Before you begin

Ensure that you have SUPER-ADMIN-ROLE permissions.

Step 1 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.

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

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

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

Step 9 Click **Delete**.

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

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

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).

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

Before you begin

- To enable Smart Licensing, you must configure Cisco Credentials (see Configure Cisco Credentials, on page 42) 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 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 49.

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.

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.

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 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 Click the menu icon (☰) and choose **System** > **Settings** > **Device Settings** > **Device EULA Acceptance**.

Step 2 Click the **Cisco End User License Agreement** link and read the EULA.

Step 3 Check the **I have read and accept the Device EULA** check box.

Step 4 Click **Save**.

Configure SNMP Properties

You can configure retry and timeout values for SNMP.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles, on page 93.

Step 1 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**.

Enable ICMP Ping

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

The following procedure describes how to enable an ICMP ping.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Device Settings** > **ICMP Ping**.

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

Step 3 Click **Save**.

Configure an Image Distribution Server

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

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Device Settings**.

Step 2 From the **Device Settings** drop-down list, choose **Image Distribution Servers**.

Step 3 In the **Image Distribution Servers** window, click **Servers**.

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

Step 4 Click **Add** to add a new image distribution server.

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

Step 5 Configure the following image distribution server settings:

- **Host**: Enter the hostname or IP address of the image distribution server.
- **Root Location**: Check the **Use root directory for file transfers** check box to use the root directory for file transfers, or uncheck the **Use root directory for file transfers** check box and enter the root location.

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

Step 6 Click **Save**.

Step 7 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:

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

Step 8 (Optional) To edit the settings, click the **Edit** icon next to the corresponding image distribution server in the **Action** column, make the required changes in the **Edit** window, and click **Save**.

Step 9 (Optional) To delete an image distribution server, click the **Delete** icon next to the corresponding image distribution server in the **Action** column and click **Delete**.

Enable PnP Device Authorization

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

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Device Settings**.

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

Note By default, devices are automatically authorized.

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

Step 4 Click **Save**.

Configure Device Prompts

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

Create Custom Prompts

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Device Settings** > **Device Prompts**.

The **Device Prompts** window appears.

Step 2 Click **Create Custom Prompt**.

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

Step 3 To create custom prompts for the username, do the following:

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

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

c. Click **Save**.

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

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

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

c. Click **Save**.

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

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

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

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

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

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

Configure Device Configuration Backup Settings

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

Note By default, the configuration backup is scheduled every Sunday at 11:30 p.m. (UTC time zone).

Step 1 Click the menu icon (≡) and choose **System** > **Settings** > **Configuration Archive**.

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

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

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

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

Step 4 Choose the backup day and time.

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

Step 5 Click **Save**.

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

Step 6 Click the **External** tab to configure an external server for archiving the device configuration. For more information, see Configure an External Server for Archiving the Device Configuration, on page 53.

Configure an External Server for Archiving the Device Configuration

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

For information about the supported servers, see the Server Requirements for Automation Data Backup section in Backup Server Requirements, on page 131.

Step 1 Click the menu icon (≡) and choose **System** > **Settings** > **Configuration Archive**.

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

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

Note Only one SFTP server can be added.

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

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

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

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

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

d) Choose the **Backup Format**:

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

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

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

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

e) Schedule the backup cycle.

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

Step 5 Click **Save**.

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

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

Cloud Access Keys

You can register cloud access keys after installing the Cloud Device Provisioning Application package in 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 wireless controllers.

Before you begin

- Obtain the access key ID and secret key from the Amazon Web Services (AWS) console.
- Subscribe to CSR or wireless controller products in the AWS marketplace and verify the image ID for the target region.
- Identify the key pair that CSRs will use during HA failover on AWS. The key pair's name is selected from a list in 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 65.

- 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 Application Updates, on page 91.

Step 1 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/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar

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

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

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles, on page 93.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Integrity Verification**.

Step 2 Review the current KGV file information:

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

Step 3 To import the KGV file, perform one of the following steps:

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

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

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

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

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

Step 6 Perform one of the following procedures to import locally:

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

Step 7 Click **Import**.

The KGV file is imported into Cisco DNA Center.

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

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

The following KGV auto download information is displayed:

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

What to do next

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

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

Configure an IP Address Manager

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

Before you begin

- You should have an external IP address manager already set up and functional.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **IP Address Manager**.

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

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

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

a) Click the warning icon.

A **Certificate Warning** dialog box appears.

b) Verify the issuer, serial number, and validity dates for the certificate.
c) If the information is correct, click the check box to allow Cisco DNA Center to access the IP address and add the untrusted certificate to the trustpool.
d) Click **Allow**.

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

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

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

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

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

Step 7 Click **Save**.

What to do next

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

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

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

Configure Webex Integration

Cisco DNA Center provides Webex meeting session information for client 360.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Webex Integration**.

Step 2 Click **Authenticate to Webex**.

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

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

Webex authentication is completed successfully.

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

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

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

Configure an MS Teams Integration

Once enabled, Cisco DNA Center provides call quality metrics information for Application 360 and Client 360 dashboards.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **External Services**.

Step 2 Click **MS Teams Integration**.

Step 3 Click **Register**.

Step 4 In the **Microsoft** login window, enter the Microsoft admin username and password, and click **Sign In**.

Step 5 Click **Accept** to enable Microsoft Teams integration.

Step 6 (Optional) Click **Delete** to delete the Microsoft Teams integration.

Configure ThousandEyes Integration

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

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

Before you begin

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

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **ThousandEyes Integration**.

Step 2 In the **Insert new token here** field, enter the authentication token.

Note To receive the OAuth Bearer Token, go to the **ThousandEyes** page.

Step 3 Click **Save**.

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 93.

Step 1 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 93.
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 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 Click the menu icon (☰) and choose **Activities** > **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:

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

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

c. Click **Apply**.

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

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

Note An audit log captures data about a task performed by 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 the event ID.

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

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

A list of syslog servers appears.

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

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

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

Step 9 Click the menu icon (☰) and choose **Activities** > **Scheduled Tasks** to view the upcoming, in-progress, completed, and failed administrative tasks, such as operating system updates or device replacements.

Step 10 Click the menu icon (☰) and choose **Activities** > **Work Items** tab to view the 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 Click the menu icon (☰) and choose **Activities** > **Audit Logs**.

Step 2 Click **Subscribe**.

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

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

View Tasks

You can view information about in progress, completed, and failed tasks running on Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Activities** > **Tasks**.

In the left pane, the **SUMMARY** area lists the following:

- **Status**: The **Upcoming**, **In Progress**, **Success**, and **Failed** tasks.
- **Last Updated**: The tasks updated in the last **3 Hours**, **24 Hours**, or **7 Days**.
- **Categories**: The tasks based on multiple categories. You can choose multiple categories at a time.
- **Recurring**: The recurring tasks.

Step 2 Click the task link to open a slide-in pane that shows **Starts**, **Status**, **Last updated**, and additional information about upcoming, in progress, completed, and failed tasks.

Step 3 In the failed task slide-in pane, click the **Download Error Report** link to download an error report of the respective task.

A tar file is created and saved to your local machine.

Note While creating a support case, you can attach the downloaded error report in addition to other details you may want to include.

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 (☰) 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 Click the menu icon (☰) and choose **System** > **Settings** > **Integration Settings**.

Step 2 Enter the **Callback URL Host Name** or **IP Address** that the third-party app needs to connect to when communicating with the 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 up a message that appears to all users after 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 Click the menu icon (☰) and choose **System** > **Settings** > **System Configuration** > **Login Message**.

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

Step 3 Click **Save**.

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

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

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

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

Configure the Proxy

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

Note 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 93.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **System Configuration**.

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

Step 3 Enter the proxy server's URL address.

Step 4 Enter the proxy server's port number.

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

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

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

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

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

After configuring the proxy, you are able to view the configuration in the **Proxy** window.

Security Recommendations

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.
- 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.
- Replace the self-signed server certificate from Cisco DNA Center with the certificate signed by your internal certificate authority (CA).
- If possible in your network environment, disable SFTP Compatibility Mode. This mode allows legacy network devices to connect to Cisco DNA Center using older cipher suites.
- Disable the browser-based appliance configuration wizard, which comes with a self-signed certificate.
- Upgrade the minimum TLS version. Cisco DNA Center comes with TLSv1.1 and TLSv1.2 enabled by default, and we recommend that you set the minimum TLS version to 1.2 if possible in your network environment. For more information, see Change the Minimum TLS Version and Enable RC4-SHA (Not Secure), on page 66.

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 an 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 recommend that you do not downgrade Cisco DNA Center TLS version or enable RC4-SHA ciphers.

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

Note 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.

The following is an example:

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

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

The following example shows how to change from TLS Version 1.1 to 1.0:

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

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

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

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

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

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

The following example shows TLS version 1.2 is not enabled:

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

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

The following is an example:

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

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

Step 7 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 93.
- 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 Click the menu icon (☰) and choose **System** > **Settings** > **System Configuration**.

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

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

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

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

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

Step 5 Click **Save**.

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

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

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

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

Upload an SSL Intercept Proxy Certificate

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

Note For added security, access to the root shell is disabled in Cisco DNA Center. With restricted shell, users can't access the underlying operating system and file system, which reduces operational risk. However, the commands in this section require that you contact the Cisco TAC to access the root shell temporarily. See About Restricted Shell, on page 82.

Step 1 Transfer your proxy server's certificate (in .pem format) to the `/home/maglev` directory on the Cisco DNA Center server.

Step 2 As the maglev user, SSH to the Cisco DNA Center server and enter the following command, where <*proxy.pem*> is your proxy server's TLS/SSL certificate file:

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

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

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

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

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

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

Step 5 Check cloud connectivity from the Cisco DNA Center GUI.

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 to 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 Click the menu icon (☰) and choose **System** > **Settings** > **Trust & Privacy** > **System Certificates**.

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

When you first view this window, the current certificate data that is displayed 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 is displayed 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 In the **System Certificates** window, click **Replace Certificate**.

In Cisco DNA Center 2.3.2 and later, you will see the **Generate New CSR** link if you are generating the CSR for the first time. Otherwise, you will see the **Download existing CSR** link. You can download the existing CSR and submit it to your provider to generate your certificate. If you don't want to use the existing CSR, click **Delete existing CSR** and click **Accept** in the subsequent **Confirmation** window. You can now see the **Generate New CSR** link.

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

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

Step 6 Click **Generate New CSR**.

The generated new CSR is downloaded automatically.

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

- Copy the CSR properties in plain text.
- Copy Base64 and paste to MS CA.

- Download Base64.

Step 7 (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 8 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.

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

Step 9 Confirm that the certificate issuer provides the certificate full chain (server and CA) in p7b. When in doubt, do the following to examine and assemble the chain:

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

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

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

Step 10 If the certificate issuer provides the certificate and its issuer CA chain in loose files, do the following:

a) Gather the PEM (base64) files or use openssl to convert DER to PEM.
b) Concatenate the certificate and its issuer CA, starting with the certificate, followed by subordinate CA, all the way to the root CA, and output it to dnac-chain.pem file.

cat certificate.pem subCA.pem rootCA.pem > dnac-chain.pem

c) Continue to upload as PEM.

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

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

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

After the upload succeeds, the system certificate is validated.

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

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

After the upload succeeds, the private key is validated.

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

Step 12 For a **PKCS** file, perform the following tasks:

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

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

After the upload succeeds, the system certificate is validated.

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

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

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

Step 13 Click **Save**.

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

Step 14 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

Cisco DNA Center uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and the provisioning of certificates to network devices. You can use your own SCEP broker and certificate service, or you can use an external SCEP broker. To set up an external SCEP broker, complete the following procedure:

Note For more information regarding SCEP, see Simple Certificate Enrollment Protocol Overview.

Step 1 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 By default, **Manages Device Trustpoint** is enabled, meaning Cisco DNA Center configures the sdn-network-infra-iwan trustpoint on the device. You must complete the following steps:

a) Enter the enrollment URL where the device requests the certificate via SCEP.
b) (Optional) Enter any optional subject fields used by the certificate, such as country, locality, state, organization, and organization unit. The common name (CN) is automatically configured by Cisco DNA Center with the device platform ID and device serial number.
c) In the **Revocation Check** field, click the drop-down list and choose the appropriate revocation check option.

d) (Optional) Check the **Auto Renew** check box and enter an auto enrollment percentage.

If **Manages Device Trustpoint** is disabled, in order for devices to send wired and wireless Assurance telemetry to Cisco DNA Center, you must manually configure the sdn-network-infra-iwan trustpoint on the device and then import a certificate. See Configure the Device Certificate Trustpoint.

Step 6 Click **Save**.

The external CA certificate is uploaded.

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

Switch Back to an Internal PKI Certificate

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

Step 1 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.

Export the Cisco DNA Center PKI Certificate

Cisco DNA Center allows you to download the device certificates that are required to set up an external entity such as a AAA (pronounced "triple A") server or Cisco ISE server to authenticate the devices.

Step 1 Click the menu icon (≡) and choose **System** > **Settings** > **Trust & Privacy** > **PKI Certificates**.

Step 2 Click **Download CA Certificate** to export the device CA and add it as the trusted CA on the external entities.

Certificate Management

Manage Device Certificates

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

Step 1 Click the menu icon (≡) and choose **System** > **Settings** > **Trust & Privacy** > **Device Certificate**.

The **Device Certificate** window shows the status of issued certificates in separate status tabs:

- **Expired** status tab: Shows the list of certificates whose lifetime has expired.

- **Expiring** status tab: Shows the list of certificates that are nearing the expiry date, in the ascending order.
- **All** status tab: Shows the list of valid, expired, and expiring certificates.
- **Revoked** status tab: Shows the certificates that are revoked.

Step 2 You can filter the certificates, based on the **Device Name** and **Issue To** value.

Step 3 If you want to revoke a valid certificate, do the following:

a) Click the **All** status tab.
b) In the **Actions** column, click the **Revoke** icon that corresponds to the certificate that you want to revoke.
c) In the confirmation window, click **OK**.

Step 4 If you want to export the certificate details, click **Export**.

The certificate details are exported in CSV format.

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.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Trust & Privacy** > **Device Certificate**.

Step 2 Review the device certificate and the current device certificate lifetime.

Step 3 In the **Device Certificate** window, click **Modify**.

Step 4 In the **Device Certificate Lifetime** dialog box, enter a new value, in days.

Step 5 Click **Save**.

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.

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. When making this change, do 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.
- If device controllability is enabled (which is the default) before the switchover from the internal root CA to the subordinate CA, the new device certificate is updated automatically.
- The subordinate CA certificate lifetime, as displayed in the GUI, is just read from the certificate; it is not computed against the system time. Therefore, if you install a certificate with a lifespan of 1 year today and look at it in the GUI the same time next year, the GUI will still show that the certificate has a 1-year lifetime.
- The subordinate CA certificate must be in PEM or DER format only.
- The subordinate CA does not interact with the higher CAs; therefore, it is not aware of revocation, if any, of the certificates at a higher level. Because of this, any information about certificate revocation is also not communicated from the subordinate CA to the network devices. Because the subordinate CA does not have this information, all the network devices use only the subordinate CA as the Cisco Discovery Protocol (CDP) source.

Before you begin

You must have a copy of the root CA certificate.

Step 1 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 are displayed:

For example,

- Changing from root CA to subordinate CA is a process that cannot be reversed.
- You must ensure that no network devices have been enrolled or issued a certificate in root CA mode. Network devices that have been accidentally enrolled in root CA mode must be revoked before changing from root CA to subordinate CA.
- Network devices must come online only after the subordinate CA configuration process finishes.

Step 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 is displayed.

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 76.
- 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 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.

Configure the Device Certificate Trustpoint

If **Manages Device Trustpoint** is disabled in Cisco DNA Center, in order for devices to send wired and wireless Assurance telemetry to Cisco DNA Center, you must manually configure the sdn-network-infra-iwan trustpoint on the device and then import a certificate.

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

Step 1 Enter the following commands:

```
crypto pki trustpoint sdn-network-infra-iwan
  enrollment url http://<SCEP_enrollment_URL_to_external_CA>
  fqdn <device_FQDN>
  subject-name CN=<device_platform_ID>_<device_serial_number>_sdn-network-infra-iwan
  revocation-check <crl, crl none, or none>  # to perform revocation check with CRL, CRL fallback to
 no check, or no check
  rsakeypair sdn-network-infra-iwan
  fingerprint <CA_fingerprint> # to verify that the CA at the url connection matches the fingerprint
 given
```

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

```
auto-enroll 80 regenerate
```

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

```
source interface <interface>
```

Renew Certificates

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 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.

About Restricted Shell

For added security, access to the root shell is disabled starting in this release of Cisco DNA Center. With restricted shell, users can't access the underlying operating system and file system, which reduces operational risk.

Restricted shell is enabled for security purposes. However, if you want to access the root shell temporarily, you must contact the Cisco TAC for assistance.

If necessary, you can use the following restricted list of commands:

```
$ ?
Help:
  cat                  concatenate and print files in restricted mode
  clear                clear the terminal screen
  date                display the current time in the given FORMAT, or set the system date

  debug                enable console debug logs
  df                   file system information
  dmesg                print or control the kernel ring buffer.
  du                 summarize disk usage of the set of FILEs, recursively for directories.

  free                 quick summary of memory usage
  history              enable shell commands history
  htop                 interactive process viewer.
  ip                   print routing, network devices, interfaces and tunnels.
  last                 show a listing of last logged in users.
  ls                   restricted file system view chrooted to maglev Home
  lscpu                print information about the CPU architecture.
  magctl               tool to manage a Maglev deployment
  maglev               maglev admin commands
  maglev-config        tool to configure a Maglev deployment
  manufacture_check    tool to perform manufacturing checks
  netstat              print networking information.
  nslookup             query Internet name servers interactively.
  ntpq                 standard NTP query program.
  ping                 send ICMP ECHO_REQUEST to network hosts.
  ps                   check status of active processes in the system
```

```
rca                 root cause analysis collection utilities
reboot              Reboot the machine
rm                  delete files in restricted mode
route               print the IP routing table.
runonce             Execute runonce scripts
scp                 restricted secure copy
sftp                secure file transfer
shutdown            Shutdown the machine
ssh                 OpenSSH SSH client.
tail                Print the last 10 lines of each FILE to standard output
top                 display sorted list of system processes
traceroute          print the route packets trace to network host.
uname               print system information.
uptime              tell how long the system has been running.
vi                  text editor
w                   show who is logged on and what they are doing.
```

About Product Usage Telemetry Collection

Telemetry data is collected by default in Cisco DNA Center, but you can opt out of some data collection. The data collection is designed to help the development of product features and address any operational issues, providing greater value and return on investment (ROI). Cisco collects the following categories of data: Cisco.com ID, System, Feature Usage, Network Device Inventory, and License Entitlement. See the *Cisco DNA Center Data Sheet* for a more expansive list of data that we collect. To opt out of some of data collection, contact your Cisco account representative and the Cisco Technical Assistance Center (TAC).

Click the menu icon (☰) and choose **System** > **Settings** > **Terms and Conditions** > **Telemetry Collection**. You can review the license agreement, the privacy statement, and the privacy data sheet from the **Telemetry Collection** window.

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 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 Click the menu icon (☰) and choose **System** > **Settings** > **Trust & Privacy** > **Account Lockout**.

Step 2 Click the **Enforce Account Lockout** toggle button so that you see a check mark.

Step 3 Enter values for the following **Enforce Account Lockout** parameters:

- Maximum Login Retries
- Lockout Effective Periods (minutes)
- Reset Login Retries after (minutes)

Note Hover your cursor over **Info** to view details for each parameter.

Step 4 Choose the **Idle Session Timeout** value from the drop-down list.

Step 5 Click **Save**.

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

Password Expiry

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

Step 1 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.

IP Access Control

IP access control allows you to control the access to Cisco DNA Center based on the IP address of the host or network. Cisco DNA Center provides the following options for IP access control:

- Allow all IP addresses to access Cisco DNA Center. By default, all IP addresses can access Cisco DNA Center.
- Allow only selected IP addresses to access Cisco DNA Center.

Configure IP Access Control

To configure IP access control and allow only selected IP addresses to access Cisco DNA Center, perform the following steps:

1. Enable IP Access Control, on page 85.
2. Add an IP Address to the IP Access List, on page 85.
3. (Optional) Delete an IP Address from the IP Access List, on page 86.

Enable IP Access Control

Before you begin

Ensure that you have SUPER-ADMIN-ROLE permissions.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 Click the **Allow only listed IP addresses to connect** radio button.

Step 3 Click **Add IP List**.

Step 4 In the **IP Address** field of the **Add IP** slide-in pane, enter your IPv4 address.

Note If you don't add your IP address to the IP access list, you may lose access to Cisco DNA Center.

Step 5 In the **Subnet Mask** field, enter the subnet mask.

The valid range for subnet mask is from 0 through 32.

Step 6 Click **Save**.

Add an IP Address to the IP Access List

To add more IP addresses to the IP access list, perform the following steps.

Before you begin

Ensure that you enable IP access control.

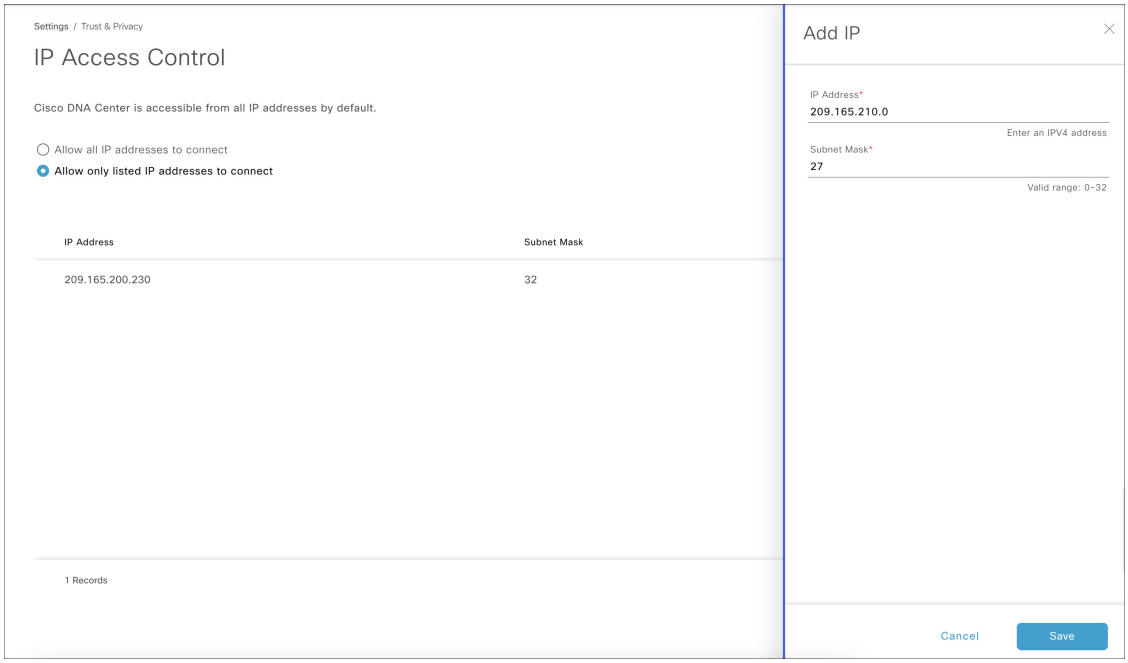
Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 Click **Add**.

Step 3 In the **IP Address** field of the **Add IP** slide-in pane, enter the IPv4 address of the host or network.

Step 4 In the **Subnet Mask** field, enter the subnet mask.

The valid range for subnet mask is from 0 through 32.



Step 5 Click **Save**.

Delete an IP Address from the IP Access List

The following section provides information about how to delete an IP address from the IP access list to disable its access to Cisco DNA Center.

Before you begin

Ensure that you have enabled IP access control and added IP addresses to the IP access list.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 In the **Action** column, click the **Delete** icon for the corresponding IP address.

Step 3 Click **Delete**.

Disable IP Access Control

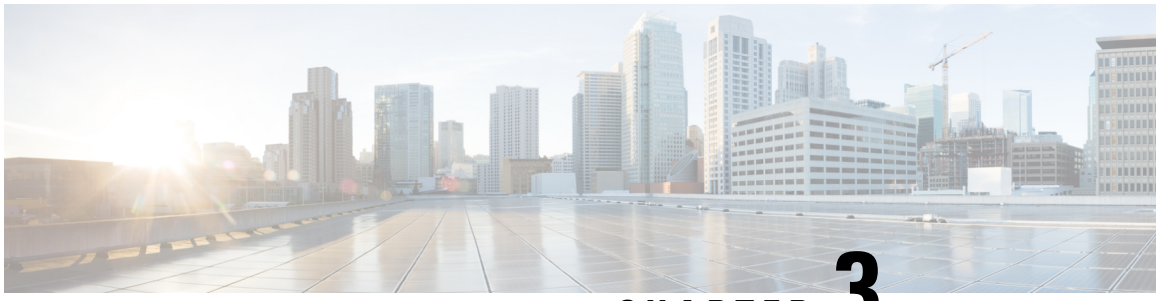
The following section provides information about how to disable IP access control to allow all IP addresses to access Cisco DNA Center.

Before you begin

Ensure that you have SUPER-ADMIN-ROLE permissions.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 Click the **Allow all IP addresses to connect** radio button.



CHAPTER 3

Manage Applications

- Application Management, on page 89
- Download and Install the Latest System Version, on page 89
- Download and Install a Previous System Version, on page 90
- Download and Install Application Updates, on page 91
- Uninstall an Application, on page 92

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 Management** 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, click the **Currently Installed Applications** link and place your cursor over its name.

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 Install the Latest System Version

The **Software Management** window indicates when the latest Cisco DNA Center version is available. Complete the following procedure to download and install it.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles, on page 93.

Step 1 Click the menu icon (☰) and choose **System** > **Software Management**.

Important At this point, Cisco DNA Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window will not display a system update that's currently available.

Step 2 If the window indicates that a system update is available, click **Download now**.

Step 3 After Cisco DNA Center completes its prechecks, click **Download**.

Step 4 After the package download completes, click **Install now**.

Step 5 After Cisco DNA Center completes its prechecks, click **Install**.

Step 6 Cisco DNA Center enters Maintenance mode and is unavailable as the system update takes place. After the update completes, log back in to Cisco DNA Center.

Step 7 Click the menu icon (☰) and choose **System** > **Software Management** to reopen the **Software Management** window.

A message at the top of the window indicates that your system is up to date.

Download and Install a Previous System Version

Complete the following procedure if you want to download and install an available Cisco DNA Center version other than the latest version.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles, on page 93.

Step 1 Click the menu icon (☰) and choose **System** > **Software Management**.

Step 2 In the **Looking for other releases?** field, click the **Click here** link.

Step 3 Click the radio button for the Cisco DNA Center version you want to download, then click **Select**.

Note Refer to the **Installed version** field to determine the version that you currently have installed.

Step 4 After Cisco DNA Center completes its prechecks, click **Download**.

The overall progress of the download is updated as the process runs. Click the **More details** link to open a slide-in pane that displays the progress of the individual applications that are being downloaded to your system.

After the download completes, the **Software Management** window updates and indicates that previous Cisco DNA Center versions are available to install.

Step 5 Click the **Available installations** link.

Step 6 Click the radio button for the version that you want to install, then click **Select**.

Step 7 After Cisco DNA Center completes its prechecks, click **Install**.

The overall progress of the installation is updated as the process runs. Click the **More details** link to open a slide-in pane that displays the progress of the individual applications that are being installed onto your system.

Step 8 If prompted after the installation completes, click **Refresh** to update the **Software Management** window.

Download and Install Application 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 93.

Step 1 Click the menu icon (☰) and choose **System** > **Software Management**.

Important At this point, Cisco DNA Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window will not display application updates that are currently available.

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

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

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

Note To open a slide-in pane that indicates an update's file size and provides a brief description of the corresponding application, click its **More details** link.

Step 3 Click **Install**.

Step 4 After Cisco DNA Center completes a dependency check, click **Continue**.

The window displays a progress bar for each application that's being updated. The **Software Management** window updates after all of the updates have been installed.

Step 5 Click the **Currently Installed Applications** link and confirm that the applications you selected have been updated.

Package Download and Upgrade Event Notifications

You can receive a notification whenever a package download or upgrade event takes place. To configure and subscribe to these notifications, complete the steps described in the Cisco DNA Center Platform User Guide's "Work with Event Notifications" topic. When completing this procedure, ensure that you select and subscribe to the SYSTEM-SOFTWARE-UPGRADE event.

A notification is generated and sent when:

- The download of a package upgrade failed. This typically happens because your Cisco DNA Center appliance doesn't have the necessary disk space or you're attempting to download a corrupted package.
- The installation of a package upgrade failed (possibly because the service that's associated with the package is currently down).
- The download or installation of a package upgrade succeeded.

Note A notification is sent only if the previous attempt to complete the operation failed.

Uninstall an Application

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 93.

Step 1 Click the menu icon (☰) and choose **System** > **Software Management**.

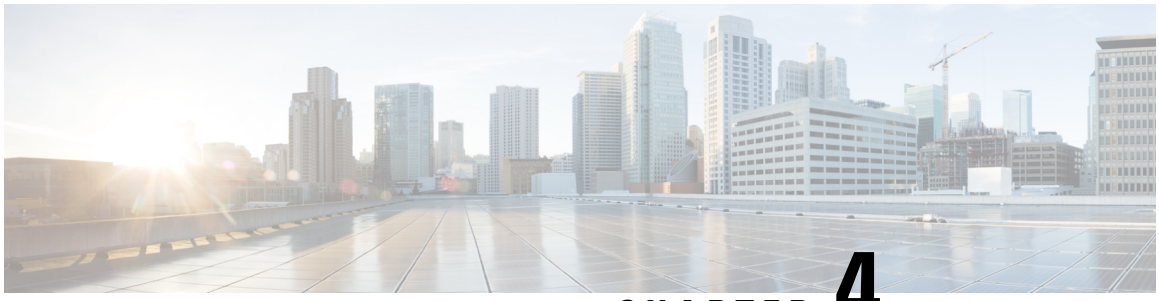
Step 2 Click the **Currently Installed Applications** link to view all of the applications that are installed on your Cisco DNA Center appliance.

Step 3 For the package that you want to remove, click its **Uninstall** link.

Note You cannot uninstall multiple packages simultaneously.

Step 4 Confirm that you want to remove the application by clicking **Uninstall**.

Cisco DNA Center displays a message after the application has been removed.



CHAPTER 4

Manage Users

- About User Profiles, on page 93
- About User Roles, on page 93
- Create an Internal User, on page 94
- Edit a User, on page 94
- Delete a User, on page 95
- Reset a User Password, on page 95
- Change Your Own User Password, on page 96
- Reset a Forgotten Password, on page 96
- Configure Role-Based Access Control, on page 97
- Display Role-Based Access Control Statistics, on page 102
- Configure External Authentication, on page 103
- Two-Factor Authentication, on page 105
- Display External Users, on page 109

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 93.

Step 1 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 93.

Step 1 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 93.

Step 1 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 93.

Step 1 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

Before you begin

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

Step 1 Click the menu icon (☰) and choose **System** > **Users & Roles** > **Change Password**.
Step 2 Enter information in the required fields.
Step 3 Click **Update**.

Change Your Own User Password Without Admin Permission

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

Step 1 Click the menu icon, hover your cursor over **admin**, and choose **My Profile and Settings** > **My Account**.
Step 2 Click **Update Password**.
Step 3 Enter the current password, enter the new password, and confirm the new password.
Step 4 Click **Update**.

Reset a Forgotten Password

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

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) Click the menu icon (☰) and choose **System** > **Users & Roles** > **Role Based Access Control**.
b) Click **Create a New Role**.
The **Create a Role** window appears. If this is your first iteration of RBAC, after you have created the new role, you will be asked to assign users to the new role.
c) If a task overview window opens, click **Let's do it** to go directly to the workflow.
The **Create a New Role** window 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) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
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. This role lets you: • Resolve, close, and ignore issues. • Run Machine Reasoning Engine (MRE) workflows. • Analyze trends and insights. • Troubleshoot issues, including path trace, sensor dashboards, and rogue management. • Run workflows for rogue and Cisco Advanced Wireless Intrusion Prevention System (aWIPS). These workflows include AP-allowed list, vendor-allowed list, aWIPS profile creation, assigning an aWIPS profile, and so on.
Monitoring Settings	Configure and manage issues. Update network, client, and application health thresholds. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.

Capability	Description
Troubleshooting Tools	Create and manage sensor tests. Schedule on-demand forensic packet captures (Intelligent Capture) for troubleshooting clients. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.
Network Analytics	Manage network analytics-related components.
Data Access	Enable access to query engine APIs. Control functions such as global search, rogue management, and aWIPS. Note: Setting the permission to Deny will affect Search and Assurance functionality.
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	• Update network settings, such as global device credentials, authentication and policy servers, certificates, trustpool, cloud access keys, Stealthwatch, Umbrella, and data anonymization. • Export the device inventory and its credentials. **Note** To complete this task, you must have Read permission on **Network Settings**.
Image Repository	Manage software images and facilitate upgrades and updates on physical and virtual network entities.
Network Hierarchy	Define and create a network hierarchy of sites, buildings, floors, and areas based on geographic location. Users with this role can also add CMX servers in **System** > **Settings**.
Network Profiles	Create network profiles for routing, switching, and wireless. Assign profiles to sites. This role includes Template Editor, Tagging, Model Config Editor, and Authentication Template. Note: To create SSIDs, you must have Write permission on **Network Settings**.
Network Settings	Common site-wide network settings such as AAA, NTP, DHCP, DNS, Syslog, SNMP, and Telemetry. Users with this role can add an SFTP server and modify the Network Resync Interval in **System** > **Settings**. Note: To create wireless profiles, you must have Write permission on **Network Profiles**.
Virtual Network	Manage virtual networks (VNs). Segment physical networks into multiple logical networks for traffic isolation and controlled inter-VN communication.
Network Provision	Configure, upgrade, provision, and manage your network devices.
Compliance	Manage compliance provisioning.
EoX	Scan the network for details on publicly announced information pertaining to the **End of Life**, **End of Sales**, or **End of Support** of the hardware and software in your network.
Image Update	Upgrade software images on devices that don't match the Golden Image settings after a complete upgrade lifecycle.

Capability	Description
Inventory Management	Discover, add, replace, or delete devices on your network while managing device attributes and configuration properties. Note: To replace a device, you must have Write permission on **Network Provision** > **PnP**.
Inventory Management > Device Configuration	Device Configuration: Display the running configuration of a device.
Inventory Management > Discovery	Discovery: Discover new devices in your network.
Inventory Management > Network Device	Network Device: Add devices from Inventory, view device details, and perform device-level actions.
Inventory Management > Port Management	Port Management: Allow port actions on a device.
Inventory Management > Topology	Topology: Display network device and link connectivity. Manage device roles, tag devices, customize the display, and save custom topology layouts. Note: To view the SD-Access Fabric window, you must have at least Read permission on **Network Provision** > **Inventory Management** > **Topology**.
License	Unified view of your software and network assets relative to license usage and compliance. The role also controls permissions for cisco.com and Smart accounts.
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. Note: To enable or disable network telemetry, you must have Write permission on **Provision**.
PnP	Automatically onboard new devices, assign them to sites, and configure them with site-specific contextual settings.
Provision	Provision devices with the site-specific settings and policies that are configured for the network. This role includes Fabric, Application Policy, Application Visibility, Cloud, Site-to-Site VPN, Network/Application Telemetry, Stealthwatch, Sync Start vs Run Configuration, and Umbrella provisioning. On the main dashboards for rogue and aWIPS, you can enable or disable certain actions, including rogue containment. To provision devices, you must have Write permission on **Network Design** and **Network Provision**.
Network Services	Configure additional capabilities on the network beyond basic network connectivity and access.
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	Configure network elements to send data to Cisco Stealthwatch to detect and mitigate threats, even in encrypted traffic. To provision Stealthwatch, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Services** > **Stealthwatch** • **Network Design** > **Advanced Settings**
Umbrella	Configure network elements to use Cisco Umbrella as the first line of defense against cybersecurity threats. To provision Umbrella, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Provision** > **Scheduler** • **Network Services** > **Umbrella** You must also have Read permission on **Advanced Network Settings**.
Platform	Open platform for accessible, intent-based workflows, data exchange, notifications, 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	Subscribe to get notified in near real time about network and system events of interest and initiate corrective actions. You can configure email and syslog logs in **System** > **Settings** > **Destinations**.
Reports	Generate reports using predefined reporting templates for all aspects of your network. Generate reports for rogue devices and for aWIPS. You can configure webhooks in **System** > **Settings** > **Destinations**.
Security	Manage and control secure access to the network.
Group-Based Policy	Manage group-based policies for networks that enforce segmentation and access control based on Cisco security group tags. This role includes Endpoint Analytics.
IP-Based Access Control	Manage IP-based access control lists that enforce network segmentation based on IP addresses.
Security Advisories	Scan the network for security advisories. Review and understand the impact of published Cisco security advisories that may affect your network.

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. This role includes Cisco Credentials, Integrity Verification, Device EULA, HA, Integration Settings, Disaster Recovery, Debugging Logs, Telemetry Collection, System EULA, IPAM, vManage Servers, Cisco AI Analytics, 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.
Event Viewer	View network device and client events for troubleshooting.
Network Reasoner	Initiate logical and automated troubleshooting for network issues while drawing on the knowledge wealth of network domain experts.
Remote Device Support	Allow the Cisco support team to remotely troubleshoot the network devices managed by Cisco DNA Center. With this role enabled, an engineer from the Cisco Technical Assistance Center (TAC) can connect remotely to a customer's Cisco DNA Center setup for troubleshooting purposes.
Scheduler	Integrated with other back-end services, scheduler lets you run, schedule, and monitor network tasks and activities such as deploy policies, provision, or upgrade the network. You can also schedule rogue containment.
Search	Search for various objects in 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 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 93.
- You must configure at least one authentication server.

Note 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.

When external authentication fallback is enabled, external users and local admins can log in to Cisco DNA Center.

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 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 TACACS authentication, the following AAA attributes are supported:

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

For RADIUS authentication, the following AAA attributes are supported:

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

a) In the **AAA Attribute** field, enter the appropriate attribute for your use case, as described in the preceding tables.
b) Click **Update**.

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

Configure these settings only if you want to swap the current primary or secondary AAA servers or define different AAA servers. Click the menu icon (≡) and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers** to open the **Authentication and Policy Servers** window.

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

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

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

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

Table 5: Cisco ISE Server Settings

Name	Description
Shared Secret	Key for device authentications. The shared secret can contain up to 100 characters. The shared secret must be provided before the AAA address can be updated.
Username	Name that is used to log in to the Cisco ISE CLI.
Password	Password for the Cisco ISE CLI username.
FQDN	Fully qualified domain name (FQDN) of the Cisco ISE server. The FQDN consists of two parts, a hostname and the domain name, in the following format: *hostname.domainname.com* For example, the FQDN for a Cisco ISE server might be ise.cisco.com.
Subscriber Name	A unique text string—for example, `acme`—that is used during Cisco DNA Center-to-Cisco ISE integration to set up a new pxGrid client in Cisco ISE.
Virtual IP Address(es)	Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

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

Table 6: AAA Server Advanced Settings

Name	Description
Protocol	TACACS or RADIUS.
Authentication Port	Port used to relay authentication messages to the AAA server. • For RADIUS, the default is UDP port 1812. • For TACACS, the port is 49 and cannot be changed.

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

e) Click **Update**.

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, see the "Configure Authentication Policies" topic.

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

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

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

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

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

Enable Two-Factor Authentication Using RADIUS

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

Step 1 Integrate Cisco ISE with 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.

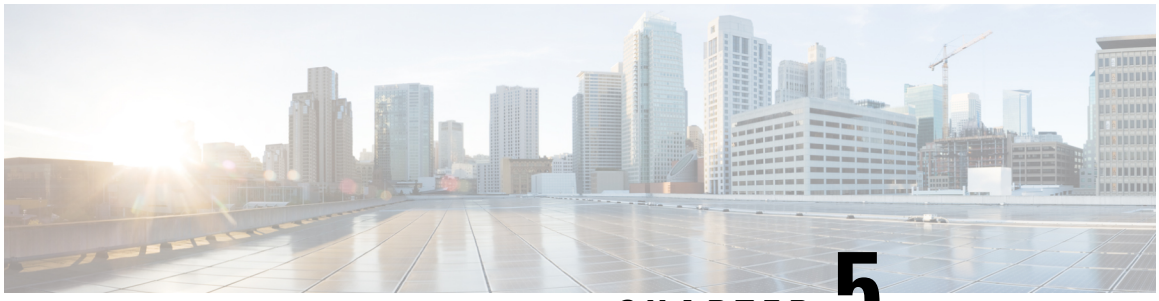
Step 4 Click **Log In**.

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 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 5

Manage Licenses

This chapter contains the following topics:

- License Manager Overview, on page 111
- Integration with Cisco Smart Accounts, on page 115
- Set Up License Manager, on page 115
- Visualize License Usage and Expiration, on page 116
- View Historical Trends for License Consumption, on page 117
- View License Details, on page 118
- Change License Level, on page 119
- Export License Information, on page 120
- Auto Registration of Smart License-Enabled Devices, on page 120
- Day 0 Configuration for Smart License-Enabled Devices, on page 120
- Apply Specific License Reservation or Permanent License Reservation to Devices, on page 121
- Cancel SLR or PLR Applied to Devices, on page 123
- Install the Authorization Code and Enable the High Security License, on page 123
- Disable High Security License, on page 124
- Upload Resource Utilization Details to CSSM, on page 125
- Change Device Throughput, on page 126
- Transfer Licenses Between Virtual Accounts, on page 126
- Manage Customer Tags to Smart License-Enabled Devices, on page 126
- Modify License Policy, on page 127

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. 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).

- **Licenses**: 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.
- **Devices**: The **Devices** table shows the license type, license expiry, license mode, virtual account, associate site, and registrations status of each device managed by Cisco DNA Center.
- **Reporting**: 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** work flow.
- **Sync Status**: In a table, the Smart License Policy (SLP) compliance shows the devices and timeline graph of license usage reports sent from Cisco DNA Center to CSSM. You can filter the devices based on their status and export the compliance report in CSV or PDF format.
- **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
Filter	Click **Filter** to specify one or more filter values and then click **Apply**. You can apply multiple filters. To remove a filter, click the **x** icon next to the corresponding filter value.
Change Cisco DNA License	Select one or more licenses and choose **Actions** > **Change Cisco DNA License** to change the level of a selected 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 Change License Level, on page 119.
Change Virtual Account	Select one or more licenses and choose **Actions** > **Change Virtual Account** to specify the Virtual Account used to manage these licenses.
Manage Smart License > **Register**	Select one or more Smart License-enabled devices and choose **Actions** > **Manage Smart License** > **Register** to register the Smart License-enabled devices.
Manage Smart License > **Deregister**	Select one or more Smart License-enabled devices and choose **Actions** > **Manage Smart License** > **Deregister** to unregister the Smart License-enabled devices.
Manage License Reservation > **Enable License Reservation**	Choose the device for which you want to apply Specific License Reservation (SLR) or Permanent License Reservation (PLR), then choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.

Control	Description
Manage License Reservation > Update License Reservation	The device must be in SLR registered state. You can update the SLR applied to a wireless device or switch with a wireless controller package. Choose the device for which you want to update SLR, then choose **Actions** > **Manage License Reservation** > **Update License Reservation**.
Manage License Reservation > Cancel/Return License Reservation	Choose the device and choose **Actions** > **Manage License Reservation** > **Cancel/Return License Reservation** to cancel or return the SLR or PLR applied to the device.
Manage License Reservation > Factory License Reservation	Choose the device and choose **Actions** > **Manage License Reservation** > **Factory License Reservation** to enable the factory-installed SLR on the device.
Recent Tasks	Click **Recent Tasks** to see a list of all 50 of the most recently performed Cisco DNA Center tasks. Use the drop-down to filter the list to show only those tasks with a status of **Success**, **Failure**, or **In Progress**.
License Usage	Click **License Usage** to see the license utilization percentage for all types of licenses.
Refresh	Click **Refresh** to reload the window with current data.
Export	Click **Export** to export the list of displayed licenses as a CSV file. For more information, see Export License Information, on page 120.
Find	Enter a search term in the **Find** field to find all licenses in the list that have that term in any column. Use the asterisk (*) character as a wildcard anywhere in the search string.
Show Entries	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). For more information, see View License Details, on page 118.
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.

Column	Description
Purchased Licenses: Network/Legacy	The total number of purchased Network (or Legacy) perpetual licenses for the devices in this product series.
Used Licenses	The total number of Cisco DNA Center subscription licenses applied to the devices in this product series.
Used Licenses: Network/Legacy	The total number of Network perpetual licenses for the devices in this product series.
Feature Licenses (applicable only for Routers)	The number of licenses purchased for specific features such as security, AVC, and so on.

Table 9: All License Information

Column	Description
Device Name	Name of the device. For more information, see View License Details, on page 118.
Device Family	The category of the device, such as Switches and Hubs, as defined by Cisco DNA Center.
IP Address	IP address of the device.
Device Series	The full name of the Cisco product series to which the listed device belongs (for example, Cisco Catalyst 3850 Series Ethernet Stackable Switch).
Cisco DNA License	The Cisco DNA Center license level.
Cisco DNA License Expiry	The expiration date of the Cisco DNA Center license.
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 the 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	The last time this entry in the table was updated.
MAC Address	The MAC address of the licensed device.
Term	The total term during which the 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 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 Click the menu icon (☰) and choose **System** > **Settings** > **Smart Account**.

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

Step 6 Click **Save**.

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

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

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

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

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

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

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

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

What to do next

Register the 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 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**, **Licenses**, or **Reporting**.

The **License Usage** pie chart at the top of the window displays the aggregate number of purchased licenses and the number of licenses currently in use for the device category 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 Historical Trends for License Consumption

The Cisco DNA Center allows you to view the historical trends for all purchased and consumed license consumptions in CSSM on a daily, weekly and monthly basis. CSSM stores the historical information up to 1 year.

Before you begin

Cisco DNA Center must be registered to a particular smart account in Cisco Smart Software Management (CSSM). For more information, see Integration with Cisco Smart Accounts, on page 115.

Step 1 Click the menu icon (☰) and choose **Tools** > **License Manager** > **Licenses**.

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

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

A license details slide-in pane appears that displays the complete license details and license history of the chosen device.

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

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

The available frequencies are:

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

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

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

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

View License Details

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

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

Step 1 Click the menu icon (☰) and choose **Tools** > **License Manager** > **Devices**.

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

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

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

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

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

- **Customize**: Click ⋮ 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 when the license level change is complete. You can choose not to reboot with the license change, but you will need to schedule the reboot for later, or your license level change will not be applied.

Step 1 Click the menu icon (☰) and choose **Tools** > **License Manager** > **Devices**.

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

Step 2 Use **Find** or scroll through the table to find the devices whose license level you want to change. If you are having trouble finding the device you want, or want to select multiple devices, follow the tips in View License Details, on page 118 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 that you want to change.

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

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

To continue:

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

zone of the site where the device is located, click **Site Settings**. When you are finished specifying the schedule parameters, click **Confirm**.

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 Click the menu icon (☰) and choose **Tools** > **License Manager**.

Step 2 Click **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 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 Click the menu icon (☰) and choose **Tools** > **License Manager** > **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 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 121.

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 122.

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

Step 1 Click the menu icon (☰) and choose **Tools** > **Licenses** > **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 Click the menu icon (☰) and choose **Tools** > **Licenses** > **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 Click the menu icon (☰) and choose **Tools** > **Licenses** > **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

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

Before you begin

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

Step 1 Click the menu icon (☰) and choose **Tools** > **License Manager**.

Step 2 Click the **Reporting** 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 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 **Review Device Features** window, click **Next**.

Step 11 In the **Installing Device Features** window, view the authorization code and HSEC installation status and click **Next**.

Step 12 In the **Sync Data with Cisco** window, click **Next**.

Step 13 The **Summary** window displays the authorization code and HSEC installation status.

Step 14 Click **Finish**.

Disable High Security License

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

Step 1 Click the menu icon (☰) and choose **Tools** > **License Manager**.

Step 2 Click the **Reporting** 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 disable the High Security license and click **Next**.

Step 8 In the **Policy Settings** window, click **Next**.

Step 9 In the **Choose Device Features** window, do the following:

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

Step 10 In the **Review Device Features** window, click **Next**.

Step 11 In the **Installing Device Features** window, view the HSEC disable operation status and click **Next**.

Step 12 In the **Sync Data with Cisco** window, click **Next**.

Step 13 The **Summary** window displays the HSEC disable operation status.

Step 14 Click **Finish**.

Upload Resource Utilization Details to CSSM

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

Step 1 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 **Modify Policy** window. To modify the scheduled reporting frequency, do the following:

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

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

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

c) Click **Save**.

Step 9 In the **Sync Data with Cisco** window, click **Next**.

The **Summary** window shows the status of operations that are performed in this workflow.

Step 10 Click **Finish**.

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

What to do next

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

Change Device Throughput

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

Step 1 Click the menu icon (☰) and choose **Tools** > **License Manager**.

Step 2 Click the **Reporting** tab.

The **Reporting** window displays a table listing all your Smart License-enabled devices and their licenses.

Step 3 Choose the device that you want to change.

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

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

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

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

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

Manage Customer Tags 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 Click the menu icon (☰) and choose **Tools** > **License Manager**.

Step 2 Click the **Reporting** tab.

The **Reporting** 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 network devices report their feature usage to CSSM.

Step 1 Click the menu icon (☰) and choose **Tools** > **License Manager**.

Step 2 Click the **Reporting** tab.

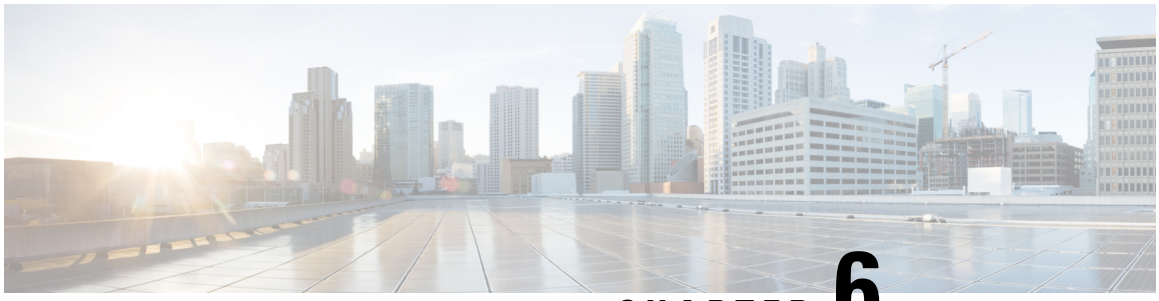
Step 3 In the **Smart License** table, click **Modify Policy**.

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 6

Backup and Restore

- About Backup and Restore, on page 129
- Backup Server Requirements, on page 131
- Backup Storage Requirements, on page 134
- Example of NFS Server Configuration—Ubuntu, on page 134
- Example of NFS Server Configuration—CentOS, on page 135
- Configure Firewall Rules to Allow NFS, on page 136
- Configure Backup Servers, on page 137
- Back Up Data Now, on page 138
- Schedule Data Backups, on page 140
- Restore Data from Backups, on page 141

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 or delete 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 131.

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 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 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 release with the same first four digits and the same application versions as the appliance from which the backup was taken. To view the current applications and versions, choose **System** > **Software Management** and click **Currently Installed Applications**.

You can restore a backup to a 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 and Restore Event Notifications

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

A notification is generated and sent whenever one of the events listed in the following table occur:

Operation	Event
Backup	The process to create a backup file for your system has started.
	A backup file was successfully created for your system.
	A backup file could not be created for your system. This typically happens because: • The necessary disk space is not available on remote storage. • You are unable to fetch the status of your system's NFS server, which is a precheck for the backup operation. • You encountered connectivity issues or latency while creating a backup file on your system's NFS server.
Restore	The process to restore a backup file has started.
	The restoration of a backup file was successful.
	The restoration of a backup file failed. This typically happens because: • The backup file has become corrupted. • You encountered connectivity issues or latency while creating a backup file on your system's NFS server.

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.
- *(Not applicable to RedHat 7/CentOS 7)* The C.UTF-8 locale must be installed. To confirm whether C.UTF-8 is installed, enter:

```
# localectl  list-locales | grep -i c.utf
C.utf8
en_SC.utf8
```

- The backup user must own the destination folder for the backup or have read-write permissions for the user's group. For example, assuming the backup user is *backup* and the user's group is *staff*, 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 SFTP subsystem path depends on which Ubuntu release is installed. For the latest Ubuntu release, the following line must be uncommented and present in the SSHD configuration:

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

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

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

Server Requirements for Assurance Backup

To support Assurance data backups, the server must be a Linux-based NFS server that meets 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.
- Have the C.UTF-8 locale installed. To confirm whether C.UTF-8 is installed, enter:

  ```
  # localectl  list-locales | grep -i c.utf
  C.utf8
  en_SC.utf8
  ```

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.

Requirements for Multiple Cisco DNA Center Deployments

If your network includes multiple Cisco DNA Center clusters, you cannot use the same backup location for automation and Assurance backups. For multiple Cisco DNA Center deployments, the best practice is to separate the backup directory structure for each Cisco DNA Center cluster. The following example configuration shows how to separate your backup directory structure.

Resource	Example Configuration
Cisco DNA Center clusters	1. *cluster1* 2. *cluster2*
Backup server hosting automation and Assurance backups	The example directory is `/data/`, which has ample space to host both types of backups.
Directory ownership and permissions	Earlier in this section, see "Server Requirements for Automation Data Backup."
Directory ownership and permissions	Earlier in this section, see "Server Requirements for Assurance Backup."
NFS export configuration	The content of the `/etc/exports` file: `/data/assurance/cluster1 *(rw,sync,no_subtree_check,all_squash) /data/assurance/cluster2 *(rw,sync,no_subtree_check,all_squash)`

Requirements When Migrating to New Cisco DNA Center Hardware

If you upgrade your Cisco DNA Center cluster to new hardware or you replace your existing cluster hardware as part of the return materials authorization (RMA) process, use a different directory structure for the backup after restoring from the existing backup location.

Note If you replace one or two nodes from an existing three-node cluster, there is no need to change the backup directory structure.

Backup Server Directory Layout

To simplify backups, we recommend that you use the following directory layout for your backup server:

Single Cisco DNA Center Cluster Deployment

- Full backup (Automation and Assurance):
  - cluster1: /data/automation/cluster1
  - cluster1: /data/assurance/cluster1
- Automation-only backup:

  cluster1: /data/automation/cluster1

Multiple Cisco DNA Center Cluster Deployment

- Full backup (Automation and Assurance):
  - cluster1: /data/automation/cluster1

- cluster1: /data/assurance/cluster1
- cluster2: /data/automation/cluster2
- cluster2: /data/assurance/cluster2

- Automation-only backup:
  - cluster1: /data/automation/cluster1
  - cluster2: /data/automation/cluster2

Backup Storage Requirements

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 GB = 250 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 apt-get 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 automation backup server. If you plan to back up both automation and Assurance data, you need to configure the Cisco DNA Center automation 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 93.
- The server that you plan to use for data backups must meet the requirements described in Backup Server Requirements, on page 131.

Step 1 Click the menu icon (☰) and choose **System** > **Backup & Restore** > **Configure**.

Step 2 To configure the automation 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. 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 do the following:

a) 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.

b) 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 93.
- Backup servers meet the requirements described in Backup Server Requirements, on page 131.
- Backup servers have been configured in Cisco DNA Center. For information, see Configure Backup Servers, on page 137.

Step 1 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 137.

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 93.
- Backup servers meet the requirements described in Backup Server Requirements, on page 131.
- Backup servers have been configured in Cisco DNA Center. For information, see Configure Backup Servers, on page 137.

Step 1 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**.

Choose the days and time for scheduling the backup.

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 automation data only.

Step 6 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 release with the same first four digits and the same application versions as the appliance from which the backup was taken. To view the current applications and versions, choose **System** > **Software Management** and click **Currently Installed Applications**.
- 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 93.
- 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 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.

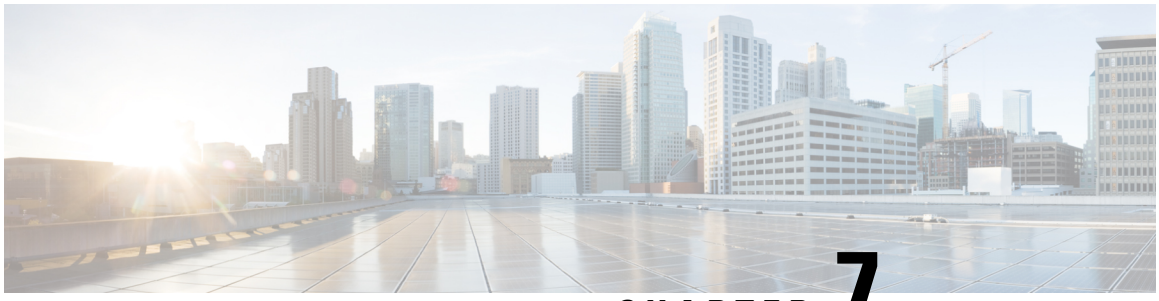
Step 3 In the **Actions** column, choose **Restore**.

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 7

Implement Disaster Recovery

- Overview, on page 143
- Prerequisites, on page 148
- Install the Witness Site, on page 153
- Configure Disaster Recovery, on page 155
- Upgrade a Disaster Recovery System, on page 170
- Failovers: An Overview, on page 170
- Pause Your Disaster Recovery System, on page 174
- Rejoin Your System, on page 176
- Disaster Recovery System Considerations, on page 178
- Disaster Recovery Event Notifications, on page 180
- Troubleshoot Your Disaster Recovery System, on page 182

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 155.
- **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 148.
- **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 155.
- **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 A message will indicate when you are currently viewing your system's standby site. You need to initiate all disaster recovery tasks from the active site.

- **Failover**: 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 171.

Important

- After a failover, Assurance restarts and processes a fresh set of data on the new active site. Historical Assurance data from the former active site is *not* migrated over.
- After a failover, the Cisco DNA Center inventory service triggers a full device sync. This can take anywhere from a few minutes to a few hours, depending on the number of devices that are managed. As is the case when Cisco DNA Center's normally scheduled device sync is running, you will not be able to provision devices on the newly activated cluster until the device sync triggered by a failover completes.

- **Isolate**: During a failover, the former active site is separated from the disaster recovery system. 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 174.
- **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).

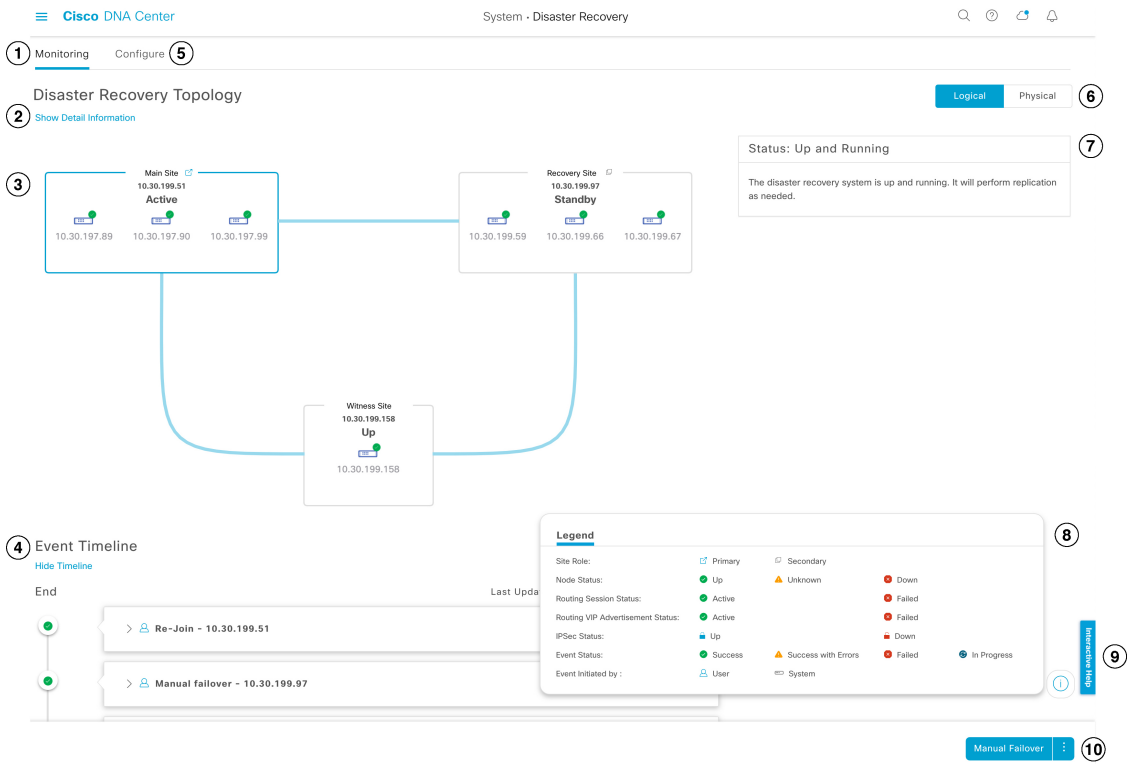
Either a full or incremental replication of data takes place, depending on which of the following scenarios is applicable:

- **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.



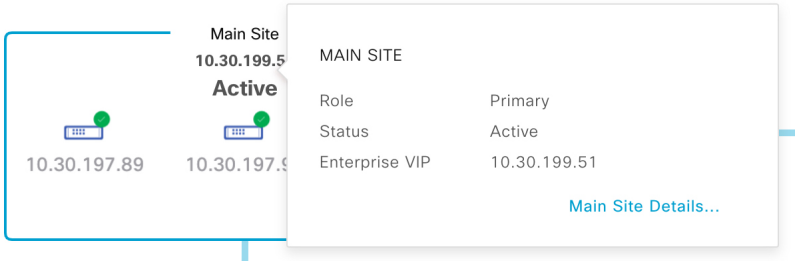
Callout	Description
1	**Monitoring** tab: Click to do the following: • View a topology of the sites that make up your system. • Determine the current status of your system. • Perform disaster recovery tasks. • View a listing of the tasks that have been completed to date.
2	**Show Detail Information** link: Click to open the **Disaster Recovery System** slide-in pane. See View Disaster Recovery System Status, on page 147 for more information.

Callout	Description
3	**Topology**: Displays either a logical or physical topology of your system that indicates the current status of your sites and their members. • In both the logical and physical topologies, a blue box indicates the site that's currently acting as your system's active site. • In the logical topology, a blue line indicates that the IPSec tunnel connecting two sites is operational, and a red line indicates that the tunnel is currently down. • To view a description of the possible site states, see System and Site States, on page 166.
4	**Event Timeline**: Lists every disaster recovery task that is currently in progress or has been completed for your system. For more information, see Monitor the Event Timeline, on page 164.
5	**Configure** tab: Click to enter the settings necessary to establish a connection between your disaster recovery system's sites. See Configure Disaster Recovery, on page 155 for more information.
6	**Logical** and **Physical** tabs: Click the appropriate tab to toggle between a logical and physical topology of your system.
7	**Status** area: Indicates the current status of your system. To view a description of the possible system states, see System and Site States, on page 166.
8	**Legend**: Indicates what the topology icons represent. To view the legend, click in the bottom right corner of the **Disaster Recovery** page.
9	**Interactive Help** button: Click to open a slide-in pane that provides links to walkthroughs that provide on-screen guidance to help you complete specific tasks in Cisco DNA Center.
10	**Action** area: Displays the disaster recovery tasks that are currently available for you to initiate. The tasks you can choose from vary, depending on whether you have configured your sites and your system's status.

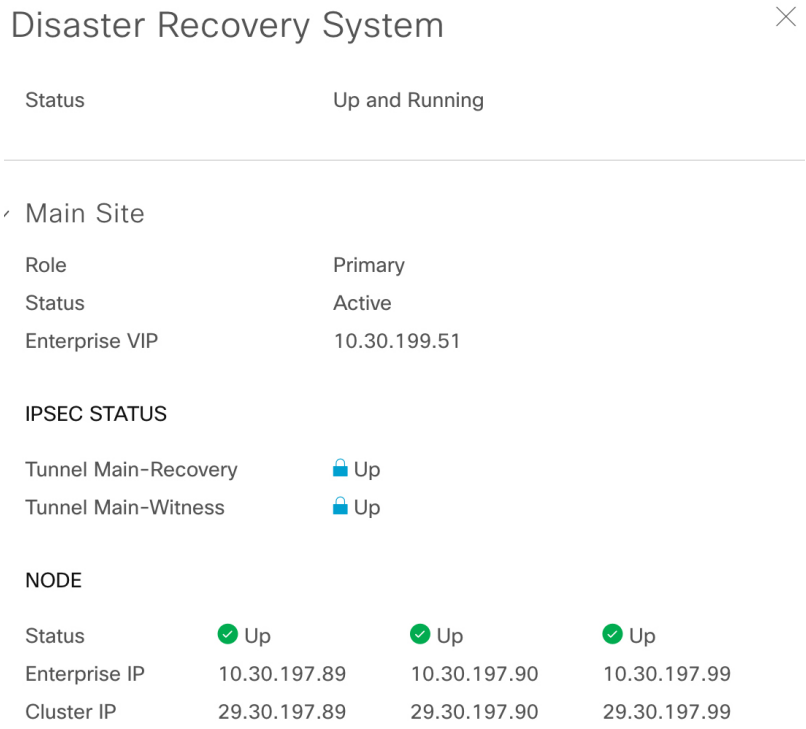
View Disaster Recovery System Status

The topology provides a graphical representation of your disaster recovery system's current status. If you want to view this information in a tabular format, you can do so in the **Disaster Recovery System** slide-in pane. To open this pane, do one of the following:

- Click the **Show Detail Information** link. Then expand the site whose status you want to view in the slide-in pane.
- In the topology, place your cursor over a site's Enterprise virtual IP address or a particular node's icon. In the dialog box that opens, click the link in the bottom right-hand corner of the window.



The slide-in pane opens with the relevant site's information displayed.



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 this version of Cisco DNA Center, you must complete several steps to ensure that disaster recovery works properly after the upgrade. See Configure Disaster Recovery on an Upgraded Cisco DNA Center Appliance, on page 152 for more information.
- Note that disaster recovery does not support IPv6.

General Prerequisites

- Cisco DNA Center supports two disaster recovery setups:
  - **1+1+1 setup**: One Cisco DNA Center appliance functions as your Main Site, a second appliance serves as your Recovery Site, and a third system (residing on a virtual machine) acts as your Witness Site. The following appliances and versions support this setup:
    - DN1-HW-APL/DN2-HW-APL (44-Core appliance): Cisco DNA Center 2.2.2.x and later
    - DN2-HW-APL-L (56-Core appliance): Cisco DNA Center 2.2.1.x and later
    - DN2-HW-APL-XL (112-Core appliance): Cisco DNA Center 2.2.1.x and later
  - **3+3+1 setup**: One three-node Cisco DNA Center cluster functions as your Main Site, a second three-node cluster serves as your Recovery Site, and a third system (residing on a virtual machine) acts as your Witness Site. The following appliances and versions support this setup:
    - DN1-HW-APL/DN2-HW-APL (44-Core appliance): Cisco DNA Center 2.2.2.x and later
    - DN2-HW-APL-L (56-Core appliance): Cisco DNA Center 2.1.2.x and later
    - DN2-HW-APL-XL (112-Core appliance): Cisco DNA Center 2.1.2.x and later
- 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 Advanced Install Configuration Wizard" topic.
- You have assigned a super-admin user to carry out disaster recovery tasks. Only users with this privilege level can access this functionality.
- You have confirmed that the links connecting the following sites are one GB links with 350 ms RTT latency (at most).
  - Main and recovery sites
  - Main and witness sites
  - Recovery and witness sites
- You have opened all of the ports listed in the Cisco DNA Center Security Best Practices Guide's "Disaster Recovery Ports" topic.

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:

Supported Cisco DNA Center Appliances	Cisco Part Numbers
First and second generation 44-core appliance	• DN1-HW-APL • DN1-HW-APL-U • DN2-HW-APL • DN2-HW-APL-U
Second generation 56-core appliance	• DN2-HW-APL-L • DN2-HW-APL-L-U
Second generation 112-core appliance	• DN2-HW-APL-XL • DN2-HW-APL-XL-U

Also ensure that your main and recovery site are running the same Cisco DNA Center version.

- 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.

Important This is applicable to three-node setups only.

- You have generated one third-party certificate and installed the same 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.

- The main site's Enterprise VIP is reachable from the recovery site's Cisco DNA Center cluster.
- The recovery site's Enterprise VIP is reachable from the main site's Cisco DNA Center cluster.
- Ensure that all of the IP addresses (especially the Enterprise port's virtual IP address) and fully qualified domain names (**FQDN**) that the main and recovery sites use are included in this certificate. Also ensure that **digitalSignature** is specified for the certificate's **keyUsage** parameter. For a description of how to generate a third-party certificate, see Generate a Certificate Request Using Open SSL in the *Cisco DNA Center Security Best Practices Guide*.
- Ensure that the main and recovery site have the same Federal Information Processing Standards (FIPS) mode setting. If FIPS mode is enabled on one site and disabled on the other, the registration of your disaster recovery system will fail due to a validation error. For more information on FIPS mode, see the description of the **IP addressing mode used for the services** screen (located in the Cisco DNA Center Second-Generation Appliance Installation Guide's "Configure the Primary Node Using the Maglev Wizard" topic).

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

  Interior BGP (iBGP) Configuration Example

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

  where:

  - `64555` is the neighbor router'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 DENY_ALL out
  !
  ip prefix-list DENY_ALL seq 5 deny 0.0.0.0/0 le 32
  !
  route-map DENY_ALL permit 10
  match ip address prefix-list DENY_ALL
  ```

Witness Site Prerequisites

- You have confirmed that the virtual machine that hosts your witness site is running (at a minimum) VMware ESXi hypervisor version 7.0 or later with a 2.1-GHz core and two virtual CPUs, 4 GB of RAM, and 10 GB of hard drive space.
- Witness site deployment in a public cloud is not supported.
- You have set up your witness site in a different location than your main and recovery sites and confirmed that it is reachable from both of these sites.

- You have configured an NTP server that is accessible by the witness site. You must synchronize this NTP server with the NTP servers that are used by the main and recovery sites.

Configure Disaster Recovery on an Upgraded Cisco DNA Center Appliance

To successfully configure disaster recovery after upgrading your system to the latest Cisco DNA Center version, complete the following steps:

Step 1 Install the Witness Site, on page 153.

Step 2 Configure Disaster Recovery, on page 155.

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 72).
- For more information about the disaster recovery certificate requirements, reference the Security Best Practices Guide.

Step 1 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:

a) Import the certificate by dragging and dropping the PEM file into the highlighted area.

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

After the upload succeeds, the system certificate is validated.

b) In the **Private Key** area, import the private key by dragging and dropping it into the highlighted area.

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

After the upload succeeds, the private key is validated.

c) Specify whether the private key will be encrypted by clicking the appropriate radio button.
d) If the private key will be encrypted, enter its password in the **Password** field.

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

a) Import the certificate by dragging and dropping the PKCS file into the highlighted area.

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

After the upload succeeds, the system certificate is validated.

b) In the **Password** field, enter the certificate's password (a PKCS requirement).
c) Specify whether the private key will be encrypted by clicking the appropriate radio button.
d) If the private key will be encrypted, enter its password in the **Password** field.

Step 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.

Install the Witness Site

Complete the following procedure to set up 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:

a) Open https://software.cisco.com/download/home/286316341/type.

Note You need a Cisco.com account to access this URL. See the following page for a description of how to create an account: https://www.cisco.com/c/en/us/about/help/registration-benefits-help.html

b) In the **Select a Software Type** area, click the Cisco DNA Center software link.

The **Software Download** page updates, listing the software that's available for the latest Cisco DNA Center release.

c) 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 7.0 or later.

Step 3 From the vSphere client, choose **File** > **Deploy OVF Template**.

Step 4 Complete the **Deploy OVF Template** wizard:

a) Do the following in the wizard's **Source** screen:

1. Click **Browse**.
2. Navigate to the witness site's OVF package (.ova).
3. Click **Open**.
4. 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.

b) Click **Next >**.

c) 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.

d) Click the host or cluster on which you want to run the deployed template and then click **Next >**.

The wizard's **Storage** screen opens.

e) 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.

Note Later, if you need to change the password configured for the **maglev** user on the witness site's VM, use the standard Linux **passwd** utility. You don't need to pause the disaster recovery system before doing this, and the password change will have no functional impact on disaster recovery operation.

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:

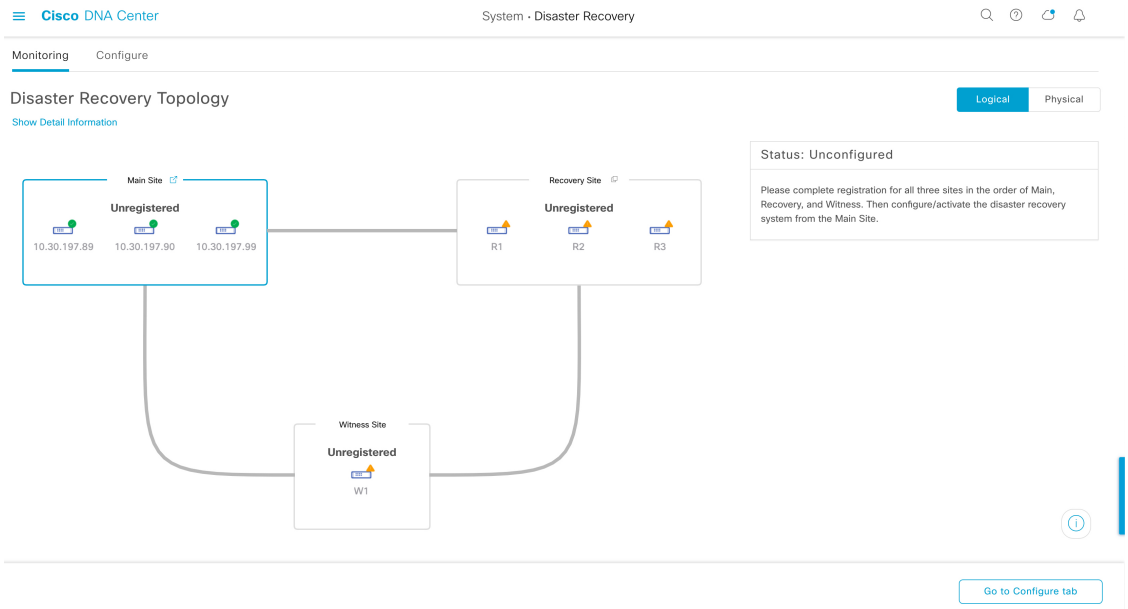
- You can specify a virtual IP address that uses Border Gateway Protocol (BGP) route advertising.
- You can choose to not configure a virtual IP address. If you choose this option, you must enable device controllability so that a site's virtual IP address can be reconfigured after a failover occurs. For more information, see Device Controllability, on page 47.

Before you begin

Assurance data (Elasticsearch), as well as your deployment's backup schedule and proxy server configuration, are not replicated after a failover. For the clusters where your disaster recovery system's main and recovery sites will reside, do the following *before* configuring your system:

- Configure a separate NFS device for each site.
- Configure the same backup schedule.
- Configure the same proxy server.

Step 1 Click the menu icon (☰) and choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

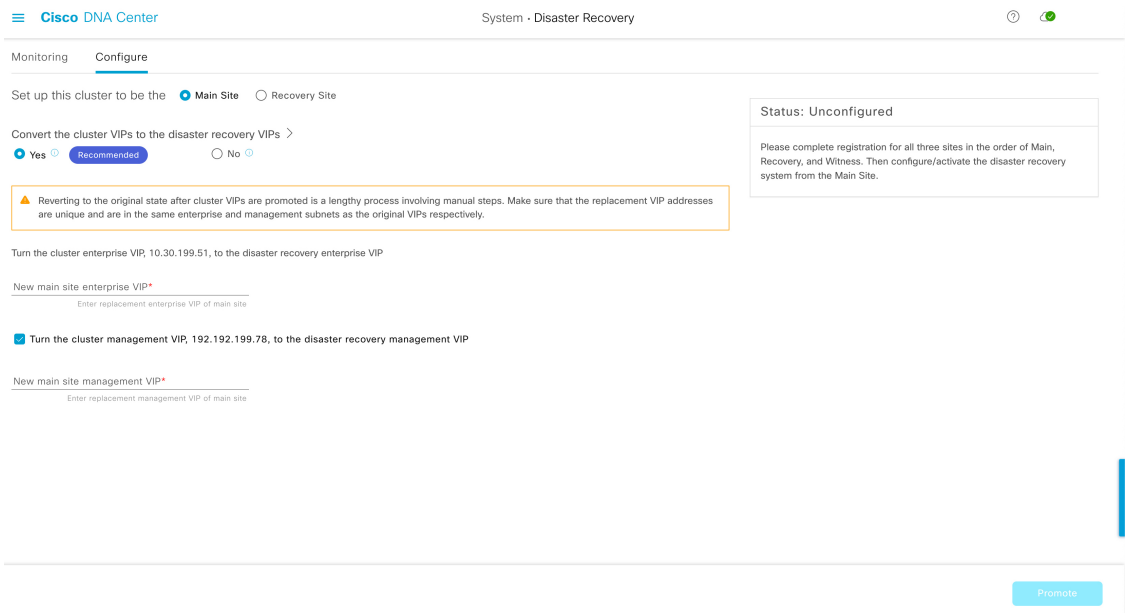


The **Monitoring** tab is selected, by default.

Step 2 Register your main site:

a) Click the **Configure** tab.

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



b) In the **Convert the cluster VIPs to the disaster recovery VIPs** area, click one of the following radio buttons:

- Click **Yes** to set up a cluster as the main site and automatically propagate virtual IP address changes to the devices that are connected to this cluster. This is accomplished by promoting the virtual IP addresses that are currently configured for the cluster and assigning them as your disaster recovery system's global virtual IP addresses. We recommend choosing this option if you are enabling disaster recovery on a cluster that has a lot of connected

devices. Otherwise, these devices will need to be reconfigured to communicate with the new disaster recovery virtual IP address. If you choose this option, do the following:

1. In the **New main site enterprise VIP** field, enter a new virtual IP address for the site's Enterprise network. This will replace the address that is going to be promoted. Ensure that it is a unique address that is not already used and that it resides in the same subnet as the previous virtual IP address.
2. (Optional) Check the **Turn the cluster management VIP, *<IP-address>*, to the disaster recovery management VIP** check box.
3. (Optional) In the **New main site management VIP** field, enter a new virtual IP address for the site's Management network. This will replace the address that is going to be promoted. Ensure that it is a unique address that is not already used and that it resides in the same subnet as the previous virtual IP address.

- Click **No** to set up a cluster as the main site without propagating virtual IP address changes to connected devices. We recommend this option for a brand-new cluster that isn't connected to any devices yet or is only connected to a few devices. If you choose this option, skip ahead to Step 2f.

c) In the **Action** area, click **Promote**.

The **Disaster Recovery VIP Promotion** dialog opens.

d) Click **Continue**.

Cisco DNA Center validates the virtual IP addresses you entered.

e) In the **Details** area, view the validation status:

- If any of the addresses you entered are invalid (likely because it doesn't reside in the same subnet as the address it's replacing), make the necessary corrections and repeat Step 2c.
- If the addresses you entered are successfully validated, the **Details** area lists all of the virtual IP addresses that will be configured for your disaster recovery system. Proceed to the next step.

f) Enter the following information in the **Site VIP/IPs** area:

- **Main Site VIP**: The virtual IP address that manages traffic between the active site's cluster nodes and your Enterprise network. Cisco DNA Center prepopulates this field, based on your system's information.
- **Recovery Site VIP**: The Enterprise virtual IP address that manages traffic between the recovery site's cluster nodes and your Enterprise network.
- **Witness Site IP**: The IP address that manages traffic between the witness site's virtual machine and your Enterprise network.

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

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

g) Click one of the following radio buttons in the **Route advertisement** area:

- **Border Gateway Protocol (BGP)**: This option, which is recommended for most disaster recovery systems, is selected by default. BGP route advertisement ensures that you can access your system's current active site, which is critical after a failover takes place.
- **Disaster recovery VIPs without route advertisement**: Choose this option if you want to configure virtual IP addresses for your system whose routes are not advertised using BGP. This option is suitable for data centers where both the main and recovery sites can access the subnet that the system's global virtual IP addresses reside within.
- **No disaster recovery VIPs**: When this option is selected, the virtual IP addresses that are configured for a site are automatically configured on the devices that belong to that site. Each time a failover takes place, these virtual IP addresses are reconfigured on the devices. Skip ahead to Step 2k.

h) If you clicked either of the first two radio buttons in the previous step, enter a value in the **Enterprise VIP for Disaster Recovery** field.

When configured, this floating virtual IP address automatically moves to and operates on the site that is currently acting as your network's active site. This address manages traffic between your disaster recovery system and your Enterprise network.

Note
- If you clicked the **Border Gateway Protocol (BGP)** radio button and don't want to configure a Management virtual IP address, skip ahead to Step 2j.
- If you clicked the **Disaster recovery VIPs without route advertisement** radio button and don't want to configure a Management virtual IP address, skip ahead to Step 2k.

i) (Optional) Enter a value in the **Management VIP for Disaster Recovery** field.

When configured, this floating virtual IP address automatically moves to and operates on the site that is currently acting as your network's active site. This address manages traffic between your disaster recovery system and your Management network.

j) If you clicked the **Border Gateway Protocol (BGP)** radio button, enter the information required to enable route advertisement:

- In the **Border Gateway Protocol Type** area, specify whether your BGP peers will establish exterior (**Exterior BGP (eBGP)**) or interior (**Interior BGP (iBGP)**) sessions with one another.
- In the **Main Site Router Settings for Enterprise Network** and **Recovery Site Router Settings for Enterprise Network** areas, enter the IP address of the remote router that Cisco DNA Center will use to advertise the Enterprise virtual IP address that's configured for the disaster recovery system's Main and Recovery sites. Also enter the router's remote and local AS numbers.

  Note the following points:

  - Click the **Add** (+) icon if you want to configure an additional remote router. You can configure a maximum of two routers for each site.
  - When entering an AS number, ensure that it's a 32-bit unsigned number that falls within the 1–4,294,967,295 range.
  - When the **iBGP** option is selected, Cisco DNA Center will automatically set the local AS number to the value you enter as the remote AS number.
  - If you configured a Management virtual IP address in the previous step, the **Main Site Router Settings for Management Network** and **Recovery Site Router Settings for Management Network** areas are also

displayed. Enter the appropriate information for the remote router that Cisco DNA Center will use to advertise this virtual IP address.

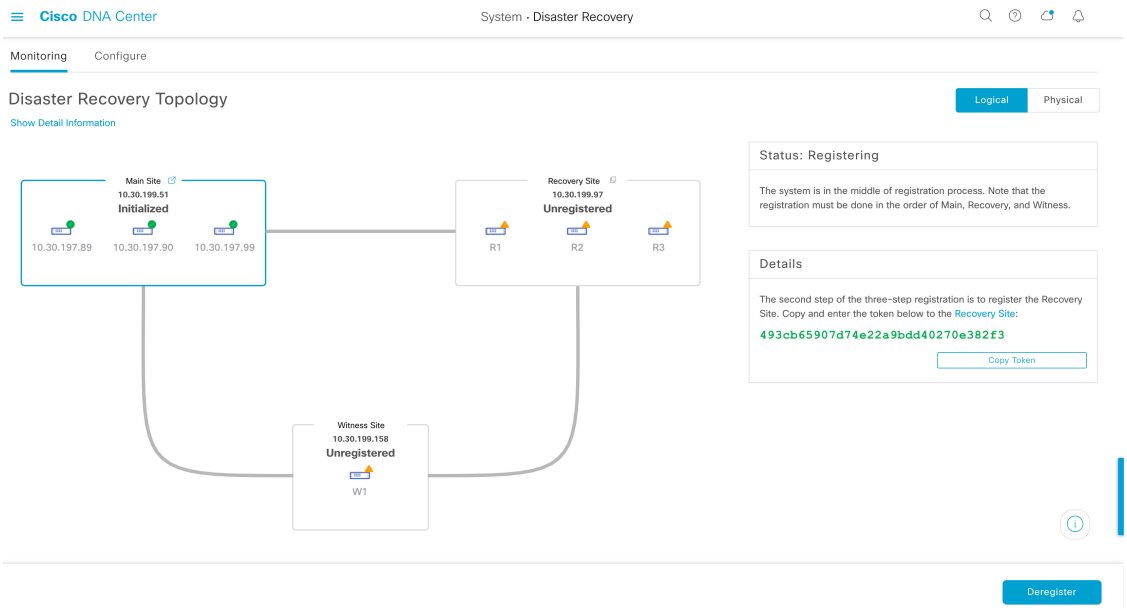
k) From the **Action** area, click **Register**.

The **Disaster Recovery Registration** dialog opens.

l) Click **Continue**.

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

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



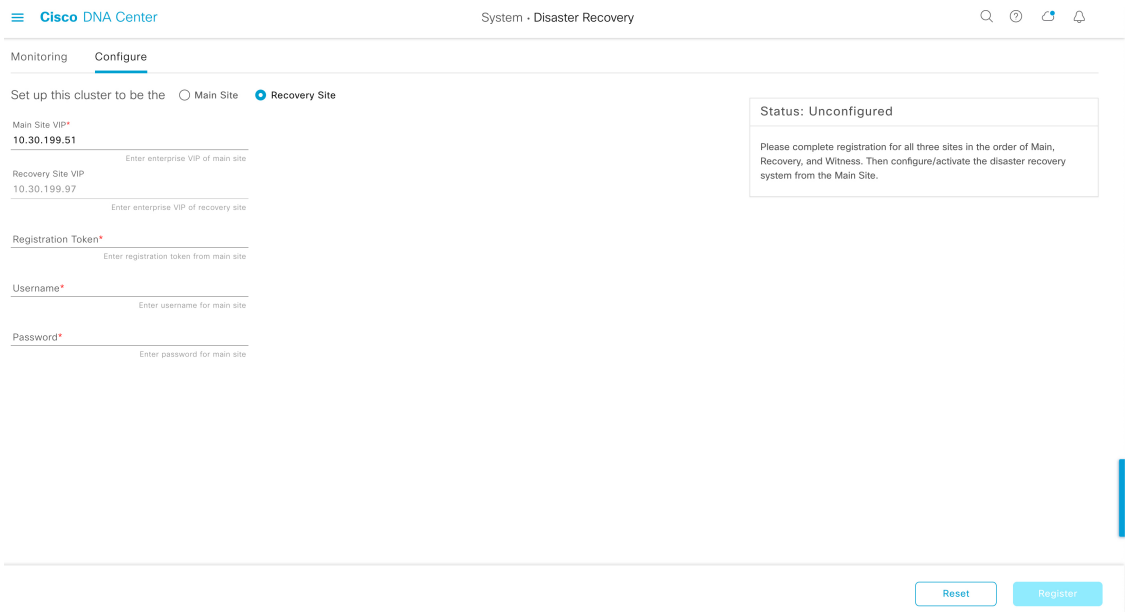
Step 4 Register your recovery site:

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 **Details** 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.



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. Cisco DNA Center prepopulates this field, based on your system's information.

  Note After a IPSec tunnel has been configured between the main and recovery sites, Enterprise traffic on the node(s) hosting the VIP will be sourced via the Enterprise VIP (UDP/TCP/ICMP).

- The registration token 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**.

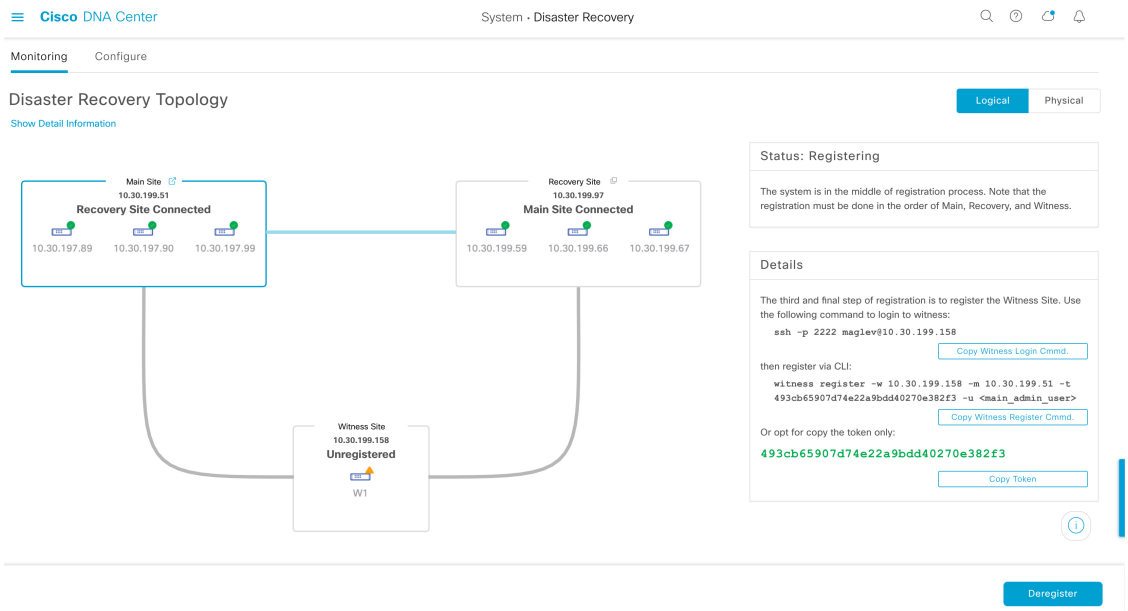
The **Disaster Recovery Registration** dialog opens.

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:

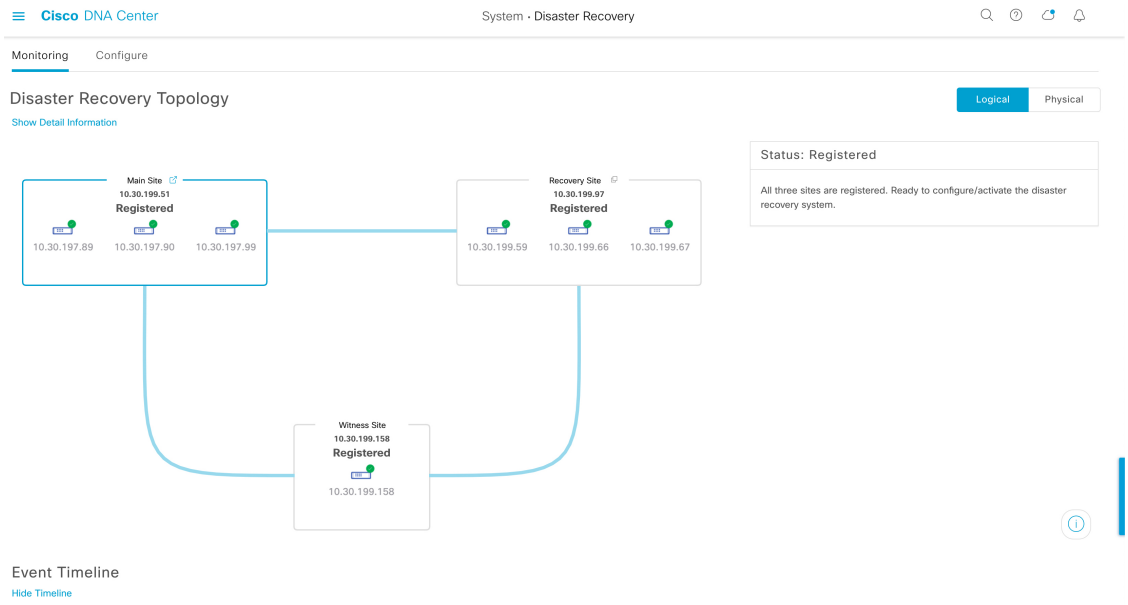
a) Return to the main site's browser tab.



b) From the **Details** 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 **Details** 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.

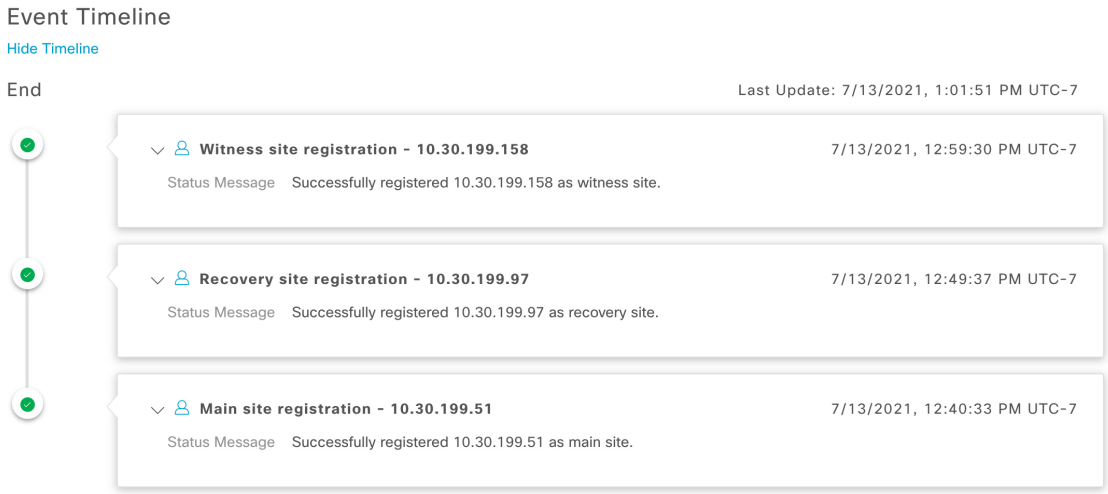
Step 6 Verify that your main, recovery, and witness sites have been registered successfully:

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**.

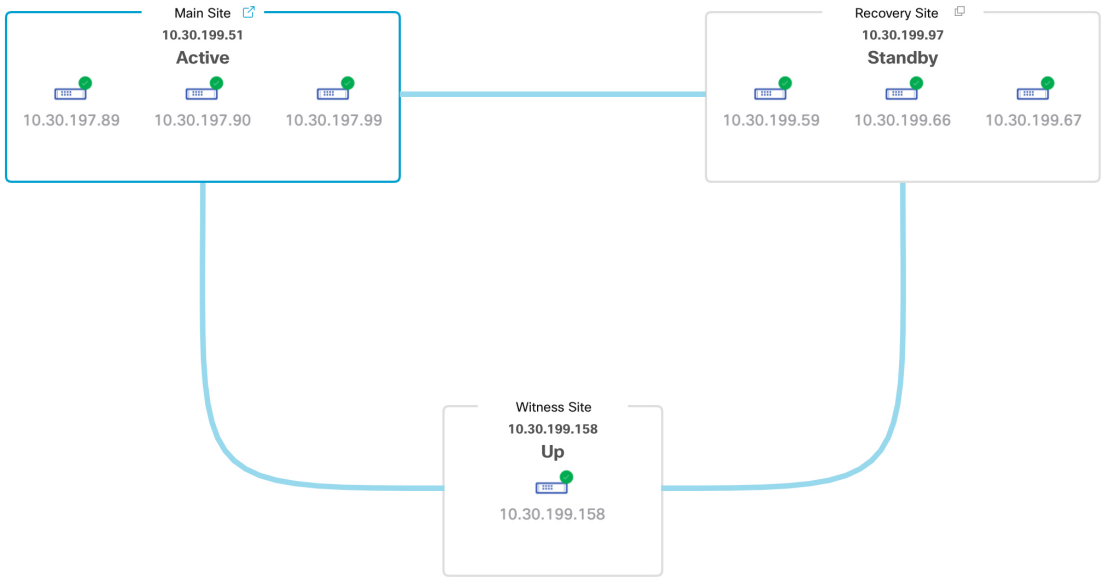
A dialog appears, indicating that all of the data that currently resides in your recovery site will be erased.

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**.

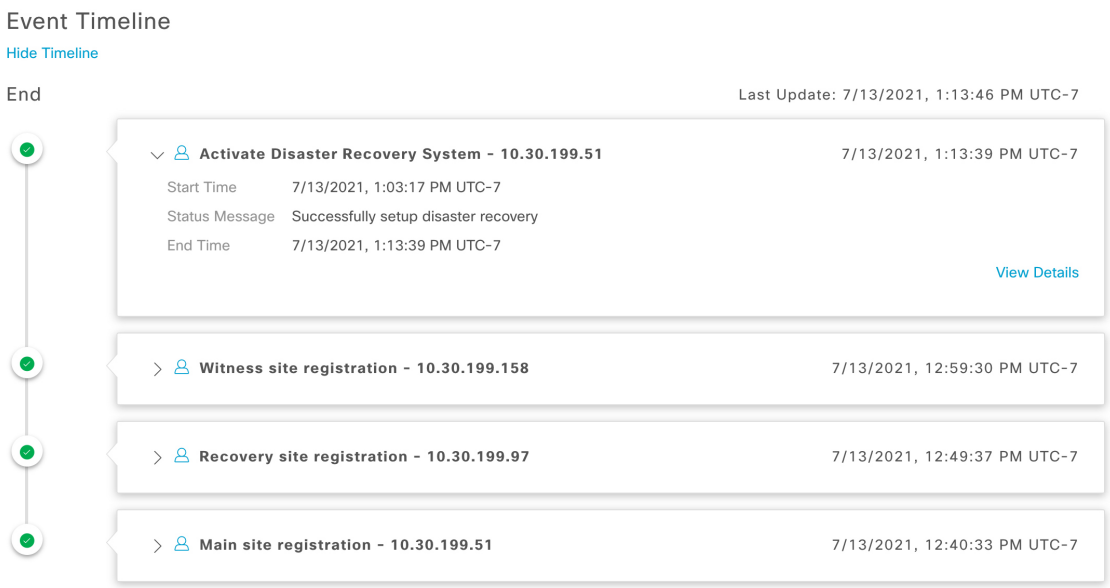
Note The activation process may take some time to complete. View the Event Timeline in order to monitor its progress.

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:



b. View the Event Timeline and confirm that the **Activate Disaster Recovery System** 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:

a) Open an SSH console to the witness site and run the **ssh -p 2222 maglev@***witness-site's-IP-address* command.

b) Enter the default (maglev) user's password.

Note Before you proceed to the next step, note the witness site's IP address. You'll need to configure the same address after you upgrade the witness site. Otherwise, the witness site won't work as expected.

Step 2 Run the **witness reset** command.

Step 3 Delete the current witness site's virtual machine.

Step 4 Install the new witness site's virtual machine, as described in Install the Witness Site, on page 153.

Step 5 Log in to the new witness site:

a) Open an SSH console to the witness site and run the **ssh -p 2222 maglev@***witness-site's-IP-address* command.

b) Enter the default (maglev) user's password.

Step 6 Run the **witness reconnect -w** ***witness-site's-IP-address*** **-m** ***main-site's-Enterprise-virtual-IP-address*** **-u** ***admin-username*** command.

Note the following points:

- Regardless of the main site's current disaster recovery status, use the main site's Enterprise VIP when reconnecting the witness site.
- To verify that the witness site is operational after running this command, do the following:

a. From the Disaster Recovery Topology, click the **Show Detail Information** link to open the **Disaster Recovery System** slide-in pane.

b. In the **Witness Site** section, confirm that the status for the witness site and configured IPSec links is `Up`.

- To view all of the available options for this command, run the **witness reconnect --help** command.

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** to suspend the operation of your system.

See Place Your System on Pause, on page 174 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 155 in order to enter the appropriate settings for your sites, reregister them, and reactivate your system.

Monitor the Event Timeline

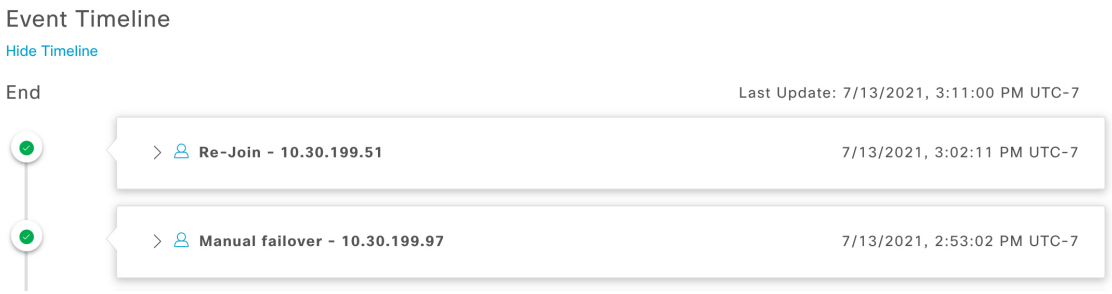
From the Event Timeline, you can track the progress of disaster recovery tasks that are currently running and confirm when these tasks have completed. To view the timeline, do the following:

1. Click the menu icon (☰) and choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

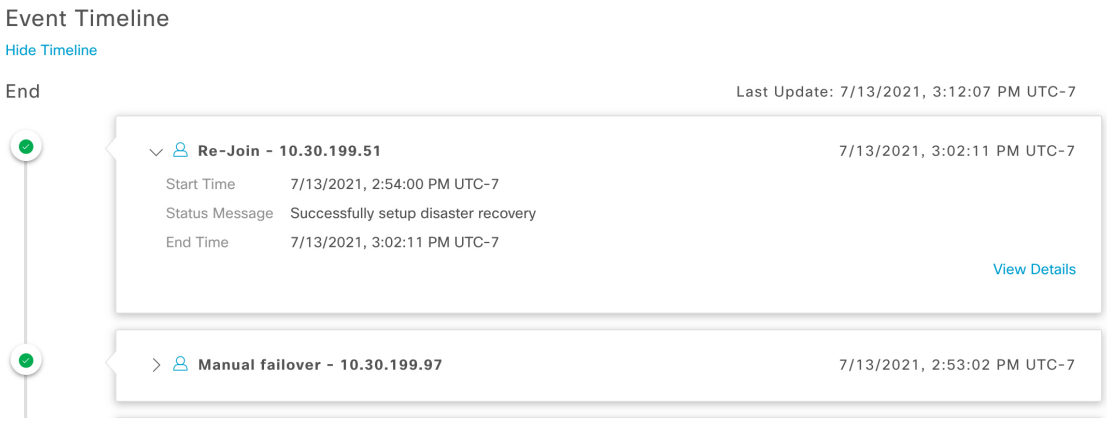
   The **Monitoring** tab is selected, by default.

2. Scroll to the bottom of the page.

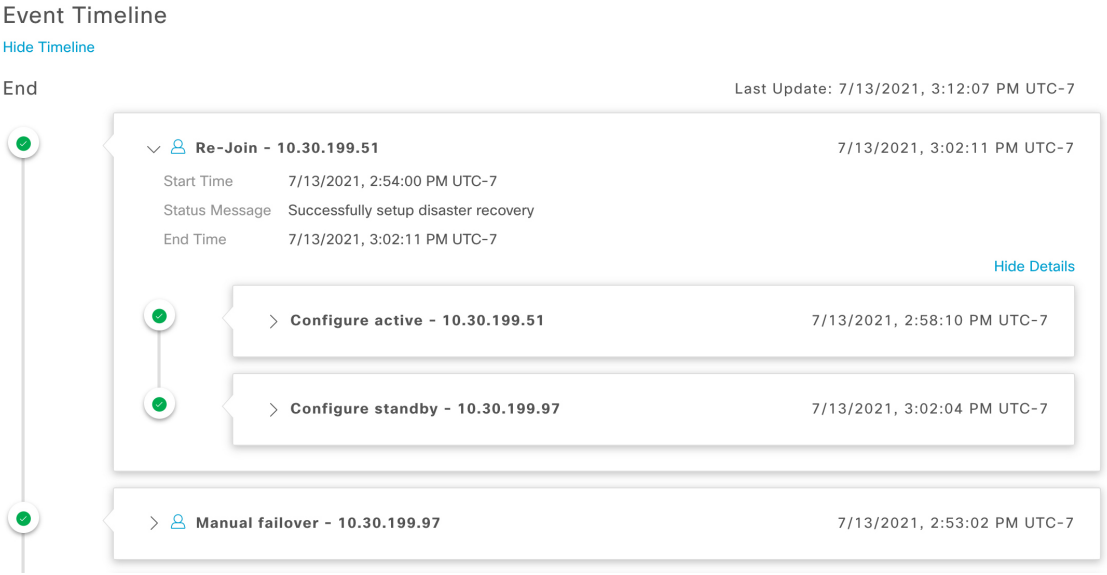
Every task that is in progress or has completed for your system is listed here (in descending order based on their completion timestamp), starting with the most recent task. Cisco DNA Center indicates whether each task was initiated by the system (🖥) or a user (👤).



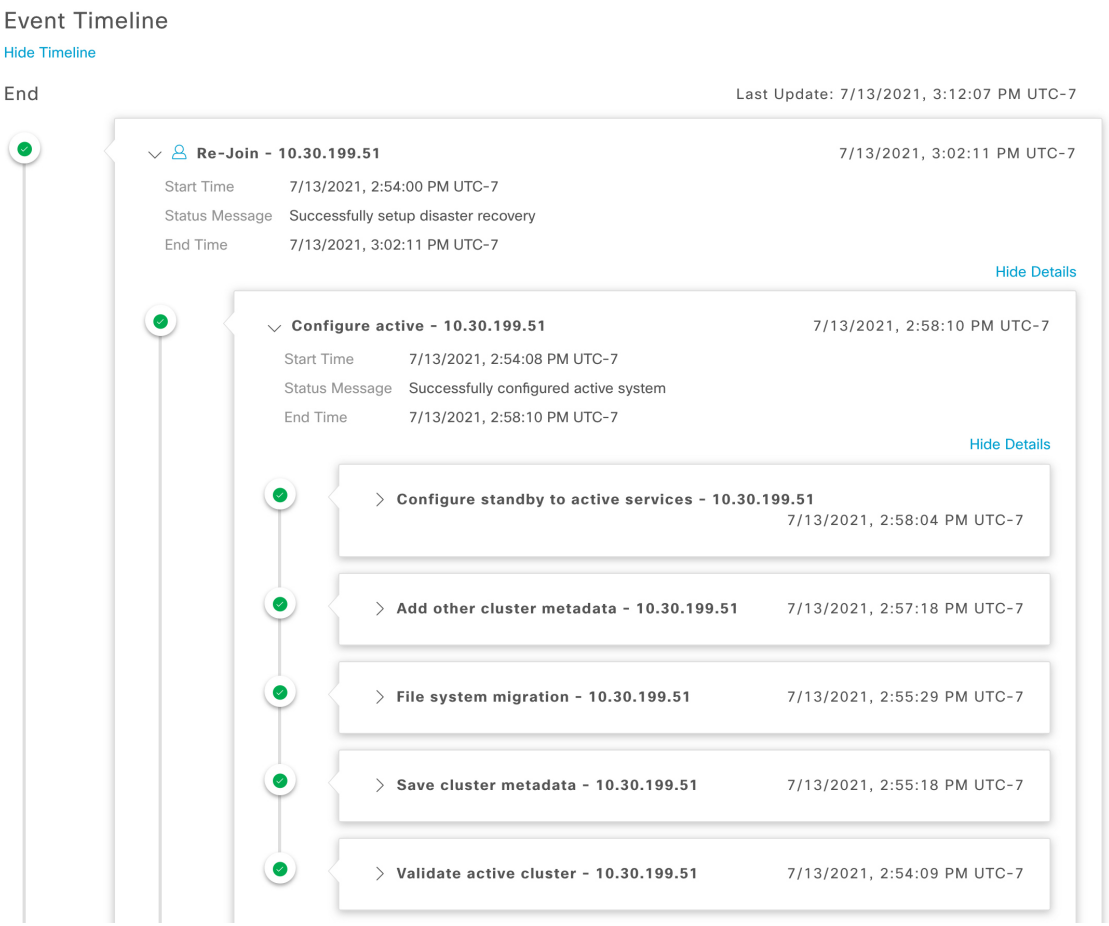
Say you want to monitor the restoration of your system after it was paused. Cisco DNA Center updates the Event Timeline as each task in the restoration process is started and then completed. To view a summary of what took place during a particular task, click >.



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



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



See Troubleshoot Your Disaster Recovery System, on page 182 for a description of the issues you may encounter while monitoring the Event Timeline and how to remedy them.

System and Site States

In the disaster recovery GUI, the **Status** area indicates the current state of your system. The following tables explain the various states you may see for your system's individual sites in the Topology.

Table 10: Active Site States

State	Description
Unregistered	Newly installed site. Disaster recovery information is not available yet.
Initializing	The site is preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Initialized	The site has successfully prepared the data it will transmit to the other sites in order to set up the disaster recovery cluster during the registration process.
Failed to Initialize	The site encountered an error while preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.

State	Description
Connecting Recovery	The main site is contacting the recovery site to retrieve the initialized data required to set up secure communication with the main site.
Connecting Witness	The main site is contacting the witness site to retrieve the initialized data required to set up secure communication with the main site.
Recovery Site Connected	The main site successfully established secure communication with the recovery site.
Failed to Connect Recovery	The main site encountered an error while establishing a secure channel with the recovery site.
Failed to Connect Witness	The main site encountered an error while establishing a secure channel with the witness site.
Registered	The active site successfully established secure communication with the other two sites.
Deregistering	Removing the current disaster recovery configuration from the system.
Deregister Failed	An error occurred while removing the current disaster recovery configuration from the system.
Validating	Validating the state of the system before starting disaster recovery configuration.
Validated	Successfully validated the state of the system before starting disaster recovery configuration.
Validation Failed	An error occurred while validating the state of the system before starting disaster recovery configuration.
Configuring Active	Executing the workflows to establish this site as the active site.
Failed to Configure	An error occurred while running the workflows to enable disaster recovery on this site.
Syncing Config Data	Syncing the data required from the other sites to set up the disaster recovery system.
Config Data Synced	Successfully synced the data required from the other sites to set up the disaster recovery system.
Active Sync Failed	An error occurred while the pending active site was syncing the data required from the other sites to set up the disaster recovery system.
Waiting Standby Configuration	Successfully completed the workflows to establish this site as the active site; waiting for the standby site's workflows to complete.
Active	The site is successfully managing the network as the active site.
Failed to Configure	The site failed to execute some of the workflows that would enable itself as the active site in the disaster recovery cluster.
Isolating	The site is executing the workflows to isolate itself because it either lost connectivity with the other two sites or is preparing to become standby-ready (as part of a manual failover).
Isolated	The site has successfully executed the workflows to isolate itself because it either lost connectivity with the other two sites or is preparing to become standby-ready (as part of a manual failover).
Failed to Isolate	The site encountered an error while executing the workflows to isolate itself because it either lost connectivity with the other two sites or is preparing to become standby-ready (as part of a manual failover).

State	Description
Configuring Active	Configuring a previous standby site as the active site (as part of a system-triggered or manual failover).
Failed during Failover	An error occurred while executing the workflows to establish this site as the active site (as part of a failover or recovery from a two-system failure).
Pausing Active	Executing the workflows that disable disaster recovery operations on the active site (in order to prepare for an administrative operation or a planned outage).
Active Paused	Successfully disabled disaster recovery operations on the active site.
Failed to Pause Active	An error occurred while disabling disaster recovery operations on the active site.
Active Stand Alone	Executing the workflows to establish a previous active site that lost connectivity with the other two sites as an independent system by removing all disaster recovery configurations.
Down	The active site has lost connectivity with the other two sites.

Table 11: Standby Site States

State	Description
Unregistered	Newly installed site. Disaster recovery information is not available yet.
Initializing	The site is preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Initialized	The site has successfully prepared the data it will transmit to the other sites in order to set up the disaster recovery cluster during the registration process.
Failed to Initialize	The site encountered an error while preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Connecting Main	The recovery site is contacting the main site to retrieve the initialized data required to set up secure communication with the main site.
Connecting Witness	The recovery site is contacting the witness site to retrieve the initialized data required to set up secure communication with the main site.
Main Site Connected	The recovery site successfully established secure communication with the main site.
Failed to Connect Main	The recovery site encountered an error while establishing a secure channel with the main site.
Failed to Connect Witness	The recovery site encountered an error while establishing a secure channel with the witness site.
Registered	The standby site successfully established secure communication with the other two sites.
Deregistering	Removing the current disaster recovery configuration from the system.
Deregister Failed	An error occurred while removing the current disaster recovery configuration from the system.
Validating	Validating the state of the system before starting disaster recovery configuration.

State	Description
Validated	Successfully validated the state of the system before starting disaster recovery configuration.
Validation Failed	An error occurred while validating the state of the system before starting disaster recovery configuration.
Configuring Standby	Executing the workflows to establish this site as the standby site.
Failed to Configure	An error occurred while running the workflows to enable disaster recovery on this site.
Syncing Config Data	Syncing the data required from the other sites to set up the disaster recovery system.
Config Data Synced	Successfully synced the data required from the other sites to set up the disaster recovery system.
Standby Sync Failed	An error occurred while the pending standby site was syncing the data required from the other sites to set up the disaster recovery system.
Waiting Active Configuration	Successfully completed the workflows to establish this site as the standby site; waiting for the active site's workflows to complete.
Standby	The site is successfully configured as the standby site in the disaster recovery cluster.
Failed to Configure	The site failed to execute some of the workflows that would enable itself as the standby site in the disaster recovery cluster.
Isolating	The site is executing the workflows to isolate itself because it lost connectivity with the other two sites.
Isolated	The site has successfully executed the workflows to isolate itself because it lost connectivity with the other two sites.
Failed to Isolate	The site encountered an error while executing the workflows to isolate itself because it lost connectivity with the other two sites.
Configuring Standby	Configuring a previous active site as the standby-ready site (as part of a manual failover).
Standby Ready	A previous active system is ready to be configured as a standby system (as a result of a failover).
Pausing Standby	Executing the workflows that disable disaster recovery operations on the standby site (in order to prepare for an administrative operation or a planned outage).
Standby Paused	Successfully disabled disaster recovery operations on the standby site.
Failed to Pause Standby	An error occurred while disabling disaster recovery operations on the standby site.
Standby Stand Alone	Executing the workflows to establish a previous standby site that lost connectivity with the other two sites as an independent system by removing all disaster recovery configurations.
Down	The site has lost connectivity with the other two sites.

Table 12: Witness Site States

State	Description
Unregistered	Newly installed site. Disaster recovery information is not available yet.
Registered	This site has been designated as the witness site and the validation checks have completed successfully.
Up	Configuration of the witness site has completed successfully.
Down	The site has lost connectivity with the other two sites.

Upgrade a Disaster Recovery System

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 2.3.4. Also, disaster recovery is enabled and operational on these appliances. Complete the following steps to complete the upgrade:

Step 1 Place Your System on Pause, on page 174.

Step 2 Upgrade the appliances at your main and recovery sites to version 2.3.4. In the *Cisco DNA Center Upgrade Guide*, see the "Upgrade to Cisco DNA Center 2.3.4.x" chapter.

Step 3 Replace the Current Witness Site, on page 163.

Step 4 Rejoin Your System, on page 176.

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 Click the menu icon (☰) and choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

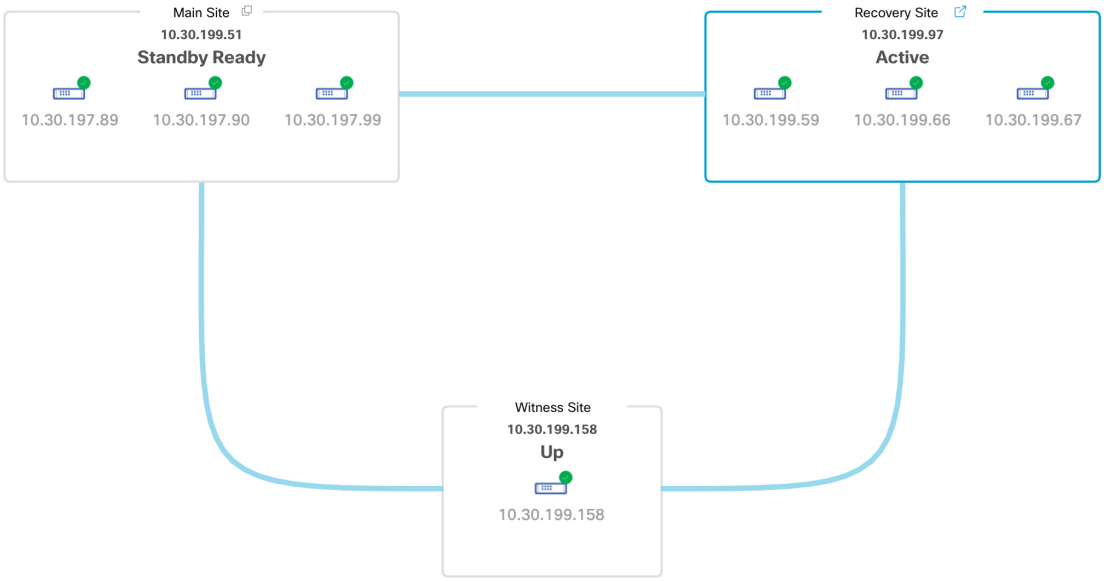
The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology. In the following example, the user is logged in to the current active site.

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.



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:

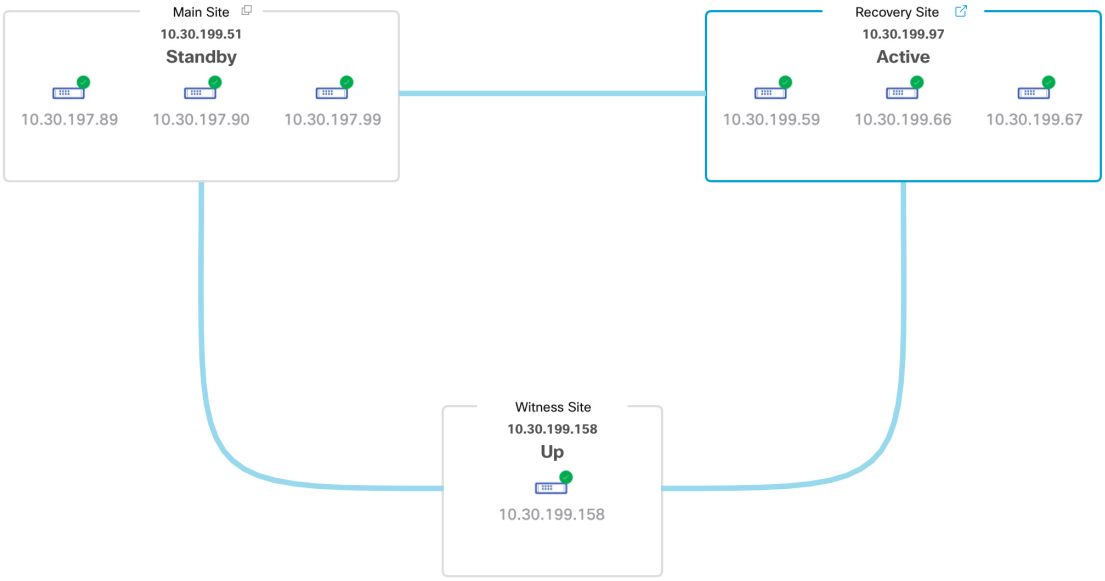
a. Log in to your recovery site.

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.

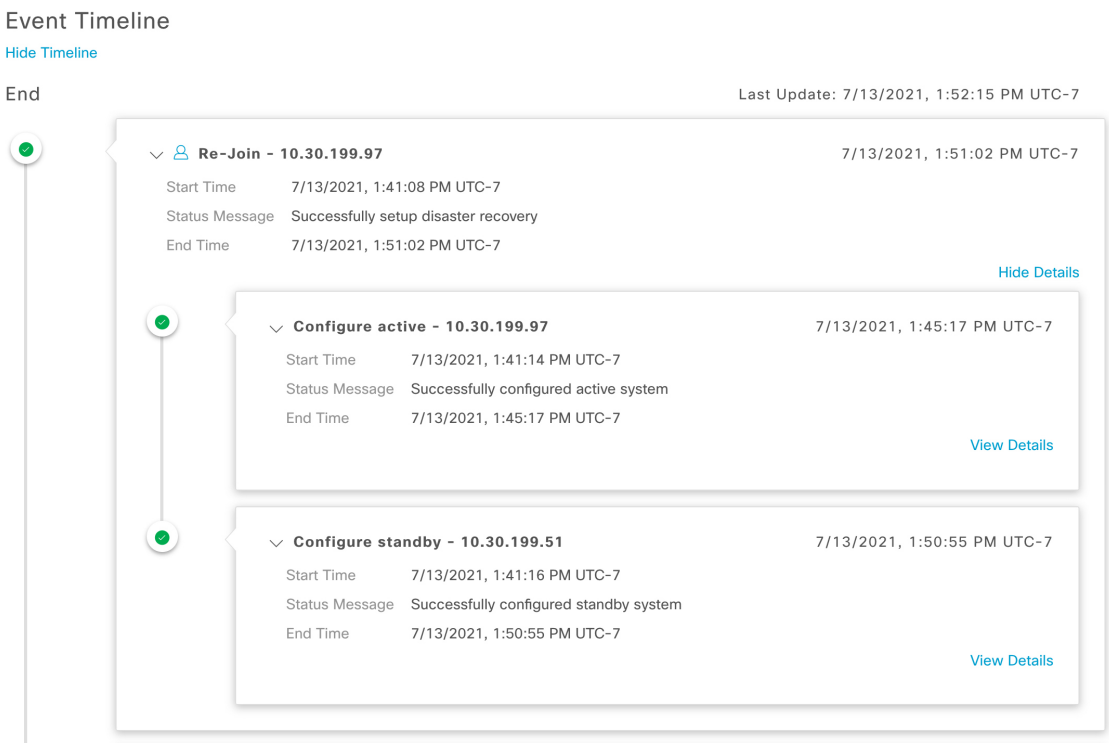
After Cisco DNA Center completes the relevant workflows, the manual failover completes. The main site, which was currently serving as the active site, is now the standby site.



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.



Pause Your Disaster Recovery System

By pausing your main and recovery sites, you are effectively breaking up your disaster recovery system. The sites will no longer be connected and instead will act as standalone clusters. You would want to pause your system to temporarily disable the replication of data from the active site to the standby site if you plan to break up your system for an extended period of time. You would also pause the disaster recovery system to do one of the following:

- Complete any administrative tasks, such as upgrade the clusters or install additional packages
- Replace the system or disaster recovery certificate
- Perform maintenance on the main, recovery, or witness site clusters
- Prepare for a planned network or power outage

Place Your System on Pause

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

Step 1 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.

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

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

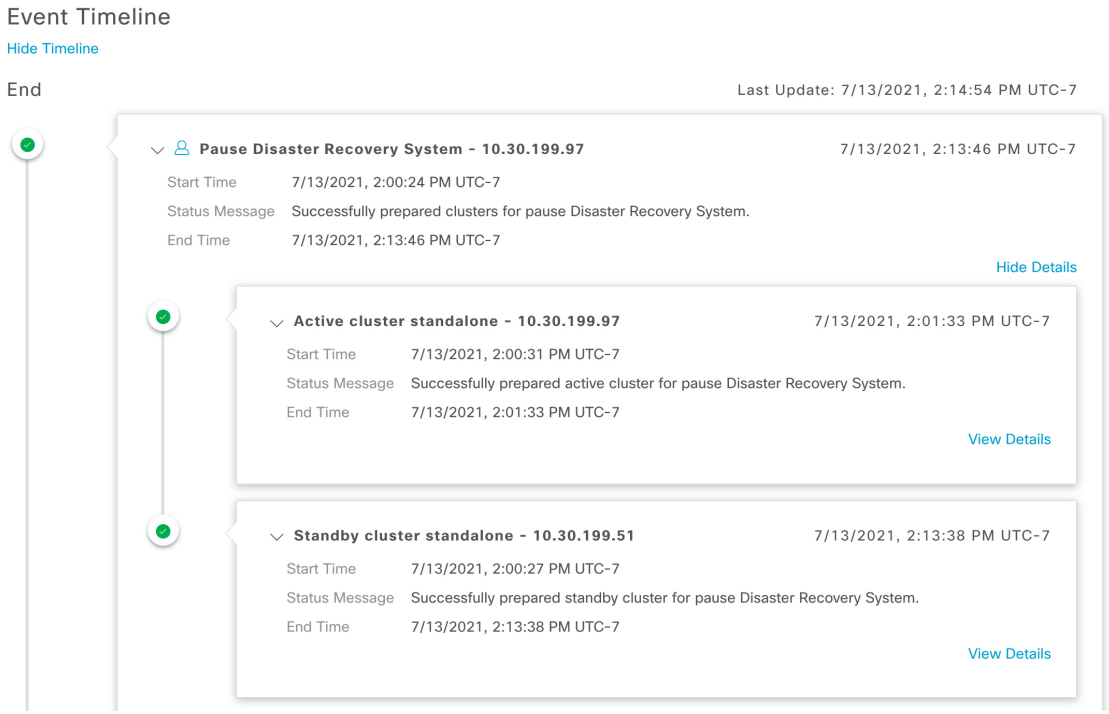
A message appears in the bottom right corner of the page, indicating that the process to pause your system has started. To pause your system, Cisco DNA Center disables data and service replication. It also reinstates the services that were suspended on your recovery site. As this is taking place, the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

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

Step 4 Confirm that your disaster recovery system has been paused:

a. In the top right corner of the **Monitoring** tab, verify that its status is listed as **Paused**.

b. In the Event Timeline, verify that the **Pause Disaster Recovery System** 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 Click the menu icon (☰) and choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

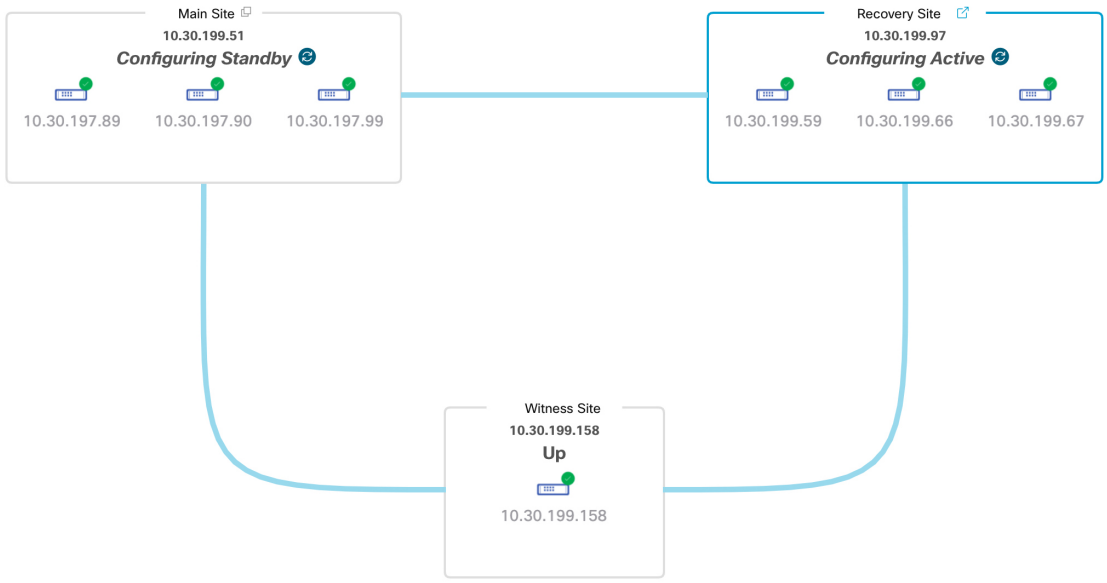
The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology.

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

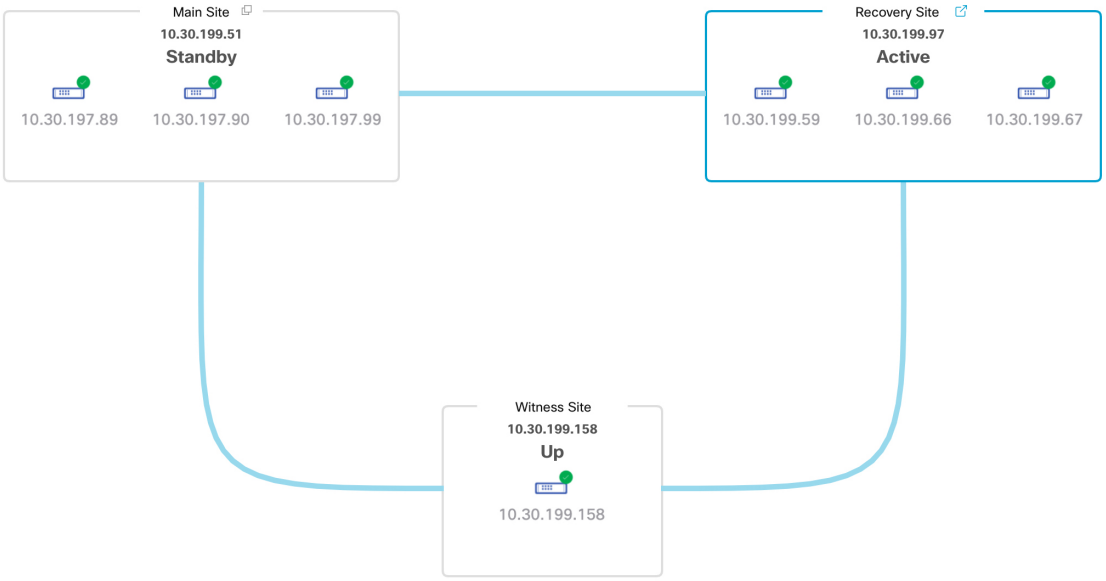
A dialog opens, indicating that all of the data on your standby site will be erased.

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.



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



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

Disaster Recovery System Considerations

This section describes things to be aware of when managing your disaster recovery system.

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 174 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 176 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.
- After a failover takes place, your deployment's backup and restore settings and schedule are not replicated to the new active site. You will need to configure them again.
- If applicable to your deployment, we recommend that you upgrade the TLS version for incoming TLS connections to Cisco DNA Center. In the Cisco DNA Center Security Best Practices Guide, see the "Change the Minimum TLS Version and Enable RC4-SHA (Not Secure)" topic.

For more information on backing up and restoring your disaster recovery system, see Backup and Restore, on page 129.

Node or Cluster Replacement Considerations

You cannot do either of the following without breaking your disaster recovery system's configuration:

- Replace one of the nodes in a 1+1+1 setup.
- Replace all of one site's nodes in a 3+3+1 setup.

If you need to do so, ensure that you then complete the steps described in Deregister Your System, on page 164 to get your system up and running again.

Reconfiguration Considerations

- Any data present on the appliances that reside at the recovery site will be deleted in the following scenarios:
  - When setting up your disaster recovery system for the first time and you activate the system.
  - When the recovery site is the current active site, you pause your system, deregister it, and then reregister it as the recovery site.
- When you reconfigure an existing disaster recovery system, make sure you know which site is the current active site and register it as your system's main site. Alternatively, you can make a backup of the recovery site's data (if it's currently active) and restore this data on your system's main site prior to the system's reconfiguration.
- The following changes cannot be made without reconfiguring your system:
  - Changing the IP addresses and static/default routes configured for your disaster recovery system's Enterprise and Management interfaces.
  - Updating a disaster recovery certificate's **cluster_hostname** value.

  Complete the steps described in Deregister Your System, on page 164 to configure new IP addresses and routes. If you updated the **cluster_hostname** value, complete these same steps after doing so.

HA Considerations

You cannot convert the main and recovery sites from single-node clusters to HA clusters without breaking your disaster recovery system's configuration. If you need to do so, do the following:

1. Deregister Your System, on page 164.
2. Convert both sites to HA clusters.
3. Reregister and reactivate disaster recovery (see Configure Disaster Recovery, on page 155).

Site Failure Considerations

By default, the disaster recovery system waits seven minutes before recognizing that a site has failed and taking one of the following actions:

- When the active site goes down, it starts the failover process.
- When either the standby or witness site goes down, the system marks that site as down and disables the ability to start any tasks from the **Action** area.

If you try to initiate a task before the seven minutes have passed, the **Details** area will display a message that indicates why it cannot be completed.

Certificate Replacement Considerations

If you want your disaster recovery system to use a different certificate or need to replace an expired certificate, do the following:

1. Place Your System on Pause.
2. Replace your system's certificate by completing the steps described in the Add the Disaster Recovery Certificate, on page 152 topic.

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 Event Notifications" 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 174.
2. On both your main and recovery site, replace the current system certificate. Click the menu icon (☰) and choose **System** > **Settings** > **Trust & Privacy** > **System Certificates**.
3. Rejoin Your System, on page 176.

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)`

System Health Status	Event	Notification
OK	Failover to either the main or recovery site has completed successfully.	`Failover Successful`
OK	Registration of the main site has completed successfully.	`Successfully Registered Main Site`
OK	Registration of the recovery site has completed successfully.	`Successfully Registered Recovery Site`
OK	Registration of the witness site has completed successfully.	`Successfully Registered Witness Site`
OK	The disaster recovery system has been paused successfully.	`DR Pause Success`
OK	The standby site is operational.	`Standby Site Up`
OK	The witness site is operational.	`Witness Site Up`
OK	The disaster recovery system has been unregistered successfully.	`Unregister Success`
Degraded	Failover to either the main or recovery site has failed.	`Failover Failed`
Degraded	Automated failover is not available because the standby site is currently down.	`Standby Cluster Down`
Degraded	Automated failover is not available because the witness site is currently down.	`Witness Cluster Down`
Degraded	Unable to place the disaster recovery system on pause.	`Pause Failure`
Degraded	BGP route advertisement failed.	`BGP Failure`
Degraded	The IPsec tunnel connecting your system's sites is operational.	`IPsec Up`
Degraded	The IPsec tunnel connecting your system's sites is currently down.	`IPsec Down`
NotOk	Disaster recovery system configuration failed.	`Activate DR Failure`
NotOk	The site that is currently in the **Standby Ready** state is unable to rejoin the disaster recovery system.	`Activate DR Failure`
NotOk	Unregistration of the disaster recovery system failed.	`Unregistration Failed`
NotOk	Registration of the main site failed.	`Main Registration Failed`
NotOk	Registration of the recovery site failed.	`Recovery Registration Failed`
NotOk	Registration of the witness site failed.	`Witness Registration Failed`

Troubleshoot Your Disaster Recovery System

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

Note If a disaster recovery operation fails or times out, click **Retry** to perform the operation again. If the problem persists and its solution is not provided in the following table, contact Cisco TAC for assistance.

Table 13: Disaster Recovery System Issues

Error Code	Message	Solution
SODR10007	`Token does not match.`	The token provided during recovery site registration does not match the token generated during main site registration. From the main site's **Disaster Recovery** > **Configuration** tab, click **Copy Token** to ensure that you copy the correct token.
SODR10048	`Packages (package names) are mandatory and not installed on the main site.`	Install the listed packages before registering the system.
SODR10056	`Invalid credentials.`	Confirm that you entered the correct credentials for the main site during recovery and witness site registration.
SODR10062	`() site is trying to () with invalid IP address. Expected is (); actual is ().`	The main site IP address provided during recovery and witness site registration is different from the IP address that was provided during main site registration.
SODR10067	`Unable to connect to (recovery or witness site).`	Verify that the main site is up.
SODR10072	`All the nodes are not up for (main or recovery site).`	Check whether all three of the site's nodes are up.
SODR10076	`High availability should be enabled on (main or recovery) site cluster.`	Enable high availability (HA): 1. Log in to the site you need to enable HA on. 2. Click the menu icon (☰) and choose **System** > **Settings** > **System Configuration** > **High Availability**. 3. Click **Activate High Availability**.
SODR10100	`(Main or recovery) site has no third party certificate.`	Replace the default certificate that Cisco DNA Center is currently using with a third-party certificate. See Update the Cisco DNA Center Server Certificate, on page 72 for more information.
SODR10113	`Save cluster metadata failed.`	Contact Cisco TAC for help with completing the appropriate recovery procedure.

Error Code	Message	Solution
SODR10118	`Appliance mismatch between main () and recovery ().`	Different appliances are used by the main and recovery sites. To successfully register disaster recovery, both sites must use the same 56 or 112 core appliance.
SODR10121	`Failed to advertise BGP. Reason: ().`	See Troubleshoot BGP Route Advertisement Issues, on page 190 for more information.
SODR10122	`Failed to stop BGP advertisement. Reason: ().`	See Troubleshoot BGP Route Advertisement Issues, on page 190 for more information.
SODR10123	`Failed to establish secure connection between main () and ()().`	No solution is available for this issue. Contact Cisco TAC for assistance.
SODR10124	`Cannot ping VIP: (`*`main, recovery, or witness site's VIP or IP address`*`).`	Do the following: • Verify that the address specified is correct. • Check whether the address is reachable from the other addresses.
SODR10129	`Unable to reach main site. ()`	Check whether the Enterprise virtual IP address configured for the main site is reachable from the recovery and witness sites.
SODR10132	`Unable to check IP addresses are on the same interface. Retry the operation. ()`	Retry the operation you just attempted.
SODR10133	`The disaster recovery enterprise VIP () and the IP addresses () are not configured or reachable via the same interface. Check the gateway or static routes configuration.`	Communication between a disaster recovery system's sites relies on the Enterprise network. The main and recovery site's Enterprise virtual IP address, and the witness site's IP address, need to be reachable via the Enterprise interface. This error indicates that the IP address/virtual IP address configured for one or multiple sites uses an interface other than the Enterprise interface for communication.
SODR10134	`The disaster recovery management VIP (`*`VIP address`*`) and the IPs (`*`IP addresses`*`) are configured/reachable via same interface. It should be configured/reachable via management interface. Check the gateway or static routes' configuration.`	The disaster recovery system's Management virtual IP address needs to be configured on the Management interface. This error indicates that the virtual IP address is currently configured on an interface where the Management cluster's virtual IP address has not been configured. Add a /32 static route to the Management virtual IP address that's configured on the Management interface.
SODR10136	`Certificates required to establish IPsec session not found.`	From the **System Certificate** page (**System** > **Settings** > **Trust & Privacy** > **System Certificates**), try uploading the third-party certificate again and then retry registration. If the problem persists, contact Cisco TAC for assistance.

Error Code	Message	Solution
SODR10138	`Self-signed certificate is not allowed. Upload a third-party certificate and retry.`	—
SODR10139	`Disaster recovery requires first non-wildcard DNS name to be same in main and recovery. {} in {} site certificate is not same as {} in {} site certificate.`	The third-party certificate installed on your main and recovery sites has different DNS names specified for your disaster recovery system. Generate a third-party certificate that specifies a DNS name for your system and upload this certificate to both sites. **Note** Ensure that the DNS name does *not* use a wildcard.
SODR10140	`Disaster recovery requires at least one non-wildcard DNS name. No DNS name found in certificate.`	The third-party certificate installed on your main and recovery sites does not specify a DNS name for your disaster recovery system. 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. **Note** Ensure that the DNS name does *not* use a wildcard.
—	—	When all three of your system's sites are not connected due to network partitioning or another condition, Cisco DNA Center sets the status of the sites to **Isolated**. Contact Cisco TAC for help with completing the appropriate recovery procedure.
—	`External postgres services does not exists to check service endpoints.`	Do the following: 1. Log in to the site that the error occurred on. 2. Run the following commands: • **Kubectl get sep -A** • **kubectl get svc -A | grep external** 3. In the resulting output, search for `external-postgres`. 4. If present, run the following command: **kubectl delete sep external-postgres -n fusion** 5. Retry the operation that failed previously.
—	`Success with errors.`	If you see this message after initiating a failover or pausing your disaster recovery system, it indicates that the operation completed successfully even though one or multiple services encountered minor errors. You can go ahead and click **Rejoin** to restart your system. These errors will be resolved after you do so.

Error Code	Message	Solution
—	`Failed.`	This message indicates that a disaster recovery operation failed because one or multiple services encountered a critical error. To troubleshoot the failure, we recommend that you view the Event Timeline and drill down to the relevant error. When you see this message, click **Retry** to perform the operation again.
—	`Cannot ping VIP: (`*`VIP address`*`).`	Verify that the Enterprise VIP address configured for your system is reachable.
—	`VIP drop-down list is empty.`	Confirm that your system's VIP addresses and intracluster link are configured properly.
—	`Cannot perform (`*`disaster recovery operation`*`) due to ongoing workflow: BACKUP. Please try again at a later time.`	A disaster recovery operation was triggered while a scheduled backup was running. Retry the operation after the backup finishes.
—	`The GUI indicates that the standby site is still down after it has come back online.`	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. To restore the standby site, do the following: **1.** In an SSH client, log in to the standby site. **2.** Run the **maglev maintenance disable** command to take the site out of maintenance mode. **3.** Log in to Cisco DNA Center. **4.** Click the menu icon (☰) and choose **System** > **Disaster Recovery**. The **Monitoring** tab is selected by default. **5.** In the **Action** area, click **Rejoin** in order to restart your disaster recovery system.
—	`Multiple services exists for MongoDB to check node-port label.`	For debugging, the MongoDB node port is exposed as a service. Run the following commands to identify this port and hide it: • **kubectl get svc --all-namespaces | grep mongodb** • **magctl service unexpose mongodb** <*port-number*>

Error Code	Message	Solution
—	`Multiple services exist for Postgres to check node-port label.`	For debugging, the Postgres node port is exposed as a service. Run the following commands to identify this port and hide it: • **kubectl get svc --all-namespaces | grep postgres** • **magctl service unexpose postgres** <*port-number*>

Two-Site Failure Scenarios

A two-site failure occurs when at least two of your disaster recovery system's three sites go down at the same time or the sites have been partitioned. Refer to the following table for a description of how Cisco DNA Center responds to the various failure scenarios and any user actions that need to be taken.

Failure Scenario	System and User Response
Scenario 1: Two of your system's sites go down.	**1.** The system isolates the site that's still online. **Important** Even if this operation fails, complete the first task described in Step 3 if you plan to operate this site as a standalone site. **2.** Log in to this site. **3.** If you want the site to operate as a standalone site, click **Standalone** and then click **Continue** in the resulting dialog box. If you choose this option and want to reestablish your disaster recovery system later, you'll need to do the following: **a.** Reset the witness site by running the **witness reset** command. **b.** Log in to the other site that failed and click **Standalone** so that it also operates as a standalone site for the time being. **c.** Log in to the site that's still online and reconfigure your Configure Disaster Recovery. When you set this site to operate in standalone mode, the VIP configured for your system is deleted from the sites that went down. This step is key since it will reconfigure your system's VIP on these sites. If you don't want the site to operate as a standalone site, first bring the two sites that went down back up. Then do one of the following: • If the witness site remains offline, refer to the Scenario 3 system and user response. • If the standby site remains offline, refer to the Scenario 4 system and user response. • If the active site remains offline, refer to the Scenario 5 system and user response. When a site enters standalone mode, the system automatically configures its virtual IP address for that site. It also advertises its virtual IP address routes to prevent network reprovisioning.

Failure Scenario	System and User Response
Scenario 2: The active, standby, and witness sites go down and come back online about the same time.	1. The system isolates the active and standby sites. 2. The system restores the active site and the standby site enters the **Standby Ready** state. 3. You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Monitor the Event Timeline. 4. Configure Disaster Recovery, on page 155.
Scenario 3: The active, standby, and witness sites go down. The active and standby sites come back online while the witness site remains offline.	1. The system isolates the active and standby sites. 2. The system restores the active site and the standby site enters the **Standby Ready** state. 3. You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Monitor the Event Timeline. 4. Do one of the following: • After the witness site comes back online, Configure Disaster Recovery, on page 155. • Place Your System on Pause, on page 174.

Failure Scenario	System and User Response
Scenario 4: The active, standby, and witness sites go down. The active and witness sites come back online while the standby site remains offline.	**1.** The system isolates and then restores the active site. **2.** You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Monitor the Event Timeline. **3.** After the former active site comes back online and enters the **Standby Ready** state, Configure Disaster Recovery, on page 155. If you've determined that you need to replace the nodes at the standby site, do the following instead: **a.** Log in to the witness site and run the **witness reset** command. **b.** Log in to the active site, click **Standalone**, and then click **Continue**. **c.** Replace the nodes at the standby site. **d.** If the witness site will use a virtual machine that's newer than the one that was used previously, complete the steps described in Install the Witness Site, on page 153. Otherwise, proceed to the next step. **e.** Configure Disaster Recovery, on page 155.

Failure Scenario	System and User Response
Scenario 5: The active, standby, and witness sites go down. The standby and witness sites come back online while the active site remains offline.	**1.** The system isolates the standby site and then establishes it as the new active site. **2.** You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Monitor the Event Timeline. **3.** After the former active site comes back online and enters the **Standby Ready** state, Configure Disaster Recovery, on page 155. If you've determined that you need to replace the nodes at the standby site, do the following instead: **a.** Log in to the witness site and run the **witness reset** command. **b.** Log in to the active site, click **Standalone**, and then click **Continue**. **c.** Replace the nodes at the standby site. **d.** If the witness site will use a virtual machine that's newer than the one that was used previously, complete the steps described in Install the Witness Site, on page 153. Otherwise, proceed to the next step. **e.** Configure Disaster Recovery, on page 155.

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 Disaster Recovery System** > **View Details** > **Configure active** > **View Details**).

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) 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.

d) 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.