



Cisco Digital Network Architecture Center User Guide, Release 1.0

First Published: 2017-08-21

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 SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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: <http://www.cisco.com/go/trademarks>. 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. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Get Started with Cisco DNA Center 1

About Cisco DNA Center 1

Log In 1

Default Home Page 2

Start Using DNA Center 3

CHAPTER 2

Configure Cisco DNA Center System Settings 5

About DNA Center and Cisco ISE Integration 5

Configure Authentication and Policy Servers 6

Configure Access to a AAA Server 6

Configure Access to a Cisco ISE Server 6

Device Controllability 7

Configure Device Controllability 8

Configure an IP Address Manager 9

Configure DNA Center with SFTP Server Settings 9

Configure SNMP Properties 9

CHAPTER 3

Configure Site Network Settings 11

About Global Network Settings 11

About Device Credentials 12

CLI Credentials 12

SNMPv2c Credentials 12

SNMPv3 Credentials 12

HTTPS Credentials 14

Configure Global Device Credentials 14

Configure CLI Credentials 14

Configure SNMPv2c Credentials 15

Configure SNMPv3 Credentials 16

Configure HTTPS Credentials	18
Configure IP Address Pools	19
Configure Global Network Servers	19
Configure Cisco WLC-High Availability from Cisco DNAC	19
Prerequisites for Cisco WLC High Availability	20
Configuring Cisco WLC-HA from Cisco DNA Center	20
What Happens During or After the High Availability Process is Complete	21
Commands to Configure and Verify Cisco WLC- High Availability	21

CHAPTER 4**Discover Your Network 23**

About Discovery	23
Discovery Credentials	24
Discovery Credentials Guidelines and Limitations	24
Discovery Credentials Example	25
Preferred Management IP Address	26
Discovery Prerequisites	26
NETCONF Configuration	28
SNMP Trap Configuration	28
IP Device-Tracking Configuration	29
Discovery Configuration Guidelines and Limitations	29
Perform Discovery	30
Discover Your Network Using CDP	30
Discover Your Network Using an IP Address Range	31
Manage Discovery Jobs	33
Stop and Start a Discovery Job	33
Clone a Discovery Job	33
Delete a Discovery Job	34

CHAPTER 5**Manage Your Device Inventory 35**

About Device Inventory	35
Device Inventory and Cisco ISE Authentication	41
Device Inventory Tasks	41
Add a Device Manually	42
Filter Devices	46
Change Devices Layout View	46

Change Device Role (Device Inventory)	47
Add or Remove a Device Tag in Device Inventory	48
Delete a Device	49
Update Device Credentials	49
Update Device Polling Interval	53
Resynchronize Device Information	53
Use a CSV File to Import and Export Device Configurations	54
Import Device Configurations From a CSV File	55
Export Device Configurations	55

CHAPTER 6**Manage Software Images 57**

About Software Image Management	57
Viewing Software Images	57
Import Software Images	58
About Golden Software Images	58
Provision Software Images	58

CHAPTER 7**Display Your Network Topology 61**

About Topology	61
Topology Tools	61
Display Device Data	64
Aggregate and Disaggregate Devices	65
Aggregate Devices	66
Disaggregate Devices	66
Change the Aggregated Devices Label	66
Configure the Topology Structure	67
Save a Topology Layout	68
Open a Saved Topology Layout	69
Change Device Role (Topology Layout)	69
Search for Devices and Hosts	70
Add or Remove a Device Tag in Topology	71
Display Devices with Tags	72

CHAPTER 8**Design Your Network 73**

Design A New Network Infrastructure	73
-------------------------------------	----

- About Network Hierarchy 74
- Create Sites in the Network Hierarchy 74
- Add Floors to Buildings 75
- Edit Floors 76
- Place Cisco APs on a Floor 77
- Upload Existing Site Hierarchy 77
- Search the Network Hierarchy 77
- Configure Global Wireless Settings 78
 - Create SSIDs for an Enterprise Wireless Network 78
 - Create SSIDs for a Guest Wireless Network 80
 - Create a Guest Portal Page 82
 - Create a Wireless Interface 83
 - Create a Wireless Radio Frequency Profile 84

CHAPTER 9

- Configure Policies 87**
 - Policy Overview 87
 - Policy Dashboard 87
 - Virtual Networks 88
 - Guidelines and Limitations for Virtual Networks 89
 - Configure Virtual Networks 89
 - Create a Virtual Network 89
 - Edit or Delete a Virtual Network 89
 - Group-Based Access Control Policies 90
 - Prerequisite for Creating Access Control Policies 90
 - Scalable Groups 91
 - Access Contracts 91
 - Configure Access Control Policies 91
 - Workflow to Configure a Group-Based Access Control Policy 91
 - Create a Scalable Group 92
 - Create an Access Control Contract 92
 - Edit or Delete an Access Control Contract 93
 - Create a Group-Based Access Control Policy 93
 - Edit or Delete a Group-Based Access Control Policy 94
 - Traffic Copy Policies 94
 - Sources, Destinations, and Traffic Copy Destinations 95

Guidelines and Limitations of Traffic Copy Policy	95
Configure Traffic Copy Policies	96
Workflow to Configure a Traffic Copy Policy	96
Create an IP Network Group	96
Edit or Delete an IP Network Group	97
Create a Traffic Copy Destination	97
Edit or Delete a Traffic Copy Destination	97
Create a Traffic Copy Contract	98
Edit or Delete a Traffic Copy Contract	98
Create a Traffic Copy Policy	98
Edit or Delete a Traffic Copy Policy	99

CHAPTER 10
Provision Your Network 101

Provisioning	101
Add Devices to Sites	102
Provisioning Devices	102
Provision a Cisco WLC	102
Provision a Cisco AP - Day 1 AP Provisioning	103
Delete Devices After Provisioning	104
Configuring Fabric Domains	105
Fabrics Overview	105
Create a Fabric Domain	105
Configure a Fabric Domain	105
Add Devices to a Fabric	105
Configure Host Onboarding	107
Select Authentication Template	107
Associate Virtual Networks to the Fabric Domain	108
Configure Wireless SSIDs for the Fabric Domain	108
Configure Ports Within the Fabric Domain	108
Configure Multicast Settings	109
Create a Multicast IP Address Pool	109
Add a Device as Rendezvous Point	110

CHAPTER 11
Configure Telemetry 111

About Telemetry Collection	111
----------------------------	-----

Configuring Telemetry Collection 111

CHAPTER 12

Manage Users 113

Change User Password 113

Edit User Roles 113

Change Password Policy 114

Change Authentication Timeout 114

CHAPTER 13

Back Up and Restore Cisco DNA Center 115

About Backup and Restore 115

Back Up the DNA Center 116

Restore DNA Center 117



CHAPTER

1

Get Started with Cisco DNA Center

- [About Cisco DNA Center, page 1](#)
- [Log In, page 1](#)
- [Default Home Page, page 2](#)
- [Start Using DNA Center, page 3](#)

About Cisco DNA Center

Cisco Digital Network Architecture (DNA) offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your entire network environment. It also delivers end-to-end visibility and uses network insights to optimize network performance and deliver the best user and application experience. DNA Center allows you to

- Move faster—Provision thousands of devices across your enterprise. Act fast with centralized management, and automate device deployment.
- Lower costs—Reduce errors with automation. Policy-driven deployment and onboarding deliver better uptime and improved security.
- Reduce risk—Predict problems early. Use actionable insights for optimal performance of your network, devices, and applications.

Log In

Access Cisco Digital Network Architecture (DNA) by entering its network IP address in your browser. The IP address was configured during the DNA Center installation. This IP address connects to the external network.


Procedure

- Step 1** Enter the following address in your web browser address field, where *server-ip* is the IP address (or the hostname) of the server on which you installed DNA Center:
- `https://server-ip`**

For example, <https://192.0.2.1>

Depending on your network configuration, the first time your browser connects to the DNA Center web server, you might need to update your client browser to trust the server's security certificate, which ensures the security of the connection between your client and the DNA Center server.

Step 2 Enter your username and password, which you configured during the installation.

Step 3 To log out, click the gear icon  in the top-right corner and click **Sign Out**.

Default Home Page

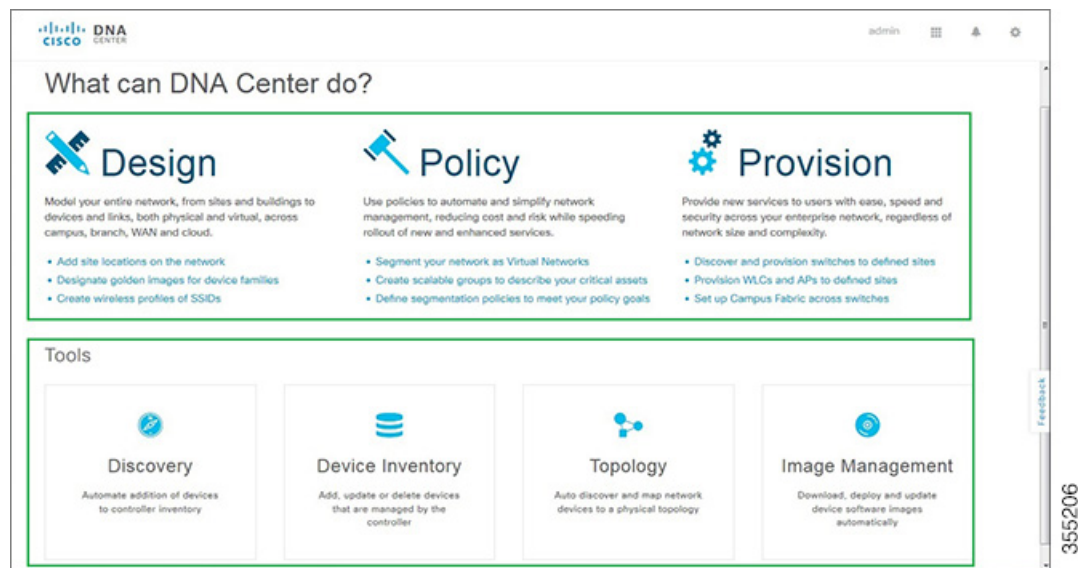
After you log in to DNA Center, you are taken to the DNA Center home page, which is divided into two main areas—Applications and Tools:

Applications include:

- **Design**—Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.
- **Policy**—Create policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.
- **Provision**—Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

Tools—Include all the installed tools that help you configure the network such as Discovery, Device Inventory, Topology, etc.

Figure 1: DNA Center Home Page



From the DNA Center home page, you can also search for applications and tools by entering an application or tool name in the **Search** field.

Start Using DNA Center

To start using DNA Center, you must first configure the DNA Center settings so that the server can communicate outside the network. See [Configure Site Network Settings](#), on page 11.

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

- Existing infrastructure—If you have an existing infrastructure, start with [About Discovery](#). After running Discovery, all your devices are displayed on the Design screen.
- New or nonexistent infrastructure—If you have no existing infrastructure and are starting from scratch, see [About Network Hierarchy](#).



CHAPTER 2

Configure Cisco DNA Center System Settings

- [About DNA Center and Cisco ISE Integration, page 5](#)
- [Configure Authentication and Policy Servers, page 6](#)
- [Device Controllability, page 7](#)
- [Configure Device Controllability, page 8](#)
- [Configure an IP Address Manager, page 9](#)
- [Configure DNA Center with SFTP Server Settings, page 9](#)
- [Configure SNMP Properties, page 9](#)

About DNA Center and Cisco ISE Integration

Before you can create and use access control policies, you need to configure DNA Center and Cisco ISE to integrate with one another. The process involves installing and configuring Cisco ISE with specific services and configuring Cisco ISE settings in DNA Center.

After Cisco ISE has successfully registered and its trust established with DNA Center, DNA Center shares information with Cisco ISE. DNA Center device inventory is propagated to Cisco ISE, and whenever you update device credentials in DNA Center, DNA Center updates Cisco ISE with the changes. Similarly, if you change the Radius shared secret for Cisco ISE, DNA Center updates Cisco ISE with the changes. However, Cisco ISE does not share existing device information with DNA Center. The only way for DNA Center to know about the devices in Cisco ISE is if the devices have the same name in DNA Center; DNA Center and Cisco ISE uniquely identify devices for this integration through the device's *hostname* variable.

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

DNA Center polls Cisco ISE every 15 minutes. If the ISE server is down, the **360 Dashboard** page shows the Cisco ISE server as red, which means the Cisco ISE server is unreachable.


When the Cisco ISE server is unreachable, DNA Center increases polling to 15 seconds, 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. DNA Center continues to poll every 15 minutes for 3 days. If DNA Center has not regained connectivity, it stops polling, and updates the Cisco ISE server status to **Untrusted**. If this happens, you will need to reestablish trust between DNA Center and the Cisco ISE server.

Configure Authentication and Policy Servers

Configure Access to a AAA Server

You can configure access to a primary and a secondary AAA server.


Procedure

- Step 1** From the DNA Center **Home** page, click  > **System Settings** > **Settings** > **Authentication and Policy Servers**.
- Step 2** Click **+ AAA Server**.
- Step 3** Configure the primary AAA server:
- **IP Address**—IP address of the AAA server.
 - **Shared Secret**—Key for RADIUS authentications. The shared secret can be up to 128 characters in length.
 - **Cisco ISE**—Toggle that configures a AAA server or a Cisco ISE server. Leave the toggle set as is. Do not choose **Cisco ISE**.
- Step 4** Click **View Advanced Settings** and configure the settings:
- **Protocol**—TACACS or RADIUS
 - **Authentication Port**—Port used to relay authentication messages to the AAA server. The default is UDP port 1812.
 - **Accounting Port**—Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. The default UDP port is 1813.
 - **Retries**—Number of times that DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default UDP port is 1814.
 - **Timeout**—The length of time that DNA Center waits for the AAA server to respond before abandoning the attempt to connect.
- Step 5** Click **Add**.
- Step 6** To add a secondary AAA server, click **+ AAA Server** and repeat Step 3 through Step 5.
-

Configure Access to a Cisco ISE Server

To use access control policies, you need to configure access to a Cisco ISE server.

Procedure

- Step 1** From the DNA Center home page, click  > **System Settings** > **Settings** > **Authentication and Policy Servers**.
- Step 2** Click **+ AAA Server**.
- Step 3** Configure the Cisco ISE settings:
- **IP Address**—IP address of the ISE server.
 - **Shared Secret**—Key for RADIUS authentications. The shared secret can be up to 128 characters in length.
 - **Cisco ISE**—Setting that indicates whether the server is a Cisco ISE server. Click the **Cisco ISE** setting to enable Cisco ISE.
 - **Username**—Name that is used to log in to Cisco ISE.
 - **Password**—Password that is used to log in to Cisco ISE.
 - **FQDN**—Fully qualified domain name (FQDN) of the Cisco ISE server. The FQDN consists of two parts: the 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**—Cisco ISE server name.
 - **SSH Key**—Diffie-Hellman-Group14-SHA1 SSH key used to connect and authenticate with Cisco ISE.
- Step 4** Click **View Advanced Settings** and configure the settings:
- **Protocol**—TACACS or RADIUS
 - **Authentication Port**—Port used to relay authentication messages to the AAA server. The default is UDP port 1812.
 - **Accounting Port**—Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. The default UDP port is 1813.
 - **Retries**—Number of times that DNA Center attempts to connect with Cisco ISE before abandoning the attempt to connect.
 - **Timeout**—The length of time that DNA Center waits for Cisco ISE to respond before abandoning the attempt to connect.
- Step 5** Click **Add**.
-

Device Controllability

When Device Controllability is enabled and under certain circumstances, DNA Center configures devices with the network settings for the site to which the device belongs.

When device controllability is disabled, DNA Center does not configure any settings on the devices.

**Note**

Device controllability is enabled by default. If you do not want device controllability enabled, you have to manually disable it. For more information, see [Configure Device Controllability, on page 8](#).

Device controllability configures SNMP (SNMPv2c and SNMPv3) credentials and Syslog on devices under the following circumstances:

- **Device in Global Site**—When you successfully add, import, or discover a device, DNA Center places the device in the **Managed** state and assigns it to the Global site by default. Even if you have defined Syslog and SNMP server settings for the Global site, DNA Center does not change the Syslog and SNMP server settings on the device.
- **Device Moved to Site**—If you move the device from the Global site to a new site, for example Site A, that has Syslog and SNMP server settings configured, DNA Center changes the Syslog and SNMP server settings on the device to the settings configured for Site A.
- **Device Removed from Site**—If you remove a device from a site, for example Site A, DNA Center does not remove the Syslog and SNMP server settings from the device.
- **Device Moved from Site to Site**—If you move a device, for example from Site A to Site B, DNA Center replaces the Syslog and SNMP server settings on the device with the settings assigned to Site B.


After discovering devices and when device controllability is enabled, DNA Center configures the following features and protocols on the devices:

- **SNMP Trap server**—If you have Device Controllability enabled, DNA Center configures these SNMP traps for you. Otherwise, you need to enable SNMP traps and configure DNA Center's server IP address as the SNMP server. For information, see [SNMP Trap Configuration, on page 28](#).
- **IP Device Tracking**—DNA Center automatically enables IP device tracking (IPDT) or Switch Integrated Security Features (SISF) on any network device where IPDT is supported and not enabled. DNA Center configures IPDT or SISF IPDT on the device based on the device type and image version that is running.
- **NetFlow controller**

Configure Device Controllability

Device controllability automatically configures discovered devices with SNMP credentials, SNMP Trap servers, IP Device Tracking, NetFlow, Syslog, and NETCONF. Device controllability is enabled by default. If you want, you can disable device controllability and reenable it at any time. For more information, see [Device Controllability, on page 7](#).


Procedure

-
- Step 1** From the DNA Center **Home** page, click  > **System Settings** > **Settings** > **Device Controllability**.
- Step 2** Click **Enable Device Control**.
-

Configure an IP Address Manager

You can configure DNAC to communicate with an external IP Address Manager such as Infoblox®.


Procedure

- Step 1** Click , then select **System Settings**.
 - Step 2** Click the **Settings** tab, then click **IP Address Manager**.
 - Step 3** In the **IP Address Manager (Infoblox)** section, click **Configure settings for IPAM**.
 - Step 4** Complete the required fields for your Infoblox server, then click **Apply**.
-

Configure DNA Center with SFTP Server Settings

To upload files from DNA Center to an SFTP server, you need to configure information about your external SFTP server.


Procedure

- Step 1** From the DNA Center **Home** page, click  > **System Settings** > **Settings** > **SFTP**.
 - Step 2** Configure the SFTP settings as follows:
 - **Host**—IP address of the SFTP server.
 - **Username**—Name that is used to log into the SFTP server.
 - **Password**—Password that is used to log into the SFTP server.
 - **Port**—Port that is used to log into the SFTP server.
 - **Root Location**—Enter the location of the SFTP root directory.
 - Step 3** Click **Update**.
-

Configure SNMP Properties

You can configure retry and timeout values for SNMP.

Procedure

Step 1 Click  and select **System Settings**.

Step 2 Click **Settings > SNMP Properties**.

Step 3 Configure the following fields:

Table 1: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 0-4. The default is 3.
Timeout (in Seconds)	Number of seconds DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 5-120 in intervals of 5 seconds. The default is 5.

Step 4 Click **Apply**.

Note To return to the default settings, click **Revert to Defaults**.



Configure Site Network Settings

- [About Global Network Settings, page 11](#)
- [About Device Credentials, page 12](#)
- [Configure Global Device Credentials, page 14](#)
- [Configure IP Address Pools, page 19](#)
- [Configure Global Network Servers, page 19](#)
- [Configure Cisco WLC-High Availability from Cisco DNAC, page 19](#)

About Global Network Settings

You can create network settings that become the default for your entire network. There are two primary areas for defining settings within your network:

- **Global settings** affect your entire network and can include settings for servers (such as NTP, Syslog, SNMP Trap, Netflow Collector, etc.), IP address pools, and device credential profiles.
- **Site settings** override Global settings and can include settings for servers, IP address pools, and device credential profiles.

You can define the following global network settings by choosing **Design > Network Settings > Network**.

- Network servers such as AAA, DHCP, and DNS Servers—See [Configure Global Network Servers, on page 19](#).
- Device credentials such as CLI, SNMP, and HTTP(S) credentials—See [Configure CLI Credentials, on page 14](#), [Configure SNMPv2c Credentials, on page 15](#), [Configure SNMPv3 Credentials, on page 16](#), and [Configure HTTPS Credentials, on page 18](#).
- IP address pools—See [Configure IP Address Pools, on page 19](#).
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—See [Configure Global Wireless Settings, on page 78](#)

About Device Credentials

Device credentials refer to the CLI, Simple Network Management Protocol (SNMP), and HTTPS credentials that are configured on network devices. DNA Center uses these credentials to discover the devices in your network. In DNA Center, you can specify the credentials that most of the devices use so that you do not have to enter them each time you run a discovery job. These credentials are called global device credentials. Specify them using the DNA Center GUI (**Design > Network Settings > Device Credentials**). After you set up these credentials, they are available for use in the **Discovery** tool.

CLI Credentials

You need to configure the CLI credentials of your network devices in DNA Center before you can run a Discovery job.

CLI credentials are used to discover and gather information about network devices. During the Discovery process, DNA Center logs into the network devices using their CLI usernames and passwords and runs **show** commands to gather device status and configuration information. DNA Center also runs **clear** commands and other commands that perform actions that are not saved in a device's configuration.

SNMPv2c Credentials

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language to monitor and manage network devices.

SNMP version 2 (SNMPv2c) is the community string-based administrative framework for SNMPv2. It does not provide authentication or encryption (noAuthNoPriv level of security). Instead, it uses a community string as a type of password that is typically provided in cleartext.

**Note**

In DNA Center's implementation, only the username is provided in clear text. SNMP community strings are not provided in cleartext for security reasons.

You need to configure the SNMPv2c community string values before you can discover your network devices using the Discovery function. The SNMPv2c community string values that you configure must match the SNMPv2c values that have been configured on your network devices. You can configure up to five read community strings and five write community strings in DNA Center.

If you are using SNMPv2 in your network, specify both the Read Only (RO) and Read Write (RW) community string values to achieve the best outcome. If you cannot specify both, we recommend that you specify the RO value. If you do not specify the RO value, DNA Center attempts to discover devices using the default RO community string, *public*. If you specify only the RW value, Discovery uses the RW value as the RO value.

SNMPv3 Credentials

The SNMPv3 values that you configure to use Discovery must match the SNMPv3 values that have been configured on your network devices. You can configure up to five SNMPv3 values.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with in transit.
- Authentication—Determines if a message is from a valid source.
- Encryption—Scrambles a packet's contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and a user's role. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption
- AuthNoPriv—Security level that provides authentication but does not provide encryption
- AuthPriv—Security level that provides both authentication and encryption

The following table describes what the combinations of the SNMPv3 security models and levels mean:

Table 2: SNMPv3 Security Models and Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	User Name	No	Uses a username match for authentication.
AuthNoPriv	Either: <ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA 	No	Provides authentication based on the Hashed Message Authentication Code-Secure Hash Algorithm (HMAC-SHA) or Hashed Message Authentication Code-Secure Hash Algorithm (HMAC-SHA)
AuthPriv	Either: <ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA 	Either: <ul style="list-style-type: none"> • CBC-DES • CBC-AES-128 	Provides authentication based on HMAC-MD5 or HMAC-SHA. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or CBC-mode AES for encryption.

HTTPS Credentials

Hyper-Text Transfer Protocol Secure (HTTPS) is a secure version of HTTP that is based on a special PKI certificate store. In DNA Center, HTTPS is used to discover Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) devices only.

Configure Global Device Credentials

Configure CLI Credentials

You can configure and save up to five global CLI credentials.

Before You Begin

You must have successfully installed DNA Center, and it must be operational. For more information about installing DNA Center, see the *DNA Center Installation and Configuration Guide*.

Procedure

-
- Step 1** From the DNA Center home page, choose **Design > Network Settings > Device Credentials**.
 - Step 2** In the **CLI Credentials** area, click **Add**.
 - Step 3** Enter information in the following fields:

Table 3: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	<p>Password that is used to log in to the CLI of the devices in your network.</p> <p>For security reasons, enter the password again as confirmation.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Field	Description
Enable Password	<p>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</p> <p>For security reasons, enter the enable password again.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Step 4 Click **OK**.

Configure SNMPv2c Credentials

If you use SNMPv2c credentials to monitor and manage your network devices, configure the SNMPv2c values to discover your devices.

Before You Begin

- You must have successfully installed DNA Center, and it must be operational. For more information about installing DNA Center, see the *DNA Center Installation Guide*.
- You must have your network's SNMP information available for this procedure.
-

Procedure

Step 1 From the DNA Center home page, select **Design > Network Settings > Device Credentials**.

Step 2 In the **SNMP** credentials area, click **Add**.

Step 3 For the SNMP type, click **SNMP v2c** and enter the following information:

Table 4: SNMP v2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMP v2c settings that you are adding. • Read Community—Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Field	Description
Write	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMP v2c settings that you are adding. • Write Community—Write community string used to make changes to SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Step 4 Click OK.

Configure SNMPv3 Credentials

If you use SNMPv3 to monitor and manage your network devices, configure the SNMPv3 values to discover your network devices.

Before You Begin

- You must have successfully installed DNA Center, and it must be operational. For more information about installing DNA Center, see the *DNA Center Installation Guide*.
- You must have your network's SNMP information available.
-

Procedure

Step 1 From the DNA Center home page, choose **Design > Network Settings > Device Credentials**.

Step 2 In the **SNMP** credentials area, click **Add**.

Step 3 For the SNMP type, click **SNMP v3** and enter the following information:

Table 5: SNMP v3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.

Field	Description
Mode	<p>Security level that an SNMP message requires, and whether the message should be authenticated. Select one of the following modes:</p> <ul style="list-style-type: none"> • noAuthNoPriv—Provides authentication or encryption. • AuthNoPriv—Provides authentication but does not provide encryption. • AuthPriv—Provides both authentication and encryption.
Auth Type	<p>Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Select one of the following authentication types:</p> <ul style="list-style-type: none"> • SHA—Authentication based on HMAC-SHA. • MD5—Authentication based on HMAC-MD5.
Auth Password	<p>SNMPv3 password used for gaining access to information from devices that use SNMPv3. Passwords (or passphrases) must be at least 8 characters in length.</p> <p>Note</p> <ul style="list-style-type: none"> • For several Cisco Wireless Controllers (WLC), passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords results in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	<p>Privacy type. (Enabled if you select AuthPriv as a the authentication mode.) Select one of the following privacy types:</p> <ul style="list-style-type: none"> • DES—DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. • AES128—CBC mode AES for encryption. • None—No privacy.
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long.</p> <p>Note</p> <ul style="list-style-type: none"> • For several Cisco WLCs, passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords will result in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 4 Click **OK**.

Configure HTTPS Credentials

Procedure

Step 1 From the DNA Center **Home** page, select **Design > Network Settings > Device Credentials**.

Step 2 In the **HTTPS Credentials** area, click **Add**.

Step 3 Enter the following information:

Table 6: SNMP v2c Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .
Read	<p>You can configure up to five HTTPS read credentials.</p> <ul style="list-style-type: none"> • Name/Description—Name or description of the HTTPS credentials that you are adding. • Username—Name used to authenticate the HTTPS connection. • Password—Password used to authenticate the HTTPS connection. • Port—Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<p>You can configure up to five HTTP write credentials.</p> <ul style="list-style-type: none"> • Name/Description—Name or description of the HTTPS credentials that you are adding. • Username—Name used to authenticate the HTTPS connection. • Password—Password used to authenticate the HTTPS connection. • Port—Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Step 4 Click **OK**.

Configure IP Address Pools

You can manually create IP address pools.

Procedure

- Step 1** Choose **Design > Network Settings > IP Address Pools**.
 - Step 2** Click **Add** and complete the required fields.
 - Step 3** Click **Overlapping** to specify overlapping IP address pool groups to allow different address spaces and concurrently use the same IP addresses in different address spaces.
 - Step 4** Click **Save**.
-

Configure Global Network Servers

You can define global network servers that become the default for your entire network.



Note You can override global network settings on a site by defining site-specific settings.

Procedure

- Step 1** Choose **Design > Network Settings > Network**. A list of default servers appears.
 - Step 2** Enter the required information for the servers listed, or click **Add Servers** to add an NTP, Syslog, SNMP Trap, or Netflow Collector server.
 - Note** You must define a DHCP server in order to create IP address pools.
 - Step 3** Complete the required fields, then click **Save**.
-

Configure Cisco WLC-High Availability from Cisco DNAC

Cisco WLC High Availability (HA) can be configured through Cisco Digital Network Architecture (DNA) Center. In DNA Center Release 2.0, only the formation of WLC-HA is supported and breaking of HA and switch-over options are not supported.

Related Topics

- [Prerequisites for Cisco WLC High Availability](#), on page 20
- [Configuring Cisco WLC-HA from Cisco DNA Center](#), on page 20
- [What Happens During or After the High Availability Process is Complete](#), on page 21
- [Commands to Configure and Verify Cisco WLC- High Availability](#), on page 21

Prerequisites for Cisco WLC High Availability

- Discovery and Inventory of Cisco WLC-1 and WLC-2 (to be formed as High Availability through the management interface) should be successful. The devices should be in the managed state.
- The service ports and the management ports of Cisco WLC-1 and WLC-2 should be configured.
- Redundancy ports of Cisco WLC-1 and WLC-2 should be physically connected.
- The management address of Cisco WLC-1 and WLC-2 should be in the same subnet. Also, the redundancy management address of WLC-1 and WLC-2 should be in the same subnet.

Configuring Cisco WLC-HA from Cisco DNA Center

Procedure

-
- Step 1** Choose **Provision > Devices**, and click WLC-1 (configuring this as primary).
- Step 2** Click the **High Availability** tab.
- Step 3** Select the Select Secondary WLC drop-down list and enter the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses.
Ensure that these IP addresses are the unused IP addresses.
- Step 4** Click **Configure HA**.
The HA configuration is initiated at the background using the CLI commands. First, the primary WLC is configured. On success, the secondary WLC is configured. After the configuration is complete, both the WLCs will reboot. This process may take up to 2.5 minutes to complete.
- Step 5** After the HA is initiated, the **Redundancy Summary** under **High Availability** tab displays the **Sync Status** as **In Progress**. When DNA Center finds the HA pairing successful, **Sync Status** becomes **Complete**. This is triggered by the inventory poller or by manual re-sync. By now, the secondary WLC (WLC-2) gets deleted from DNA Center. This flow indicates the successful HA configuration in WLC.
- Note** There is no real-time data display for Redundancy Summary. During HA pairing, under **Device Inventory**, Cisco WLC shows "Synching" but under **Provision > WLC** shows "Sync Completed".
- Note** You must perform HA on WLC before adding WLC to connectivity domain. Also ensure that the **Sync status** is **Complete** before adding to connectivity domain.
-

What Happens During or After the High Availability Process is Complete

- 1 Cisco WLC-1 and WLC-2 are configured with redundancy management, redundancy units, and SSO. The WLCs reboot in order to negotiate their role as active or stand by. Configuration is synced from active to stand by.
- 2 On the Show Redundancy Summary page, you can see these configurations:
 - SSO is Enabled
 - WLC1 is Active state
 - WLC2 is Hot Stand By state
- 3 Active WLCs management port will be shared by both the WLCs and will be pointing to active. GUI, Telnet, and SSH on the stand by WLC will not work. You can use the console and service port interface to control the stand by WLC.

Commands to Configure and Verify Cisco WLC- High Availability

The following are the configuration commands sent to primary WLC:

- **config interface address redundancy-management 9.10.45.xx peer-redundancy-management 9.10.45.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

The following are the configuration commands sent to secondary WLC:

- **config interface address redundancy-management 9.10.45.yy peer-redundancy-management 9.10.45.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

The following are the commands to verify HA configurations from Cisco WLC:

- Use the **config redundancy mode sso** command to check the HA related details.
- Use the **show redundancy summary** command to check the configured interfaces.



Discover Your Network

- [About Discovery, page 23](#)
- [Discovery Credentials, page 24](#)
- [Preferred Management IP Address, page 26](#)
- [Discovery Prerequisites, page 26](#)
- [Discovery Configuration Guidelines and Limitations, page 29](#)
- [Perform Discovery, page 30](#)
- [Manage Discovery Jobs, page 33](#)

About Discovery

Discovery and Device Inventory function as one service. The process of finding network devices is known as Discovery. The Discovery function scans the devices in your network and sends the list of discovered devices to Device Inventory. Device Inventory retrieves and saves the details about the devices in its database. Device Inventory refreshes every 25 minutes for each device. (At any given time, Device Inventory may be refreshing data for several devices at a time.)

There are two methods for discovering devices:

- Using CDP and providing a seed IP address.
- Specifying a range of IP addresses (maximum of 4096 devices).

Regardless of the method you use, you must be able to reach (ping) the device from DNA Center, and you need to configure specific credentials and protocols in DNA Center to discover your devices. These credentials can be configured globally in the **Device Credentials** page or on a per-job basis on the **Discovery** page. (Credentials configured in Discovery may be saved to use later as global credentials.)

- CLI credentials
- Simple Network Management Protocol (SNMPv2c or SNMPv3) credentials
- HTTPS credentials (These credentials are required only for discovering devices running Cisco Network Function Virtualization Infrastructure Software (NFVIS).)

- SSH/Telnet protocol

Because the various devices in a network can have different sets of credentials, you can configure multiple sets of credentials in DNA Center. The discovery process iterates through all of the sets of credentials until it finds a set that works for the device.

For discovery, one set of CLI credentials and one set of SNMP credentials (SNMPv2c Read, SNMPv2c Write, or SNMPv3) is mandatory. If valid sets of credentials are provided for both SSH and Telnet, SSH credentials will be picked because SSH is more advanced than Telnet. If all three sets of valid SNMP credentials are provided, SNMP v3 will be picked because it's the most advanced protocol of the three.

After discovering devices, Device Inventory retrieves the details about the devices, such as host IP addresses, MAC addresses, and network attachment points, using one of the following protocols, as required:

- Link Layer Discovery Protocol (LLDP)
- IP Device Tracking (IPDT) is enabled automatically for the network fabric during the provisioning.
- LLDP Media Endpoint Discovery (LLDP-MED) (This protocol is used to discover IP phones and some servers.)
- Network Configuration Protocol (NETCONF) (Only required for devices running NFVIS.)

For information about configuration requirements for specific device types, see [Discovery Prerequisites](#), on page 26.

Discovery Credentials

Discovery credentials are the CLI, SNMPv2c, SNMPv3, and HTTP configuration values for the devices that you want to discover. You need to specify the credentials based on the types of devices you are trying to discover:

- Standard Cisco devices—CLI and SNMP credentials.
- NFVIS devices—HTTP credentials.
- Both standard and NFVIS devices—CLI, SNMP, and HTTP credentials

If you use the same credential values for the majority of devices in your network, you can configure and save them as global discovery credentials, which you can reuse in multiple discovery jobs. To discover devices with unique credentials, you can add job-specific discovery credentials when you run Discovery. You can define up to five global and one job-specific credential for each of the credential types (CLI, SNMPv2c, SNMPv3, and HTTP).



Note

If you use Cisco ISE for the DNA Center access policy feature, make sure that the device credentials that you use for discovery are also configured as the device credentials used by Cisco ISE. For more information, see [Device Inventory and Cisco ISE Authentication](#), on page 41.

Discovery Credentials Guidelines and Limitations

The following are guidelines and limitations for the DNA Center discovery credentials:

- If you change a device's credential after successfully discovering the device, subsequent polling cycles for that device fail. To correct this situation, use one of the following options:
 - Use the Discovery tool to:
 - Run a new discovery job with job-specific credentials that match the device's new credential.
 - Edit the existing discovery job and re-run the Discovery.
 - Use the Design tool to:
 - Create a new global credential and run a new discovery job using the correct global credential.
 - Edit an existing global credential and re-run the discovery job.
- If an ongoing discovery polling cycle fails due to a device authentication failure, you can correct the situation using one of following options:
 - Use the Discovery tool to:
 - Stop or delete the current discovery job and run a new discovery job with job-specific credentials that match the device's credential.
 - Stop or delete the current discovery job, edit the existing discovery job, and re-run the Discovery.
 - Use the Design tool to:
 - Create a new global credential and run a new discovery job using the correct global credential.
 - Edit an existing global credential and re-run the discovery job.
- Deleting a global credential does not affect previously discovered devices. The status of the previously discovered devices does not indicate an authentication failure. However, the next discovery that tries to use the deleted credential will fail. The discovery will fail **before** it tries to contact any devices. For example, 25 minutes after you delete the credential, discovery jobs that use it will fail.
- DNA Center provides a REST API that allows an external application to retrieve a list of the managed network devices and synchronize its own managed inventory with the devices that have been discovered by DNA Center.

Discovery Credentials Example

Assume that a network of 200 devices, which form a Cisco Discovery Protocol (CDP) neighborhood (neighboring devices discovered using CDP), exists. In this network, 190 devices share a global credential (Credential 0) and the remaining devices each have their own unique credential (Credential-1 through Credential-10).

To discover all of the devices in this network using DNA Center, you would perform the following tasks:

Procedure

	Command or Action	Purpose
Step 1	Configure the CLI global credentials as Credential-0.	
Step 2	Configure the SNMP (v2c or v3) global credentials.	
Step 3	Run a discovery job using one of the 190 device IP addresses (190 devices that share the global credentials) and the global Credential-0.	
Step 4	Run 10 separate discovery jobs for each of the remaining 10 devices using the appropriate job-specific credentials, for example, Credential-1, Credential-2, Credential-3, and so on.	
Step 5	Review the results in the Device Inventory window.	

Preferred Management IP Address

DNA Center can use another interface's IP address as the preferred management IP address. DNA Center chooses the preferred management IP address as follows:

- 1 If the device has one loopback interface, DNA Center uses that loopback interface IP address.
- 2 If the device has multiple loopback interfaces, DNA Center uses the loopback interface with the highest IP address.
- 3 If there are no loopback interfaces, DNA Center uses the Ethernet interface with the highest IP address. (Subinterface IP addresses are not considered.)
- 4 If there are no Ethernet interfaces, DNA Center uses the serial interface with the highest IP address.

Discovery Prerequisites

Make the following configuration changes on these platforms for the Discovery tool to work properly.

Table 7: Required Platform Configurations

Feature	Platform	Required Configuration
Discovery (device inventory collection)	<ul style="list-style-type: none"> • Cisco ASR 9000 Series Aggregation Services Routers • Cisco Catalyst 3000 Series Switches • Cisco Catalyst 6000 Series Switches • Cisco Wireless LAN Controllers <ul style="list-style-type: none"> ◦ Cisco Series 3504 WLC ◦ Cisco Series 5508/5520 WLC ◦ Cisco Series 8510/8540 WLC • Other Cisco devices that require NETCONF support for their device pack. 	Configure NETCONF on these platforms. For information, see NETCONF Configuration, on page 28 .
Discovery (device inventory collection)	<ul style="list-style-type: none"> • Cisco ASR 9000 routers • Cisco Catalyst 3000 and 6000 series switches 	<ul style="list-style-type: none"> • Configure the username and password with privileged EXEC mode (level 15). For information, see Discovery Configuration Guidelines and Limitations, on page 29. • Configure transport protocols. For information, see Discovery Configuration Guidelines and Limitations, on page 29. • Do not change the default login methods. For information, see Discovery Configuration Guidelines and Limitations, on page 29.

Feature	Platform	Required Configuration
Discovery (host inventory collection)	Devices connected to hosts using SNMP.	Configure SNMP traps on these devices. For information, see SNMP Trap Configuration , on page 28.
	Devices connected to hosts using Switch Integrated Security Features based IP device tracking.	Enable SISF-based IP device-tracking for these devices. For information, see IP Device-Tracking Configuration , on page 29.

NETCONF Configuration

Enable the NETCONF protocol for the Cisco ASR 9000 Series Aggregation Services Routers or other Cisco devices that require NETCONF support for their device pack. If NETCONF is not enabled, the inventory collection process will be incomplete for that device.



Note Although NETCONF typically runs over SSH or on its own port, with DNA Center, NETCONF is run over a CLI session.

For specific information about enabling NETCONF on your Cisco device, refer to that device's configuration guide. The following is an example of a typical configuration sequence on a terminal to enable NETCONF on a Cisco device:

```
#ssh server v2
#netconf agent tty
#!
#xml agent tty
#!
#commit
#end
#crypto key generate rsa
```



Note The RSA key needs to be generated to succeed with SSH. Therefore, run the **crypto key generate rsa** command in EXEC mode at the end of the configuration sequence if it has not already been done.

SNMP Trap Configuration

DNA Center uses SNMP traps (notifications) to capture a device's interface status and a host's MAC address, IP address, type, and so on. If you have Device Controllability enabled, DNA Center configures these SNMP traps for you. Otherwise, you need to enable SNMP traps and configure DNA Center's server IP address as the SNMP server. For more information about Device Controllability, see [Device Controllability](#), on page 7.

Enter the following commands in order, according to the type of device that you are configuring.

Cisco IOS Commands

```
snmp-server enable traps snmp linkdown linkup  
snmp-server host IP_address version 2c public
```

Cisco Nexus Commands

```
snmp-server enable traps snmp linkdown linkup  
snmp-server host IP_address version 2c public
```

Cisco Wireless Controller Commands

```
config trapflags client enhanced-802.11-associate enable  
config trapflags client enhanced-802.11-deauthenticate enable  
config trapflags client enhanced-authentication enable  
config trapflags client enhanced-802.11-stats enable
```

**Note**

Be sure to configure DNA Center's server IP address as the SNMP trap destination.

IP Device-Tracking Configuration

IP Device Tracking (IPDT) is one of the protocols that DNA Center uses during the discovery process to retrieve host inventory information, such as host IP addresses, MAC addresses, and network attachment points. If you have device controllability enabled, you do not need to configure IPDT manually on your devices. As part of the device controllability function, DNA Center configures IPDT or Switch Integrated Security Features (SISF) IPDT on the device based on the device type and image version that is running. If device controllability is disabled, you need to manually enable IPDT on your devices and interfaces. For more information about device controllability, see [Device Controllability, on page 7](#). For more information about whether IPDT is supported and enabled on your devices, see the configuration guide for the specific device type.

Discovery Configuration Guidelines and Limitations

The following are guidelines and limitations for DNA Center to discover your Cisco Catalyst 3000 Series Switch, Catalyst 6000 Series Switches, and Cisco ASR 9000 Series Aggregation Services Routers:

- Configure the CLI username and password with privileged EXEC mode (level 15). This is the same CLI username and password that you configure in DNA Center for the Discovery function. DNA Center requires the highest access level to the device.
- Explicitly specify the transport protocols allowed on individual lines for both incoming and outgoing connections. This configuration is achieved using the **transport input** and **transport output** commands. For information about these commands, see the command reference for the specific device type.
- Do not use the **aaa new-model** command to change the default login methods for the console port and VTY lines. DNA Center cannot discover devices that have this login method.

Perform Discovery

Discover Your Network Using CDP

You can discover devices using Cisco Discovery Protocol (CDP) or an IP address range. This procedure shows you how to discover devices and hosts using CDP. For information about discovering devices using an IP address range, see [Discover Your Network Using an IP Address Range](#), on page 31.

Before You Begin

- Enable CDP on your network devices.
- Configure your network devices as described in [Discovery Prerequisites](#), on page 26.
- Configure your network device's host IP address as the client IP address.

Procedure

Step 1 From the DNA Center home page, click **Discovery**.

Step 2 Enter a name in the **Discovery Name** field.

Step 3 Expand the **IP Ranges** area, if it is not already visible, and configure the following fields:

- For **Type**, click **CDP**.
- In the **IP Address** field, enter a seed IP address for the DNA Center to use to start the discovery scan.
- (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the discovery scan

and click



You can enter the address as an individual IP address ($x.x.x.x$) or as a classless inter-domain routing (CIDR) address ($x.x.x.x/y$) where $x.x.x.x$ refers to the IP address and y refers to the subnet mask. The subnet mask can be a value from 0 to 32.

Repeat this step to exclude multiple subnets from the discovery job.

- (Optional) In the **CDP Level** field, enter the number of hops from the seed device that you want to scan. Valid values are from 1 to 16. The default value is 16. For example, CDP level 3 means that CDP will scan up to three hops from the seed device.
- In the **Preferred Management IP** field, click the drop-down list to select either **None** or **Use Loopback**. Select **None** to use the device's IP address or **Use Loopback IP** to use the device's loopback interface IP address as its management IP address. If you choose **Use Loopback IP** and the device does not have a loopback interface, DNA Center chooses a management IP address using the logic described in [Preferred Management IP Address](#), on page 26.

Note To use the loopback interface IP address as the preferred management IP address, make sure that the CDP neighbor's IP address is reachable from DNA Center.

Step 4 Expand the **Credentials** area and configure the credentials that you want to use for the discovery job. Choose any of the global credentials that have already been created or configure your own discovery credentials. If you configure the credentials, you can choose to save them for future jobs by clicking the **Save as global settings** check box.

- a) Make sure that the global credentials that you want to use are checked. If you do not want to use a credential, remove it by clicking the check mark.
- b) To add additional credentials, click **Add Credentials**, configure the fields, and click **Add**. For information about these fields, see the following sections:

- [Configure CLI Credentials, on page 14](#)
- [Configure SNMPv2c Credentials, on page 15](#)
- [Configure SNMPv3 Credentials, on page 16](#)
- [Configure SNMP Properties, on page 9](#)
- [Configure HTTPS Credentials, on page 18](#)

- Note**
- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
 - With the **Device Controllability** option enabled, DNA Center configures devices that do not have SNMP credentials with the SNMP credentials set in DNA Center.
 - CLI credentials are not required to discover hosts; hosts are discovered through the network devices that they are connected to.

Step 5 (Optional) To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

- a) Click the names of the protocols that you want to use. A green check mark indicates that the protocol is selected.
Valid protocols are **SSH** (default) and **Telnet**.
- b) Drag and drop the protocols in the order that you want them to be used.

Step 6 Click **Start**.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices for the selected discovery.


Discover Your Network Using an IP Address Range

You can discover devices using Cisco Discovery Protocol (CDP) or an IP address range. This procedure shows you how to discover devices and hosts using an IP address range. For information about discovering devices using CDP, see [Discover Your Network Using CDP, on page 30](#).

Before You Begin

Your devices must have the required device configurations, as described in [Discovery Prerequisites, on page 26](#).

Procedure

-
- Step 1** From the DNA Center **Home** page, click **Discovery**.
- Step 2** Enter a name in the **Discovery Name** field.
- Step 3** Expand the **IP Ranges** area, if it is not already visible, and configure the following fields:
- For **Type**, click **Range**.
 - In the **IP Ranges** field, enter the beginning and ending IP addresses (IP address range) for DNA Center to scan and click . You can enter a single IP address range or multiple IP addresses for the discovery scan.
 - (Optional) Repeat Step b to enter additional IP address ranges.
 - From the **Preferred Management IP** drop-down list, choose either **None** or **Use Loopback**. Select **None** to use the device's IP address or **Use Loopback IP** to use the device's loopback interface IP address as its management IP address. If you choose **Use Loopback IP** and the device does not have a loopback interface, DNA Center chooses a management IP address using the logic described in [Preferred Management IP Address](#), on page 26.
- Step 4** Expand the **Credentials** area and configure the credentials that you want to use for the discovery job. Choose any of the global credentials that have already been created or configure your own discovery credentials. If you configure the credentials, you can choose to save them for future jobs by clicking the **Save as global settings** check box.
- Make sure that the global credentials that you want to use are checked. If you do not want to use a credential, remove it by clicking the check mark.
 - To add additional credentials, click **Add Credentials**, configure the fields, and click **Save**. For information about these fields, see the following sections:
 - [Configure CLI Credentials](#), on page 14
 - [Configure SNMPv2c Credentials](#), on page 15
 - [Configure SNMPv3 Credentials](#), on page 16
 - [Configure SNMP Properties](#), on page 9
 - [Configure HTTPS Credentials](#), on page 18
- Note**
- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
 - With the **Device Controllability** option enabled, DNA Center configures devices that do not have SNMP credentials with the SNMP credentials set in DNA Center.
 - CLI credentials are not required to discover hosts; hosts are discovered through the network devices that they are connected to.
- Step 5** (Optional) To configure the protocols that are to be used to connect with devices, expand the **Advanced** area and do the following tasks:
- Click the protocols that you want to use. A green check mark indicates that the protocol is selected. Valid protocols are **SSH** (default) and **Telnet**.

b) Drag and drop the protocols in the order that you want them to be used.

Step 6 Click **Start**.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices for the selected discovery.

Manage Discovery Jobs

Stop and Start a Discovery Job

Procedure

Step 1 From the DNA Center home page, click **Discovery**.

Step 2 To stop an active discovery job, perform these steps:

- a) From the **Discoveries** pane, select the corresponding discovery job.
- b) Click **Stop**.

Step 3 To restart an inactive discovery job, perform these steps:

- a) From the **Discoveries** pane, select the corresponding discovery job.
 - b) Click **Start**.
-

Clone a Discovery Job

You can clone a discovery job and retain all of the information defined for the job.

Before You Begin

You have run at least one discovery job.

Procedure

Step 1 From the DNA Center home page, click the **Discovery** tool.

Step 2 From the **Discoveries** pane, select the discovery job.

Step 3 Click **Clone**.

DNA Center creates a copy of the discovery job, named *Copy of Discovery_Job*.

- Step 4** (Optional) Change the name of the discovery job.
 - Step 5** Define or update the parameters for the new discovery job.
-

Delete a Discovery Job

You can delete a discovery job whether it is active or inactive.

Before You Begin

You have run at least one discovery job.

Procedure

- Step 1** From the DNA Center home page, select the **Discovery** tool.
 - Step 2** From the **Discoveries** pane, select the discovery job that you want to delete.
 - Step 3** Click **Delete**.
 - Step 4** Click **OK** to confirm.
-



Manage Your Device Inventory

- [About Device Inventory, page 35](#)
- [Device Inventory and Cisco ISE Authentication, page 41](#)
- [Device Inventory Tasks, page 41](#)
- [Add a Device Manually, page 42](#)
- [Filter Devices, page 46](#)
- [Change Devices Layout View, page 46](#)
- [Change Device Role \(Device Inventory\), page 47](#)
- [Add or Remove a Device Tag in Device Inventory, page 48](#)
- [Delete a Device, page 49](#)
- [Update Device Credentials, page 49](#)
- [Update Device Polling Interval, page 53](#)
- [Resynchronize Device Information, page 53](#)
- [Use a CSV File to Import and Export Device Configurations, page 54](#)

About Device Inventory


DNA Center displays the device information gathered during the discovery process in the **Device Inventory** window. To access the **Device Inventory** window, from the DNA Center home page, click the **Device Inventory** tool.

DNA Center maintains the device inventory by polling the devices every 25 minutes. (The polling interval is set to 25 minutes by default, but you can change this setting to suit your network requirements.) Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than a day are displayed. This prevents any stale device data from being displayed. On an average, polling 500 devices takes approximately 20 minutes.

[Table 8: Device Inventory Window Elements, on page 36](#) describes the main elements in the **Device Inventory** window.

For information about the actions that you can perform from the **Device Inventory** window, see [Device Inventory Tasks](#), on page 41.

Table 8: Device Inventory Window Elements

Window Element	Description
Add Device	Discover a specific device and add it to your device inventory. If authentication of the device fails due to invalid credentials, the device enters a collection failure state. For information, see Add a Device Manually , on page 42.
	Choose one of the following layouts or customize your own layout. For a list of the columns, see Table 9: Device Inventory Information , on page 37. <ul style="list-style-type: none"> • Status—Layout shows the Device Name, IP Address, Reachability Status, Up Time, Last Updated Time, Poller Time, and Last Inventory Collection Status. • Hardware—Layout shows the Device Name, IP Address, MAC Address, IOS/Firmware, Platform, Serial Number, Last Inventory Collection Status, Config, and Device Family. • Tagging—Layout shows the Device Name, IP Address, MAC Address, Config, Device Role, Location, and Device Tag.
Filters	Refine the list of devices that are displayed in the table by device name, IP address, last inventory collection status, and location. To remove or change the filters, click Reset .

The **Device Inventory** table displays the following information for each discovered device. All of the columns, except the **Config** column, 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.

Table 9: Device Inventory Information

Column	Description
Device Name	<p>Name of the device.</p> <p>Click the name to display the Device Overview dialog box with the following information:</p> <ul style="list-style-type: none">• Name• IP Address• MAC Address• IOS Version• Up Time• Product Id• Associated WLC• Interface Name, MAC Address, and Status of the interfaces on the device. <p>Note The device name is displayed in red a device whose inventory has not been updated for more than 30 minutes.</p>
IP Address	IP address of the device.

Column	Description
Reachability Status	<p>State of the device.</p> <ul style="list-style-type: none"> • Connecting—DNA Center is connecting to the device. • Reachable—DNA Center has connected to the device and is able to execute Cisco commands using the CLI . <p>A failure indicates that DNA Center connected to the device, but was unable to execute Cisco commands using the CLI. This status usually indicates that the device is not a Cisco device.</p> <ul style="list-style-type: none"> • Authentication Failed—DNA Center has connected to the device, but is unable to determine what type of device it is. This status also may indicate that the device is not a Cisco device. • Unreachable—DNA Center is unable to connect to the device. <p>Note If credentials are not provided at the time a discovery request is made or earlier, the device status becomes Not reachable. You should perform a new discovery with the correct credentials.</p>
MAC Address	MAC address of the device.
IOS/Firmware	Cisco IOS software that is currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Up Time	Period of time that the device has been up and running.
Config	<p>Configuration information. Click View to display detailed configuration information similar to what is displayed in the output of the show running-config command.</p> <p>Note This feature is not supported for access points and WLCs. Therefore, configuration data is not returned for these device types.</p>

Column	Description
<p>Device Role</p>	<p>Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If DNA Center is unable to determine a device role, it sets the device role as unknown.</p> <p>Note DNA Center can change the device role as the network topology changes, but if you manually change the device role, then the role will not change as the network topology changes.</p> <p>If desired, you can use the drop-down list in this column to change the assigned device role. The following device roles are available:</p> <ul style="list-style-type: none"> • Unknown • Access • Core • Distribution • Border Router
<p>Location</p>	<p>Tag that you can apply to a device to denote its geographic location. By applying the same tag to several devices, you can group them based on a common attribute. The Device Inventory window and Topology window support location tags.</p> <p>Use the following guidelines when creating location tags:</p> <ul style="list-style-type: none"> • Location tag information is maintained only in DNA Center and not deployed to or derived from the device itself. • A location defined in DNA Center is not the <i>civic-location</i> of the property that some devices support. • Location tags cannot be attached to hosts. • You can apply only one location tag to a device. However, you can use both a location tag and a device tag together.

Column	Description
Device Tag	<p>Tag assigned to devices to identify them by a common attribute. For example, you can create a tag and use it to group devices based on a platform ID or the Cisco IOS release.</p> <p>A number in the Tag column indicates how many tags have been applied to that device.</p> <p>Note You can use both a location tag and a device tag together.</p> <p>For information about adding or removing device tags, see Add or Remove a Device Tag in Device Inventory, on page 48.</p> <p>For information about deleting a tag, see Delete a Device, on page 49.</p>
Policy Tag	<p>Tag applied to a group of devices that will share the same policy.</p>
Last Updated Time	<p>Most recent date and time that DNA Center scanned the device and updated the database with new information about the device.</p>
Device Family	<p>Group of related devices, such as routers, switches and hubs, or wireless controllers.</p>
Device Series	<p>Series number of the device, for example, Cisco Catalyst 4500 Series Switches.</p>
Last Inventory Collection Status	<p>Status of the last discovery scan for the device:</p> <ul style="list-style-type: none"> • Managed—Device is in a fully managed state. • Partial Collection Failure—Device is in a partial collected state and not all the inventory information has been collected. Move the cursor over the Information (i) icon to display additional information about the failure. • Unreachable—Device cannot be reached and no inventory information was collected due to device connectivity issues. This condition occurs when periodic collection takes place. • Wrong Credentials—If device credentials are changed after adding the device to the inventory, this condition is noted. • In Progress—Inventory collection is occurring.

Device Inventory and Cisco ISE Authentication

After you provision a device, DNA Center authenticates the device with Cisco ISE. If Cisco ISE is not reachable (no RADIUS response), the device uses the local login credentials (what are the local login credentials?). If Cisco ISE is reachable but the device does not exist in Cisco ISE or its credentials do not match the credentials configured in DNA Center, the device does not fall back to use the local login. Instead, it goes into a partial collection state.

To avoid this situation:

- Make sure to add the credentials that you used for discovering the device to Cisco ISE.
- Do not configure device credentials that have fewer than 4 alphanumeric characters. Although devices may have credentials with fewer than 4 alphanumeric characters, Cisco ISE allows 4 alphanumeric characters as the minimum username and password length. If the device credentials have fewer than 4 characters, DNA Center cannot collect the device's inventory data, and the device goes into a partial collection state.
- Do not use credentials that have the same username but different passwords (cisco/cisco123 and cisco/pw123). While DNA Center allows the discovery of devices with the same username but different passwords, Cisco ISE does not allow this. If a duplicate username is used, DNA Center cannot authenticate the device and collect its inventory data, and the device goes into a partial collection state.

Device Inventory Tasks

You can perform several actions from the **Device Inventory** window. To display the action buttons, check a check box next to a device (or check the check box at the top of the list to select all devices).

Table 10: Device Inventory Buttons

Button	Action
Set Device Tags	Groups devices according to common attributes. For more information, see Add or Remove a Device Tag in Device Inventory , on page 48.
Delete	Deletes the selected devices from inventory. For more information, see Delete a Device , on page 49.
Update Credentials	Changes the credentials of the selected devices. In future discoveries, these credentials are used for the selected devices instead of the global or job-specific credentials. For more information, see Update Device Credentials , on page 49
Update Polling Time	Updates the polling interval of the selected devices. These device-specific settings override the global and job-specific settings for the selected devices. For more information, see Update Device Polling Interval , on page 53.

Button	Action
Resync (Resynchronize Devices)	Polls the selected devices for updated device information and status. For more information, see Resynchronize Device Information, on page 53 .
Export	Saves the device inventory information as a CSV file. You provide a password to encrypt the CSV file. Users who want to import the file must enter this password to open the exported file. For more information, see Export Device Configurations, on page 55 .
Import Device(s)	Updates the devices in inventory with the information from an imported file. Device synchronization is started. Access Points are ignored in the device import operation. DNA Center provides a sample template in the GUI.

Add a Device Manually

Procedure

-
- Step 1** From the DNA Center home page, click **Device Inventory**.
- Step 2** Click **Add Device**.
- Step 3** In the **Add Device** dialog box, enter the device's IP address in the **Device IP** field.
- Step 4** In the **Compute Device** field, choose either **TRUE** or **FALSE**, as follows:
- If the device is a Network Functions Virtualization (NFV) or data center device, choose **TRUE** and go to the next step.
 - If the device is not an NFV or data center device, choose **FALSE** and go to Step 6.

The default is **FALSE**.

- Step 5** If you chose **TRUE** for the **Compute Device** field, configure the **HTTP(S)** fields and click **Add**.

Table 11: HTTPS Credentials

Field	Description
Username	Name used to authenticate the HTTPS connection.
Password	Password used to authenticate the HTTPS connection.

Field	Description
Port	Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

Step 6 In the **SNMP** area, choose the SNMP version from the **Version** drop-down list (**V2C** or **V3**). If you chose **V2C**, configure the following fields:

Table 12: SNMP v2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMP v2c settings that you are adding. • Read Community—Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMP v2c settings that you are adding. • Write Community—Write community string used to make changes to SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

If you chose **V3**, configure the following fields:

Table 13: SNMP v3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires, and whether the message should be authenticated. Select one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv—Provides authentication or encryption. • AuthNoPriv—Provides authentication but does not provide encryption. • AuthPriv—Provides both authentication and encryption.

Field	Description
Auth Type	<p>Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Select one of the following authentication types:</p> <ul style="list-style-type: none"> • SHA—Authentication based on HMAC-SHA. • MD5—Authentication based on HMAC-MD5.
Auth Password	<p>SNMPv3 password used for gaining access to information from devices that use SNMPv3. Passwords (or passphrases) must be at least 8 characters in length.</p> <p>Note</p> <ul style="list-style-type: none"> • For several Cisco Wireless Controllers (WLC), passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords results in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	<p>Privacy type. (Enabled if you select AuthPriv as a the authentication mode.) Select one of the following privacy types:</p> <ul style="list-style-type: none"> • DES—DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. • AES128—CBC mode AES for encryption. • None—No privacy.
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long.</p> <p>Note</p> <ul style="list-style-type: none"> • For several Cisco WLCs, passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords will result in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7 Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and configure the fields.

Table 14: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 0-4. The default is 3.

Field	Description
Timeout (in Seconds)	Number of seconds DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 5-120 in intervals of 5 seconds. The default is 5.

Step 8 Expand the **CLI** area, if it is not already expanded, and configure the following fields:

Table 15: CLI Credentials

Field	Description
Protocol	Network protocol that enables DNA Center to communicate with remote devices. Valid values are SSH2 or Telnet . If you plan to configure the NETCONF port (see next step), you need to choose SSH2 as the network protocol.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, enter the password again as confirmation. Note Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. For security reasons, enter the enable password again. Note Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 9 Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field. NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Step 10 Click **Add**.

Filter Devices



Note To remove or change the filters, click **Reset**.

Before You Begin

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

Procedure

- Step 1** From the DNA Center home page, click **Device Inventory**.
- Step 2** Click **Filters**.
The following filters are displayed:
- **Device Name**
 - **IP Address**
 - **Last Inventory Collection Status**
- Step 3** Enter the appropriate value in the selected filter field, for example, for the **Device Name** filter, enter the name of a device.
DNA Center presents you with auto-complete values as you enter values in the other fields. Choose one of the suggested values or finish entering the desired value.
You can also use a wildcard (asterisk) with these filters, for example, you can enter values with an asterisk at the beginning, end, or in the middle of a string value.
- Step 4** Click the plus (+) icon to filter the information.
The data displayed in the **Devices** table is automatically updated according to your filter selection.
- Note** You can use several filter types and more than one value per filter.
- Step 5** (Optional) If needed, add more filters.
To remove a filter, click the **x** icon next to the corresponding filter value.
-


Change Devices Layout View

Before You Begin

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

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.

Step 2 Click  and choose one of the following layout presets:

- **Status**—Displays general device status information, including **Up Time**, **Update Frequency**, and **Number of Updates**.
- **Hardware**—Displays hardware information, including **IOS/firmware**, **Serial Number**, and **Device Role**.
- **Tagging**—Displays tagging information, including **Device Role**, **Location**, and **Tag**.

Step 3 To customize your layout, select the columns that you want to display. A blue check mark next to a column means that the column is displayed in the table.

Change Device Role (Device Inventory)

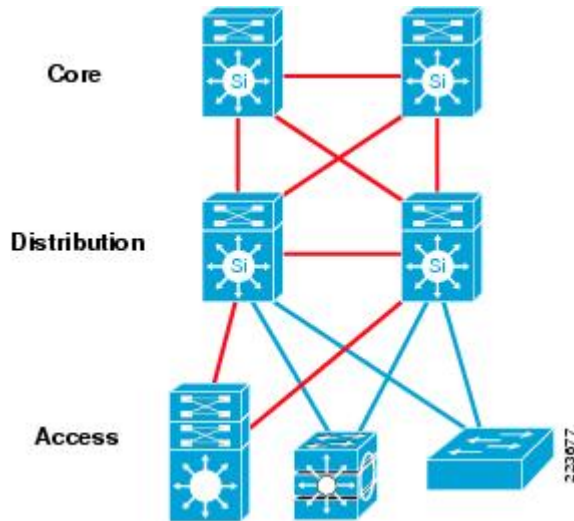
During the discovery process, DNA Center assigns a role to each of the discovered devices. Device roles are used to identify and group devices according to their responsibilities and placement in the network.

A device can have one of the following roles:

- **Unknown**—Device role is unknown.
- **Access**—Device is located in and performs the tasks required of the access layer, first tier, or edge of the network.
- **Border Router**—Device performs tasks required of a border router.
- **Distribution**—Device is located in and performs the tasks required of the distribution layer of the network.

- **Core**—Device is located in and performs the tasks required of the core of the network.

Figure 2: Device Roles and Network Locations



Before You Begin

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

Procedure

-
- Step 1** From the DNA Center home page, click **Device Inventory**.
- Step 2** Locate the device whose role you want to change and choose a new role from the **Device Role** drop-down list.
Valid choices are **Unknown**, **Access**, **Core**, **Distribution**, or **Border Router**.
-

Add or Remove a Device Tag in Device Inventory

You can group devices according to common attributes by applying device tags. For example, you can apply device tags to group devices according to their platform ID or Cisco IOS release. A single device can have multiple device tags; similarly, a single device tag can be applied to multiple devices.

Before You Begin

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

Procedure

Step 1 From the DNA Center home page, click **Device Inventory**.


Step 2 Check the check box next to the devices and click **Set Device Tags**.

Note For a single device, click the number displayed in the **Device Tag** column.


Step 3 Do one of the following tasks:

- To apply a device tag, from the **Available Tags** list, click the tags that you want to apply to the selected devices.

Note If the tag is not in the list, you can add a new tag by clicking +, entering a name for the tag, and clicking the check mark.

- To remove a device tag, from the **Applied Tags** list, click  next to the tag that you want to remove from the selected devices list.

Note The **Applied Tags** list is populated only if at least one of the selected devices has a tag applied to it.

Step 4 Click  to close the dialog box.

Delete a Device

You can delete devices from the DNA Center database.

Before You Begin

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

Procedure

Step 1 From the DNA Center home page, click the **Device Inventory** tool.

Step 2 Check the check box next to the device or devices that you want to delete.

Note You can select multiple devices by clicking additional check boxes, or you can select all devices by clicking the check box at the top of the list.

Step 3 Click **Delete**.

Update Device Credentials

You can update the discovery credentials of selected devices. The updated settings override the global and job-specific settings for the selected devices.

Before You Begin

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

Procedure

-
- Step 1** From the DNA Center home page, click **Device Inventory**.
- Step 2** Select the devices that you want to update.
- Step 3** Click **Update Credentials**.
- Step 4** Click **OK** to confirm this action.
- Step 5** From the **Update Credentials** dialog box, expand the **SNMP** area, if it is not already expanded.
- Step 6** From the **Version** field, choose the SNMP version (**V2C** or **V3**).
- Note** Because both the SNMP and CLI credentials are updated together, we recommend that you provide both credentials. If you provide only SNMP credentials, DNA Center saves only the SNMP credentials, and the CLI credentials are not updated.
- Step 7** Depending on the whether you choose **V2C** or **V3**, enter information in the remaining fields, which are described in the following tables.

Table 16: SNMP v2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMP v2c settings that you are adding. • Read Community—Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMP v2c settings that you are adding. • Write Community—Write community string used to make changes to SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Table 17: SNMP v3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.

Field	Description
Mode	<p>Security level that an SNMP message requires, and whether the message should be authenticated. Select one of the following modes:</p> <ul style="list-style-type: none"> • noAuthNoPriv—Provides authentication or encryption. • AuthNoPriv—Provides authentication but does not provide encryption. • AuthPriv—Provides both authentication and encryption.
Auth Type	<p>Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Select one of the following authentication types:</p> <ul style="list-style-type: none"> • SHA—Authentication based on HMAC-SHA. • MD5—Authentication based on HMAC-MD5.
Auth Password	<p>SNMPv3 password used for gaining access to information from devices that use SNMPv3. Passwords (or passphrases) must be at least 8 characters in length.</p> <p>Note</p> <ul style="list-style-type: none"> • For several Cisco Wireless Controllers (WLC), passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords results in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	<p>Privacy type. (Enabled if you select AuthPriv as a the authentication mode.) Select one of the following privacy types:</p> <ul style="list-style-type: none"> • DES—DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. • AES128—CBC mode AES for encryption. • None—No privacy.
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long.</p> <p>Note</p> <ul style="list-style-type: none"> • For several Cisco WLCs, passwords (or passphrases) must be at least 12 characters long. Failure to ensure these required minimum character lengths for the passwords will result in devices not being discovered, monitored, or managed by DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

- Step 8** Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and complete the following fields:

Table 18: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 0-4. The default is 3.
Timeout (in Seconds)	Number of seconds DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 5-120 in intervals of 5 seconds. The default is 5.

- Step 9** Expand the **CLI** area, if it is not already expanded, and complete the following fields:

Note Both the SNMP and CLI credentials are updated together, so you need to provide both credentials. If you provide only SNMP credentials, DNA Center saves only the SNMP credentials. The CLI credentials are not updated.

Table 19: CLI Credentials

Field	Description
Protocol	Network protocol that enables DNA Center to communicate with remote devices. Valid values are SSH2 or Telnet . If you plan to configure the NETCONF port (see next step), you need to choose SSH2 as the network protocol.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, enter the password again as confirmation. Note Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. For security reasons, enter the enable password again. Note Passwords are encrypted for security reasons and are not displayed in the configuration.

- Step 10** Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field.

NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Step 11 Click **Update**.

Update Device Polling Interval

You can update the polling interval at the global level for all devices by choosing **Settings > Network Resync Interval** or 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.

If you do not want a device to be polled, you can disable polling.

Before You Begin

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

Procedure

- Step 1** From the DNA Center home page, click **Device Inventory**.
 - Step 2** Select the devices that you want to update.
 - Step 3** Click **Update Polling Interval**.
 - Step 4** From the **Update Resync Interval** dialog box, in the **Status** field, click **Enabled** to turn on polling or click **Disabled** to turn off polling.
 - Step 5** In the **Polling Time** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24-hours).
 - Note** The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, DNA Center continues to use the device-specific polling time.
 - Step 6** Click **Update**.
-

Resynchronize Device Information

You can select the devices to be polled immediately for updated device and status information, regardless of the polling interval that is set. A maximum of 40 devices can be resynchronized at the same time.

Procedure

- Step 1** From the DNA Center home page, click **Device Inventory**.
 - Step 2** Select the devices that you want to gather information about.
 - Step 3** Click **Resync**.
 - Step 4** Confirm the resynchronization by clicking **OK**.
-

Use a CSV File to Import and Export Device Configurations

CSV File Import

If you want to use a CSV file to import your device configurations or sites from another source into DNA Center, you can download a sample template by choosing (from the DNA Center home page) **Device Inventory** > **Import Devices**. Click **Download** to download a sample CSV file template.

When you use a CSV file to import device or site configurations, the extent to which DNA Center can manage your devices, depends on the information you provide in the CSV file. If you do not provide values for CLI username, password, and enable password, DNA Center will have limited functionality and cannot modify device configurations, update device software images, and perform any other valuable functions.

You can specify the credential profile in the CSV file to apply the credentials to a set of devices. If you specify the credential profile and also enter the values manually in the CSV file, then the manually entered credentials take higher priority and the device is managed based on a combination of manually entered credentials and credential profile. For example, if the CSV file contains a credential profile with SNMP and Telnet credentials in addition to manually entered SNMP credentials, then the device is managed based on the manually entered SNMP credentials and the Telnet credentials in the credential profile.



Note

You must also provide values for the fields that correspond to the protocol you specify. For example, if you specify SNMPv3, you must specify values for the SNMPv3 fields in the sample CSV file such as the SNMPv3 username and authorization password.

For partial inventory collection in DNA Center, you must provide the following values in the CSV file:

- – Device IP address
- – SNMP version
- – SNMP read-only community strings
- – SNMP write community strings
- – SNMP retry value
- – SNMP timeout value

For full inventory collection in DNA Center, you must provide the following values in the CSV file:

- Device IP address

- SNMP version
- SNMP read-only community strings
- SNMP write community strings
- SNMP retry value
- SNMP timeout value
- Protocol
- CLI username
- CLI password
- CLI enable password
- CLI timeout value

CSV File Export

DNA Center enables you to create a CSV file that contains all or selected devices in the device inventory. When you create this file, you must enter a password to protect the configuration data that the file will contain.

Import Device Configurations From a CSV File

You can import device configurations from a CSV file.

Procedure

-
- Step 1** From the DNA Center **Home** page, click **Device Inventory**.
 - Step 2** Click **Import Device(s)** to import all of the devices from the CSV file into **Device Inventory**.
 - Step 3** Drag and drop the CSV file into the boxed area in the **Bulk Import** dialog box or click the dotted-line boxed area and browse to the CSV file.
 - Step 4** In the **Export Device** dialog box, enter a password that will be used to encrypt the exported CSV file. Users will need to supply this password to open the exported file.
 - Step 5** Click **Import**.
-

Export Device Configurations

When you export the device list to a file, all of the device configurations are exported into a CSV file. The file is then compressed and encrypted using a password that you set. The exported file includes device credentials but does not include credential profiles.



Caution

Handle the CSV file with care because it lists all of the credentials for the exported devices. Ensure that only users with special privileges perform a device export.

Procedure

- Step 1** From the DNA Center home page, click **Device Inventory**.
- Step 2** Click **Export All** to export all of the devices in the inventory or select the devices that you want to export and click **Export**.
- Step 3** In the **Export Device** dialog box, enter a password that will be used to encrypt the exported CSV file. You need to supply this password to open the exported file.
- Step 4** Confirm the encryption password and click **Export**.
- Note** Depending on your browser configuration, you can save or open the compressed file.
-



Manage Software Images

- [About Software Image Management, page 57](#)
- [Viewing Software Images, page 57](#)
- [Import Software Images, page 58](#)
- [About Golden Software Images, page 58](#)
- [Provision Software Images, page 58](#)

About Software Image Management

DNA Center stores all of the software images and software image updates (SMUs) for the devices in your network. Software Image Management provides the following functions:

- **Repository**—DNA Center stores all unique software images according to image type and version. You can view, import, and delete software images.
- **Provision**—You can push software images to the devices in your network.

Viewing Software Images

After you run discovery or manually add devices, DNA Center automatically stores all of the software images and software image updates (SMUs) for the devices.

Procedure

- Step 1** Choose **Design > Image Management** or select **Image Management** from the DNA Center home page. The software images are displayed according to device type.
 - Step 2** In the **Image Name** column, click the downward arrow to view all the software images for the specified device type family. After you select an image type, the **Using Image** field updates to indicate how many devices are using the image you specified.
 - Step 3** In the **Version** column, click the **SMU** box to view a list of SMUs versions used.
 - Step 4** Click the star in the **Mark Golden** column to indicate this is a "golden" software image. See [About Golden Software Images](#), on page 58 for more information.
-

Import Software Images

You can import a software image from your local computer or from a URL.

Procedure

- Step 1** Choose **Design > Image Management** or select **Image Management** from the DNA Center home page.
 - Step 2** Click **Import Image/SMU**.
 - Step 3** Select **Choose File** to navigate to a software image stored locally or enter a URL from where to import the software image.
 - Step 4** Click on the star next to **Make Golden** to indicate this is a "golden" software image.
 - Step 5** Click **Import**. A window appears showing the progress of the import.
-

About Golden Software Images

DNA Center allows you to designate software images and software image updates (SMUs) as *golden*. A golden software image or SMU is an ideal image for a particular device type. Designating a software image or SMU as golden saves you time by eliminating the need to make repetitive configuration changes and ensures consistency across your devices. You can designate both an image and a corresponding SMU as golden to create a standardized image.

You cannot mark a SMU as golden unless the image to which it corresponds is also marked golden.

Provision Software Images

You can push software images to the devices in your network.

Procedure

- Step 1** Choose **Provision**, then select the device whose image you want to upgrade.
 - Step 2** From the Select Devices pulldown menu, click **Update OS Image**.
 - Step 3** Click **Update**, then click **OK** to acknowledge that the device will reload after the image is upgrade.
 - Step 4** To view the progress of the image upgrade, you can open a console session to the device.
-



Display Your Network Topology

- [About Topology, page 61](#)
- [Display Device Data, page 64](#)
- [Aggregate and Disaggregate Devices, page 65](#)
- [Configure the Topology Structure, page 67](#)
- [Save a Topology Layout, page 68](#)
- [Open a Saved Topology Layout, page 69](#)
- [Change Device Role \(Topology Layout\), page 69](#)
- [Search for Devices and Hosts, page 70](#)
- [Add or Remove a Device Tag in Topology, page 71](#)
- [Display Devices with Tags, page 72](#)

About Topology

The **Topology** window displays a graphical view of your network. Using the discovery settings that you have configured, DNA Center discovers and maps devices to a physical topology with detailed device-level data.

The topology map provides the following key features:

- Auto visualization of Layer 2 and Layer 3 topologies on top of the physical topology for a granular view for design planning and simplified troubleshooting.
- For a Layer 2 topology, display of configured VLANs within your network. For a Layer 3 topology, display of OSPF, IS-IS, and so on, depending on what is currently configured and is in use in your network.
- Device information.

Topology Tools

The **Topology** page provides tools to help you view, filter, and manipulate the topology map.

Table 20: Main Topology Tools

Name or Icon	Description
Search	Searches for a device by device name, device type, or IP address. As you enter information into this field, the DNA Center displays matches. Select the device from the results that appear. The selected device appears in the Topology page.
Filter	<p>Allows you to filter what is shown on the topology map. For each filter, you can make additional adjustments using the Advanced options.</p> <ul style="list-style-type: none"> • Connections—Displays the devices according to the number of their connections. Starting from the left, first devices with no connections are displayed, then devices with one connection, then devices with two connections, and so on. There are no advanced options to refine the display. • Enterprise Collapsed—Displays a hierarchical layout of aggregated devices and links in your network topology. Advanced options allow you to refine the view by device family, role and branch. Aggregation options allow you to choose the degree to which specified nodes overlap on the map. • Enterprise Expanded—Displays a hierarchical layout of disaggregated devices and links in your network topology. Advanced options allow you to refine the view by device family, role and branch. Aggregation options allow you to choose the degree to which specified nodes overlap on the map. • Spiral—Displays a circular layout of the devices and links in your network topology. The topology is arranged starting from a central device (or cloud) with links and devices expanding out from this central point. Advanced options allow you to refine the view by radius and spacing.
Zoom In and Zoom Out	Minimizes and maximizes the topology map.
Legend	Defines the device icons that are used in the map.
Save	<p>Allows you to save the currently displayed layout and take these actions on previously saved layouts:</p> <ul style="list-style-type: none"> • Load a previously saved layout. • Save changes to a previously saved layout. • Set a layout as the default. • Delete a layout.
:	Displays additional topology tools that allow you to change the topology view, filter devices that are displayed, and other actions. For more information, see Table 21: Additional Topology Tools, on page 63

Table 21: Additional Topology Tools

Tool	Description
View Tools	
Color	Toggles the color of the devices between displaying them in different colors or in a single color. Note Devices are displayed in multiple colors by default.
Links	Toggles the display of links between devices.
Hosts	Toggles the display of hosts in the topology.
Center	Positions the topology in the middle of the pane.
Rotate	Toggles the orientation of the topology from landscape to portrait.
Details	Toggles the display of the number of links between devices.
Curved Links	Toggles the shape of the lines that represent the links. Lines can be either straight or curved.
Filter Tools	
Layers	Displays devices with the following attributes on the topology map: <ul style="list-style-type: none"> • Layer 2—Displays devices based on the selected VLAN or Layer 2 protocol. Choose either a VLAN or one of the Layer 2 protocols. • Layer 3—Displays devices based on the selected Layer 3 protocol. The following Layer 3 protocols are available: <ul style="list-style-type: none"> ◦ Intermediate System-to-Intermediate System (IS-IS) ◦ Open Shortest Path First (OSPF) ◦ Enhanced Interior Gateway Routing Protocol (EIGRP) ◦ Static-Route • VRF—Displays devices that have Virtual Routing and Forwarding (VRF) tables. Note The default Layer 3 topology shows all Layer 3 protocols.

Tool	Description
Device Tags	Displays the available device tags. Clicking a device tag highlights the devices that have this tag. You can create and apply a tag to devices by selecting the device, clicking Tag Device , and creating and applying the tag to a device.
Action Tools	
Aggregation	Enables or disables device aggregation. Aggregating devices means grouping devices together. You can group devices in any way that makes sense to you. You can save the layout for future reference by clicking the Save icon. This grouping does not effect the physical configuration on the devices. Aggregation is enabled by default.
Multiselect	Allows you to select multiple devices by dragging the mouse over the desired devices or shift-clicking on devices. You can also select multiple groups of devices by clicking shift and dragging the mouse over a group of devices. After selecting the group of devices, you can aggregate or tag them. If you aggregate devices of different product families, the DNA Center shows them as generic devices (without a device type) and the number of devices. Multiselect is off by default.
Full Capture	Downloads a screen shot of your topology.
View Capture	Downloads a screen shot of the current topology view.

Display Device Data

You can display data for a specific device in the **Topology** window. Displaying device data is helpful when troubleshooting network connectivity issues between devices.



Note

The device data that is accessible in the **Topology** window is also accessible in the **Device Inventory** window.

The following device data is available:

- Location (This information is displayed if the selected device icon has a location marker background. Click the **Location** link to display the topology of the devices that share that location marker.)
- Type
- Device role (For information about changing a device's role, see [Change Device Role \(Device Inventory\)](#), on page 47.)

- IP address
- MAC address
- OS (operating system)
- Software version
- Ports
 - Gigabit Ethernet ports
 - 10-Gigabit Ethernet ports
 - Management ports
- VLAN (if it exists)
- Number of connections
- List of connected devices (Each connected device shows its device type icon and the number of connections. Clicking on a connected device displays the details for that device.)
- Tags

Before You Begin

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

Procedure

Step 1 From the DNA Center home page, click **Topology**.

Note If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears.

Step 2 Click a location marker to display the topology for that location.

Step 3 To display data for a specific device, click that device in the **Topology** window.

Step 4 To display a list of aggregated devices:

- a) In the **Topology** window, click an **aggregated devices** icon.
 - b) In the **Device Details** pane, click the device name to view the corresponding device data.
 - c) Click the **Node List** link to return to the list of aggregated devices.
-

Aggregate and Disaggregate Devices

The following topics describe how to aggregate and disaggregate devices:

- [Aggregate Devices](#), on page 66
- [Disaggregate Devices](#), on page 66
- [Change the Aggregated Devices Label](#), on page 66

Aggregate Devices

Before You Begin


- Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.
- Determine how the devices within your network configuration should be visually grouped and organized.

Procedure

Step 1 From the DNA Center home page, click **Topology**.

Step 2 Drag and drop a device icon onto another device icon.
The two devices are aggregated.

Note

To aggregate multiple devices, click  and then **Multiselect**. Use the mouse to select multiple devices and click **Aggregate**.

Disaggregate Devices

Before You Begin

- Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.
- Determine how the devices within your network configuration should be visually grouped and organized.

Procedure

Step 1 From the DNA Center home page, click **Topology**.

Step 2 Click a group of aggregated devices.
A list of the aggregated devices is displayed.

Step 3 Click **Disaggregate All** to ungroup the aggregated devices.

Change the Aggregated Devices Label

The default label for aggregated devices is the number of devices and the device type (*number_devicetypes*). However, you can change this default label to one that is meaningful in the context of your network topology.

Before You Begin

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

- Determine how the devices within your network configuration should be visually grouped and organized.

Procedure

-
- Step 1** From the DNA Center home page, click **Topology**.
 - Step 2** Click an **aggregated devices** icon.
A list of the aggregated devices is displayed. At the top of the list is the aggregated devices label.
 - Step 3** Click the aggregated devices label to open an edit field where you can change the label.
 - Step 4** Change the label, and then click outside of the edit field to save your changes.
-


Configure the Topology Structure

You can choose from three default topology layouts. You can also modify the overall size of the topology graph, the spacing that separates individual elements, and more.

Before You Begin

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

Procedure

-
- Step 1** From the DNA Center **Home** page, click **Topology**.
 - Step 2** From the **Topology** toolbar, click .
 - Step 3** From the **Select View** drop down list, choose a view option. Available options are **Connections**, **Enterprise Collapsed**, **Enterprise Expanded**, or **Spiral**.
 - Step 4** Click the **Show Advanced Options** button to configure how each filter is displayed. Click the **Hide Advanced Options** button to return to the basic view.

Filter	Basic View	Advanced View
Connections	<p>Arranges the device icons from left to right based on the number of connections, from least to most.</p> <p>Note Aggregated devices are disaggregated in this view.</p>	<p>Connections—Use the slider to adjust the amount of space between the connections.</p> <p>Node overlap—Use the slider to adjust the amount of space between the nodes.</p> <p>centralizeY—When checked, the device icons are centered along the Y axis. When unchecked, the device icons are aligned to the Y axis.</p> <p>Note Choose x or y from the drop-down list next to each slider to change how the device icons are displayed, horizontally or vertically.</p>


Filter	Basic View	Advanced View
Enterprise Collapsed and Enterprise Expanded	<p>Arranges the device icons into a structured hierarchical view, from top to bottom.</p> <p>The Enterprise Collapsed option shows aggregated devices and the Enterprise Expanded shows the devices disaggregated.</p>	<p>ADVANCED VIEW</p> <ul style="list-style-type: none"> • Family Type—Use the slider to adjust the amount of space between the device icons based on their device types. • Device Role—Use the slider to adjust the amount of space between the device icons based on their device roles. • Branch— Use the slider to adjust the amount of space between the branches. <p>AGGREGATION</p> <ul style="list-style-type: none"> • Node overlap—Use the slider to adjust the amount of space between the nodes. • Check the check boxes corresponding to the device types that you want displayed.
Spiral	<p>Arranges the device icons from a central device with other devices connected to it.</p>	<p>AGGREGATION</p> <ul style="list-style-type: none"> • Radius—Use the slider to adjust the number of devices from the center to the outer edge of the spiral. • Spacing—Use the slider to adjust the space between devices.

Save a Topology Layout

Before You Begin

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

Procedure


-
- Step 1** From the DNA Center home page, click **Topology**.
- Step 2** From the **Topology** toolbar, click .
- Step 3** In the **Topology Title** field, enter a name for the topology and click **Save as New**.
- Step 4** Click **OK**.
-

Open a Saved Topology Layout

Before You Begin

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

Procedure

-
- Step 1** From the DNA Center home page, click **Topology**.
 - Step 2** From the **Topology** toolbar, click .
 - Step 3** Click the **Folder** icon next to the topology layout that you want to open.
 - Step 4** Click **OK**.
The topology layout opens in the **Topology** window.
-

Change Device Role (Topology Layout)

During the scan, each discovered device is automatically assigned a device role. The device role is used for identifying and grouping devices according to their responsibilities and placement within the network.

A device can have one of the following roles within the DNA Center:

- **Unknown**—Device role is unknown.
- **Access**—Device performs the tasks required for the access layer or first tier/edge.
- **Border Router**—Device performs the tasks required for a border router.
- **Distribution**—Device performs tasks required for the distribution layer.
- **Core**—Device performs tasks required for the core.

You can change the device role when you select a device and display the device data.




Note

You can also change the device role from the **Device Inventory** window.

Before You Begin

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

Procedure

- Step 1** From the DNA Center home page, click **Topology**.
- Step 2** In the **Topology** window, click a device to select it.
- Step 3** Choose a role from the **Role** drop-down list. Valid roles are **Access**, **Core**, **Distribution**, and **Border Router**.
- Step 4** (Optional) Select additional devices and change their device roles.
- Step 5** Click  on the **Topology** toolbar.
- Step 6** (Optional) Select a filter from the drop-down list. Valid options are **Connections**, **Enterprise Collapsed**, **Enterprise Expanded** and **Spiral**.
-

Search for Devices and Hosts

You use the DNA Center search function to locate specific devices or hosts within your network. This function allows you to search the network using any string value. To locate a specific device or host quickly, use any of the following values in the search field:

- Device or host name
- Aggregation label
- IP address
- Device role
- Device type



Note The search function supports fragmented results. For example, if you enter **12** in the search field, you will get results for devices with IP addresses or device names that contain 1 and 2 (.12, .120, .102, 10.20, 1-switch2, etc).

Before You Begin

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

Procedure

- Step 1** From the DNA Center **Home** page, click **Topology**.
- Note** If you added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker on the map to display the Topology for that location.
- Step 2** From the **Topology** toolbar, enter a keyword in the **Search Topology** field. As you begin typing, DNA Center displays a list of possible matches to your entry.
- Note** You can click the **x** in the search field to clear the search keyword field and the results.

- Step 3** Click on a device from the search results to highlight that device and its links in the **Topology** window. Click on the device again to display detailed data for that device.
- Step 4** Proceed with any provisioning or troubleshooting tasks on the located devices or hosts.
-

What to Do Next

Search using other string values for other devices or hosts within your network, or perform other tasks including the following:

- Viewing the data for specific devices
- Applying tags to devices within your network
- Host a meeting using the topology co-editor to collaborate with other users in real-time on the network

Add or Remove a Device Tag in Topology

In the **Topology** window, you can add device tags to associate devices that share a common attribute. For example, you can create a tag and use it to group devices based upon a platform ID, Cisco IOS releases, or location. Similarly, you can remove tags from devices.





Note Applying a tag to a host is not supported.

Before You Begin

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

Procedure

- Step 1** From the DNA Center home page, click **Topology**.
- Step 2** Click the device or devices you want to tag. To select more than one device, click the **Multiselect** icon.
Note To deselect devices, click outside of the selected device.
The **Device Information** dialog box appears.
- Step 3** Click **Tag Devices**.
- Step 4** In the **Available Device Tags** column, click a tag to apply it to the selected device or devices. If the tag that you want does not exist, create it by clicking , entering the name of the tag in the **Device Tag Name** field and pressing **Enter**.
- Step 5** Click  to close the dialog box.
-

Display Devices with Tags

To display tagged devices in the **Topology** window, perform the following steps.

Before You Begin

- Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.
- Make sure that you have created tags and applied them either through the **Device Inventory** window or the **Topology** window.

Procedure

- Step 1** From the DNA Center home page, click **Topology**.
- Step 2** From the Topology toolbar, click the **Tags**.
- Step 3** To identify the devices associated with a tag, click the tag. To return the devices to their normal display, click the tag again.
Tags are color-coded. When you click a tag, a circle of the same color is drawn around its associated devices.
- Note** You can click more than one tag at a time. The tag that you choose to display first is the innermost circle around the device, followed by the next tag as the next circle, and so on.
-



Design Your Network

- [Design A New Network Infrastructure, page 73](#)
- [About Network Hierarchy, page 74](#)
- [Create Sites in the Network Hierarchy, page 74](#)
- [Add Floors to Buildings, page 75](#)
- [Edit Floors, page 76](#)
- [Place Cisco APs on a Floor, page 77](#)
- [Upload Existing Site Hierarchy, page 77](#)
- [Search the Network Hierarchy, page 77](#)
- [Configure Global Wireless Settings, page 78](#)

Design A New Network Infrastructure

The Design area is where you create the structure and framework of your network including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. You use the Design workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the [About Discovery](#) feature.

You perform these tasks in the Design area:

Procedure

- Step 1** Create your network hierarchy. See [Create Sites in the Network Hierarchy, on page 74](#).
 - Step 2** Define global network settings. See [About Global Network Settings, on page 11](#).
 - Step 3** Define network profiles.
-

About Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations. Your network hierarchy can contain sites, which contains buildings and areas. You create site and building IDs so that later, you can easily identify where to apply design settings or configurations.

- **Areas** don't have a physical address (i.e., United States). You can think of areas as the largest element. Areas can contain buildings and subareas. For example, an area called United States can contain a subarea called California. And the subarea California can contain a subarea called San Jose. By creating areas, you can apply common settings across a large area.
- **Buildings** have physical address and contain floors and floor plans. When you create a building, you must specify a physical address and latitude and longitude coordinates. Buildings cannot contain areas. By creating buildings, you can apply settings to a specific area.


You can

- Create a new network hierarchy. See [Create Sites in the Network Hierarchy, on page 74](#).
- Upload an existing network hierarchy from Cisco Prime Infrastructure. See [Upload Existing Site Hierarchy, on page 77](#).

Create Sites in the Network Hierarchy

DNA Center allows you to easily define physical sites and then specify common resources for those sites. The Design application uses a hierarchical format for intuitive use, while eliminating the need to redefine the same resource in multiple places when provisioning devices. By default, there is one site called Global. You can add additional sites, buildings, and areas to your network hierarchy. You must create at least one site before you can use the Provision features.


Procedure

- Step 1** Choose **Design**. A world map is displayed.
 - Step 2** Click **Add Site**.
 - Step 3** Choose whether to create an area or a building. You can also upload an existing hierarchy.
 - Step 4** Enter a name for the site or building and select a parent node. By default, Global is the Parent Node.
 - Step 5** When you add a building, you must enter an address in the Address field. As you enter the address, the Design App narrows down the known addresses to the one you enter. When you see the correct address appear in the window, select it. When you select a known address, the longitude and latitude coordinates fields are automatically populated.
 - Step 6** Click **Add**. The area or building you created is added under the Global site.
 - Step 7** To add another area or building, in the hierarchy frame, click the gear icon  next to an existing area or building that you want to be the parent node.
-

Add Floors to Buildings

After you add a building, you can create floors and upload a floor map.

Procedure

- Step 1** Choose **Design > Network Hierarchy**.
- Step 2** Expand the Global site and the previously created area to see all the previously created buildings.
- Step 3** Click the gear icon  next to the building for which you want to add a floor, then click **Add Floor**.
- Step 4** Complete the required fields. The Floor Name field has a 21 character limit. The floor name must start with a letter or a hyphen (-) and the string following the first character can include one or more of the following:
 - Upper and/or lower case letters
 - Numbers
 - Underscores (_)
 - Hyphens (-)
 - Periods (.)
- Step 5** Click **Add**.
- Step 6** You can then drag a floor plan on to the map or upload a file. DNA Center supports the following file types: .jpg, .gif, .png, .dxf, and .dwg.

After you upload a floor plan, you should see the map displayed in the window.

Figure 3: Example Floor Plan



Edit Floors

After you add a floor, you can edit the floor map so that it contains the obstacles, areas, and APs contained on the floor.

Procedure

- Step 1** Choose **Design > Network Hierarchy**.
- Step 2** Expand the network hierarchy to find the floor you want to edit, or enter the floor name in the Search Hierarchy field.
- Step 3** Click on the name of the floor you want to edit. The floor map appears.

Place Cisco APs on a Floor

Procedure

- Step 1** Choose **Design > Network Hierarchy**.
 - Step 2** Expand the network hierarchy to find the floor you want to edit, or enter the floor name in the **Search Hierarchy** field.
The floor map is displayed in the right pane.
 - Step 3** Click **Manage Floor APs**.
The **Add APs** dialog box, which lists the available APs along with the AP Name and AP Mode details, appears. The table also lists APs that are not assigned to any floors.
 - Step 4** Click **Add** adjacent to the AP that you want to place on the floor map.
The APs that are added appear on the right side of the floor map.
 - Step 5** To position the APs correctly on the floor map, click and drag each AP to the appropriate location on the floor map, or click an AP point icon on the floor map to open the **Properties** window and set the horizontal and vertical position for that AP.
 - Step 6** Click **Save**.
 - Step 7** (Optional) Hover your cursor over an AP icon on the floor map to view the corresponding details.
-

Upload Existing Site Hierarchy

You can upload a CSV file that contains an existing network hierarchy. For example, you can upload a CSV file with location information that you exported from Cisco Prime Infrastructure. See [Export Device Configurations](#), on page 55 for information about how to export devices.

Procedure

- Step 1** Choose **Design > Network Hierarchy**, then click **Create Site**.
 - Step 2** At the bottom of the form, click **Upload CSV**. If you don't have an existing CSV file, click **Download Template** to download a CSV file you can edit and then upload.
 - Step 3** Navigate to where your CSV file is located, then click **Open**. The site hierarchy is uploaded.
-

Search the Network Hierarchy

You can search the network hierarchy to quickly find a site, building, or area. This is particularly helpful after you've added a large number of sites, areas, or buildings.

Procedure

- Step 1** To search the tree hierarchy, place your cursor in the Search Hierarchy window and enter the test on which you want to search. The tree is filtered on the information you enter in the search window.
- Step 2** To search the map view, place your cursor in the Search Buildings window and enter the name of the building for which you want the map view to display.
-

Configure Global Wireless Settings

Global wireless network settings include settings for Service Set Identifier (SSID), wireless interfaces, and wireless radio frequency.

**Note**

Creating wireless interfaces and wireless radio frequency is applicable only for nonfabric deployments.

The following sections provide information about how to define various global wireless network settings:

- [Create SSIDs for an Enterprise Wireless Network, on page 78](#)
- [Create SSIDs for a Guest Wireless Network, on page 80](#)
- [Create a Wireless Interface, on page 83](#)
- [Create a Wireless Radio Frequency Profile, on page 84](#)

Create SSIDs for an Enterprise Wireless Network

This workflow shows how to:

- 1 Create SSIDs.
- 2 Create wireless profiles.
- 3 Associate SSIDs to wireless profiles.

Procedure

- Step 1** Choose **Design > Network Settings > Wireless**.
- Step 2** Under **Enterprise Wireless**, click + **Add** to create a new SSID for the enterprise network. In the **Create an Enterprise Wireless Network** window, configure the following parameters:

- Step 3** Enter an SSID name in the **Wireless Network Name (SSID)** field.
- Step 4** Select the **Type of Enterprise Network: Voice and Data** or **Data Only**. This selection defines the quality of service (QoS).
- Step 5** Check the **Fast Lane** check box to enable fastlane capability on this network.
- Step 6** Under **Level of Security** area, select the encryption and authentication type for this network. The security options are:
- **WPA2 Enterprise**—Provides a higher level of security using Extensible Authentication Protocol (EAP) (802.1x) to authenticate and authorize network users with a remote RADIUS server. If you select **WPA Enterprise**, check the **MAC Filtering** check box to enable MAC-based access control on an SSID.
 - **WPA2 Personal**—Provides good security using a passphrase or a preshared key (PSK). Allows anyone with the passkey to access the wireless network. If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.
 - **Open**—Provides no security. Allows any device to access the wireless network without any authentication.
- Step 7** Click **Next**. The **Wireless Profiles** window is displayed. You can associate this SSID with the corresponding wireless profile. See [Step Step 4](#) to associate an SSID with the existing wireless profile, [Step Step 3](#) to create a new wireless profile.
- Step 8** In the **Wireless Profiles** window, click **+Add** to create a new wireless profile. The **Create a Wireless Profile** window appears. Configure the following:
- -
 -
 -
- Step 9** Enter the profile name in the **Wireless Profile Name** text box.
- Step 10** Specify whether the SSID is **Fabric** or **Non-Fabric** by selecting **Yes** or **No**.
- For Non-Fabric SSID, select the authentication method: **Central** or **Local to VLAN**. For central authentication, from the **Interface Name** drop-down list, select the interface name. For local authentication, Cisco WLC redirects the HTTP traffic to an internal or external server where the user is prompted to authenticate. In case of a guest user, an external server such as Cisco ISE is required for registering and self-provisioning. From the **Select ISE Authentication** drop-down list, select a Cisco ISE authentication server and enter the redirect URL in the **Redirect URL** text box. The client is redirected to the specified Cisco ISE redirect URL.
- Step 11** To assign this profile to any site, enter the site name in the **Site Selector** text box.
- Step 12** Click **Finish**. The created profile appears in the **Wireless Profiles** page.
- Step 13** To associate the SSID to wireless profile, do the following:
- On the **Wireless Profile** page, check the **Profile Name** check box(es) to associate the SSID you created in Step 2.
 - Click **Finish**.
-

What to Do Next

- 1 Perform discovery of devices. You can discover devices using CDP or using an IP address range. See [Discover Your Network Using CDP](#), on page 30 and [Discover Your Network Using an IP Address Range](#), on page 31.
- 2 Configure policies for your network. See [Configure Policies](#), on page 87.
- 3 Add Cisco WLC to a site. See [Add Devices to Sites](#), on page 102.
- 4 Provisioning Cisco WLCs and Cisco APs. See [Provision a Cisco WLC](#), on page 102 and [Provision a Cisco AP - Day 1 AP Provisioning](#), on page 103.
- 5 Add Cisco WLC to a fabric domain. See [Add Devices to a Fabric](#), on page 105.
- 6 Configure settings for the various kinds of devices ("hosts") that can access the fabric domain, see [Configure Host Onboarding](#).

Create SSIDs for a Guest Wireless Network

This workflow shows how to:

- 1 Create SSIDs.
- 2 Create wireless profiles.
- 3 Associate SSIDs to wireless profiles.
- 4 Guest portal customization.

Procedure

-
- Step 1** Choose **Design > Network Settings > Wireless**.
- Step 2** Under **Guest Wireless**, click **+Add** to create new SSIDs.
In the **Create a Guest Wireless Network** window, configure the following parameters:
- Step 3** Enter an SSID name in the **Wireless Network Name (SSID)** text box.
- Step 4** Under **Level of Security**, select the encryption and authentication type for this guest network. The security options are: **Web AUTH** and **Open**.
- **WEB AUTH**—Provides higher level of layer 3 security.
 - Note** The WEB AUTH option is disabled if you do not have Cisco ISE configured on the DNA Center server. Cisco ISE acts as a RADIUS server for web authentication.
 - **Open**—Provides no security. Allows devices to connect to the wireless network without any authentication.
- Step 5** Select the authentication server: **ISE Authentication** or **External Authentication**. For ISE Authentication, configure the following:
- Select the type of portal you want to create from the **WHAT KIND OF PORTAL ARE YOU CREATING TODAY ?** drop-down list:

- **Self Registered**—The guests are redirected to the Self-Registered Guest portal to register by providing information to automatically create an account.
- **HotSpot** —The guests can access the network without credentials.

Step 6 Select where you want to redirect the guests after successful authentication from the **WHERE WILL YOUR GUESTS REDIRECT AFTER SUCCESSFUL AUTHENTICATION ?** drop-down list:

- **Success Page**—The guests are redirected to an authentication success page.
- **Original URL**—The guests are redirected to the URL they had originally requested.
- **Custom URL**—The guests are redirected to the custom URL that is specified here. You need to enter a redirect URL in the **Redirect URL** text box.

Step 7 Click **Next**. The **Wireless Profiles** window is displayed. You can associate this SSID with the corresponding wireless profile. See [Step Step 4](#) to associate an SSID with the existing wireless profile, and [Step Step 3](#) to create a new wireless profile.

Step 8 In the **Wireless Profiles** window, click **+Add** to create a new wireless profile. The **Create a Wireless Profile** window appears.

- Enter the profile name in the **Wireless Profile Name** text box.
- Specify whether the SSID is **Fabric** or **Non-Fabric** by selecting **Yes** or **No**.
- To assign this profile to any site, enter the site name in the **Site Selector** field.
- Click **Save**. The created profile appears in the **Wireless Profiles** page.

Step 9 To associate the SSID to wireless profile, do the following:

- On the **Wireless Profiles** page, check the **Profile Name** check box(es) to associate the SSID.
- Click **Next**.

The **Portal Customization** page appears. You can assign the SSID to a guest portal.

Step 10 On the **Portal Customization** page, click **+ Add** to create the guest portal. The **Portal Builder** page appears. See [Create a Guest Portal Page](#) to create custom portals. The created portal appears in the **Portal Customization** page.

- Under **Portals**, select the radio button next to **Portal Name** to assign the SSID to guest portal.

Step 11 Click **Finish**.

What to Do Next

- 1 Perform discovery of devices. You can discover devices using CDP or using an IP address range. See [Discover Your Network Using CDP, on page 30](#) and [Discover Your Network Using an IP Address Range, on page 31](#).
- 2 Configure policies for your network. See [Configure Policies, on page 87](#).
- 3 Add Cisco WLC to a site. See [Add Devices to Sites, on page 102](#).

- 4 Provisioning Cisco WLCs and Cisco APs. See [Provision a Cisco WLC, on page 102](#) and [Provision a Cisco AP - Day 1 AP Provisioning, on page 103](#).
- 5 Add Cisco WLC to a fabric domain. See [Add Devices to a Fabric, on page 105](#).
- 6 Configure settings for the various kinds of devices ("hosts") that can access the fabric domain, see [Configure Host Onboarding](#).

Create a Guest Portal Page

You can create the following guest portal pages:

- Login Page
- Registration Page
- Registration Success
- Success Page

Procedure

- Step 1** Navigate to the portal page you are creating.
- Step 2** Enter the portal name in the **Portal Name** text box.
- Step 3** Expand **Page Content** in the left menu to include various variables while creating portal pages.
 - List of variables for Login page:
 - Access Code
 - Header Text
 - AUP
 - Text Fields
 - List variables for Registration page:
 - First Name
 - Last Name
 - Phone Number
 - Company
 - Sms Provider
 - Person being visited
 - Reason for a visit
 - Header text
 - User Name
 - Email Address

- AUP
- List of variables for Registration page:
 - Account Created
 - Header texts
- Variables for Success page:
 - Text fields

Step 4 Drag and drop variables in to the portal template page and edit them.

Step 5 To customize the default color scheme in the portal, expand **Color** in the left menu and change the color of these page elements:

- Body text Border
- Link text Page
- Background
- Border Color
- Header Background

Step 6 To customize the font, expand **Font** in the left menu and change the following:

- Typeface
- Header
- Title text
- Body text
- Form label

Step 7 Click **Save** to save the portal.

Create a Wireless Interface

Creating wireless interfaces is applicable for nonfabric deployment.

Procedure

Step 1 Choose **Design > Network Settings > Wireless**.

Step 2 Under **Wireless Interfaces**, click **+Add**.
The **New Interfaces** window appears.

- In the **Interfaces Name** text box, enter the dynamic interface name.

- (Optional) In the **VLAN ID** text box, enter the VLAN ID for the interface. The valid range is 0 to 4094.
 - Click **Ok**. The created interface appears under Wireless Interfaces.
-

Create a Wireless Radio Frequency Profile

Creating wireless radio frequency profile is applicable for Non-Fabric deployment.

Procedure

- Step 1** Choose **Design > Network Settings > Wireless**.
- Step 2** Under **Wireless Radio Frequency Profile**, click **+Add RF**.
The **Wireless RAdio Frequency** window appears.
- Step 3** In the **Profile Name** text box, enter the Radio Frequency (RF) profile name.
- Step 4** Select at least one radio type: **2.4 GHz** or **5 GHz**.
- Step 5** Configure the following for **2.4 GHz** radio type:
- Check the **DCA Channel** check box(es) to select channels to dynamically manage channel assignment for an RF group. The available channels are: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14**.
 - Check the **Data Rates** check box (es) to specify the rates at which data can be transmitted between the access point and the client. The available data rates are: **1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, and 44**.
- Step 6** Configure the following for **5 GHz** radio type:
- Choose one of the channel bandwidth options from the **Channel Width** drop-down list: **Best, 20 MHz, 40 MHz, 80 MHz, or 160 MHz**.
 - Set the **DCA Channel** to manage the channel assignments:
 - **UNII-1 36-48**—The channels available for UNII-1 band are: **36, 40, 44, and 48**. Check the **UNII-1 36-48** check box to include all channels or check the check box (es) of the channels to select them individually.
 - **UNII-2 52-144**—The channels available for UNII-2 band are: **52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, and 144**. Check the **UNII-2 52-144** check box to include all channels or check the check box (es) of the channels to select them individually.
 - **UNII-3 149-165**—The channels available for UNII-3 band are: **149, 153, 157, 161, and 165**. Check the **UNII-3 149-165** check box to include all channels or check the check box (es) of the channels to select them individually.
 - Check the **Data Rates** check box(es) to specify the rates. the available data rates are: **6, 9, 12, 18, 24, 36, 48, and 54**.
- Step 7** Click **OK**.
-



Configure Policies

- [Policy Overview, page 87](#)
- [Policy Dashboard, page 87](#)
- [Virtual Networks, page 88](#)
- [Group-Based Access Control Policies, page 90](#)
- [Traffic Copy Policies, page 94](#)

Policy Overview

DNA Center enables you to create policies that reflect your organization's business intent for a particular aspect of the network, such as network access. DNA Center takes the information collected in a policy and translates it into network-specific and device-specific configurations required by the different types, makes, models, operating systems, roles, and resource constraints of your network devices.

Using DNA Center, you can create virtual networks, access control policies, and traffic copy policies.

Policy Dashboard

The **Policy Dashboard** window shows the number of virtual networks, group-based access control policies, traffic copy policies, and scalable groups that you have created. In addition, it shows the number of policies that have failed to deploy.

The **Policy Dashboard** window provides a list of policies and the following information about each policy:

- **Policy Name**—Name of policy.
- **Policy Type**—Type of policy. Valid types are access control and traffic copy policies.
- **Policy Version**—Iteration of policy. Each time a policy is changed and saved, it is incremented by one version. For example, you create a policy and save it. The policy is at version 1. If you change the policy and save it again, the version of the policy is incremented to version 2.
- **Modified By**—User who modified the particular version of a policy.
- **Description**—Word or phrase that identifies a policy.

- **Policy Scope**—User and device groups or applications that a policy affects.
- **Timestamp**—Date and time when a particular version of a policy was saved.

Virtual Networks

Virtual networks are isolated routing and switching environments. By default, hosts that exist within separate virtual networks cannot communicate with each other. You can use virtual networks to segment your physical network into multiple logical networks.

A typical use case is for segmenting guests, employees, and contractors into separate groups so that you can allow and restrict access to parts of the network. The different types of networks are:

- **Guest network**—Network connections provided by a company to enable their guests to gain access to the Internet and their own enterprise without compromising the security of the host enterprise network. Guests can access the Internet but cannot access internal applications that are hosted in the data center.
- **Employee network**—Network connections that allow access to the Internet and internal applications. This group can be segmented further to allow or restrict access within the enterprise network, for example, to specific internal applications, lab environments, and servers. For example, a finance employee does not need access to the development lab. Likewise, a developer does not need access to a sales forecasting application. These might be good candidates to segment into separate virtual networks.
- **Contractor network**—Network connections that allow users to access the Internet and contractor-specific applications within the enterprise network.

A virtual network may span across multiple site locations and across network domains (wireless, campus, and WAN).

Business Intent of a Virtual Network

Only the assigned user groups are allowed to enter a virtual network. Within a virtual network, users and devices can communicate with each other unless explicitly blocked by an access policy. Users across different virtual networks cannot communicate with each other. However, an exception policy can be created to allow some users to communicate across different virtual networks.

Network Rendering of a Virtual Network

By default, DNA Center has a single virtual network, and all users and endpoints belong to this virtual network. If DNA Center is integrated with Cisco Identity Services Engine (ISE), the default virtual network is populated with user groups and endpoints from Cisco ISE.

In DNA Center, the concept of virtual network is common across wireless, campus, and WAN networks. When a virtual network is created, it can be associated with sites that have any combination of wireless, wired, or WAN deployments. For example, if a site has a campus fabric deployed that includes wireless and wired devices, the virtual network creation process triggers the creation of the Service Set Identifier (SSID) and Virtual Routing and Forwarding (VRF) in the campus fabric. If the site also has WAN fabric deployed, the VRF extends from the campus to WAN as well.

During site design and initial configuration, you can add wireless devices, wired switches, and WAN routers to the site. DNA Center detects that the virtual network and the associated policies have been created for the site, and applies them to the different devices.

Guidelines and Limitations for Virtual Networks

Virtual networks have the following limitation:

- You can create only one guest virtual network.

Configure Virtual Networks


This section provides information about how to create, edit, and delete a virtual network.

Create a Virtual Network

You can create virtual network to segment your physical network into multiple logical networks.

Procedure

Step 1 From the DNA Center home page, choose **Policy > Virtual Network**.

Step 2 Click  and enter the following information:

- **Network Name**—Name of the virtual network.
- **Guest Virtual Network**—Devices that are configured with special rules, which allow guests limited access. Check this check box to configure the virtual network as a guest network. You can create only one guest virtual network.
- **Available Groups**—Scalable groups that you can choose to include in the virtual network. Drag and drop groups from the **Available Groups** area to the **Groups in the Virtual Network** area.
- **Groups in the Virtual Network**—Scalable groups that are in the virtual network. Drag and drop groups from the **Available Groups** area to the **Groups in the Virtual Network** area.

Step 3 Click **Save**.


Edit or Delete a Virtual Network

If you move a scalable group from one custom virtual network to another custom virtual network, the mappings for the scalable groups are changed. Be aware that users or devices in the group might be impacted by this change.

Procedure

Step 1 From the DNA Center home page, click **Policy > Virtual Network**.

Step 2 Do one of the following tasks:

- Select the virtual network that you want to edit, make the changes, and click **Save**. For field definitions, see [Create a Virtual Network, on page 89](#).
 - Delete the virtual network by clicking  and confirming the deletion.
-

Group-Based Access Control Policies

Group-based access control policies are Security Group Access Control Lists (SGACLs). DNA Center integrates with Cisco ISE to simplify the process of creating and maintaining SGACLs.

During the initial DNA Center and Cisco ISE integration, scalable groups and policies that are present in Cisco ISE are propagated to DNA Center and placed in the default virtual network.



Note

DNA Center does not support access control policies with logging as an action. Therefore, Cisco ISE does not propagate any such policies to DNA Center.

Depending on your organization's configuration and its access requirements and restrictions, you can segregate the scalable groups into different virtual networks to provide further segmentation.

The access contracts that you create in DNA Center define the rules that make up the group-based access control policies. They define the actions (permit/deny) performed when traffic matches a specific port or protocol and the implicit actions (permit/deny) performed when no other rules match.

After you create a group-based access control policy, DNA Center translates the policy into an SGACL, which is ultimately deployed on a device.

The following example shows the process of authentication and access control that a user experiences when logging in to the network:

- 1 A user connects to a port on a switch and provides his or her credentials.
- 2 The switch contacts Cisco ISE.
- 3 Cisco ISE authenticates the user and downloads the SGACLs to the port to which the user is connected.
- 4 The user is granted or denied access to specific users or devices (servers) based on the access granted in the SGACLs.

Prerequisite for Creating Access Control Policies

Make sure that Cisco ISE is integrated with DNA Center. Verify that the scalable groups have been propagated to DNA Center from Cisco ISE. To do this, from the DNA Center home page, choose **Policy > Virtual Network**. You should see scalable groups populated in the **Available Scalable Groups** area. If you do not see any scalable groups, check that Cisco ISE was integrated correctly. For more information, see the *Cisco Digital Network Architecture Center Installation Guide*.

Scalable Groups

Scalable groups comprise a grouping of users, end point devices, or resources that share the same access control requirements. These groups (known in Cisco ISE as security groups or SGs) are defined in the Cisco ISE. A scalable group may have as few as one item (one user, one end-point device, or one resource) in it.

Access Contracts

An access contract is a Security Group Access Control List (SGACL). It defines the set of rules that govern the network interaction between the source and destination in an access control policy.

Configure Access Control Policies

The following topics help you create and manage access-control policies.

Workflow to Configure a Group-Based Access Control Policy

Before You Begin

Make sure that you have integrated Cisco ISE with DNA Center. For more information, see [Prerequisite for Creating Access Control Policies](#), on page 90.

Procedure

	Command or Action	Purpose
Step 1	Create virtual networks. Depending on your organization's configuration and its access requirements and restrictions, you can segregate your groups into different virtual networks to provide further segmentation.	(Optional) For more information, see Create a Virtual Network , on page 89.
Step 2	Create scalable groups. After you integrate with Cisco ISE, the scalable groups that exist in ISE are propagated to DNA Center. If a scalable group that you need does not exist, you can create it.	(Optional) For more information, see Create a Scalable Group , on page 92.
Step 3	Create an access control contract. A contract defines a set of rules that dictate the action (allow or deny) that network devices perform based on traffic matching particular protocols or ports.	For more information, see Create an Access Control Contract , on page 92.
Step 4	Create a group-based access control policy. The access control policy defines the access control contract that governs traffic between source and destination scalable groups.	For information, see Create a Group-Based Access Control Policy , on page 93

Create a Scalable Group

You can access Cisco ISE through the DNA Center interface to create scalable groups. After you have added the group in Cisco ISE, it is synchronized with the DNA Center database so that you can use it in an access policy. You cannot edit scalable groups in DNA Center; you need to edit them in Cisco ISE. For more information, see [Scalable Groups](#), on page 91.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Registry > Scalable Groups**. All of the scalable groups that have been created in Cisco ISE appear in the registry.
- Step 2** Click **Add**.
DNA Center opens a direct connection to the Cisco ISE server, where you can add the scalable group.
- Step 3** In Cisco ISE, create scalable groups (called security groups in Cisco ISE).
For more information, see the *Cisco Identity Services Engine Administrator Guide*.
- Step 4** Return to DNA Center.
-

Create an Access Control Contract

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Access Contracts**.
- Step 2** Click **Add Contract**.
- Step 3** In the **Contract Editor** dialog box, enter a name and description for the contract.
- Step 4** From the **Implicit Action** drop-down list, choose either **Deny** or **Permit**.
- Step 5** From the drop-down list in the **Action** column, choose either **Deny** or **Permit**.
- Step 6** From the drop-down list in the **Port/Protocol** column, choose a port or protocol.
Note If DNA Center does not have the port or protocol that you need, you can create your own by clicking **Add Port/Protocol**, configuring the fields, and clicking **Save**.
- Step 7** (Optional) To include more rules in your contract, click **Add** and repeat Step 5 and Step 6.
- Step 8** Click **Save**.
-

Edit or Delete an Access Control Contract



Note If you edit a contract that is used in a policy, the policy's state changes to **MODIFIED** in the **Policy Administration** window. A modified policy is considered to be stale because it is inconsistent with the policy that is deployed in the network. To resolve this situation, you need to redeploy the policy to the network.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Access Contracts**.
- Step 2** Check the check box next to the contract that you want to edit or delete and do one of the following tasks:
- To make changes to the contract, click **Edit**, make the changes, and, click **Save**.
- Note** If you made changes to a contract that is used in a policy, you need to deploy the modified policy by choosing **Policy Administration > Group-Based Access Control Policies**, checking the check box next to the policy name, and clicking **Deploy**.
- To delete the contract, click **Delete**.

Create a Group-Based Access Control Policy

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Policy Administration > Group-Based Access Control Policies**.
- Step 2** Click **Add Policy**.
- Step 3** Enter the following information:
- **Policy Name**—Name of the policy. The name can be up to 255 alphanumeric characters in length, including hyphens (-) and underscore (_) characters.
 - **Description**—Word or phrase that identifies the policy.
 - **Contract**—Rules that govern the network interaction between the source and destination scalable groups. Click **Add Contract** to choose a contract for the policy. In the dialog box, click the radio button next to the contract that you want to use. Alternatively, you can select the **permit** (permit all traffic) or **deny** (deny all traffic) contract.
 - **Enable Policy**—Determines whether or not the policy is active. If it is not active, check the check box. To disable the policy, uncheck the check box. When the policy is disabled, it is saved only to DNA Center; it is not synchronized with Cisco ISE or deployed in the network.
 - **Enable Bi-directional**—Configures the relationship of the traffic flow between the source and destination scalable groups. To enable the contract for traffic flowing in both directions (from the source to the

destination and from the destination to the source), check the **Enable Bi-directional** check box. To enable the contract for traffic flowing only from the source to the destination, uncheck the **Enable Bi-directional** check box.

- Step 4** To define the source scalable groups, drag and drop the scalable groups from the **Available Security Groups** area to the **Source Scalable Groups** area.
- Step 5** To define the destination scalable groups, drag and drop scalable groups from the **Available Security Groups** area to the **Destination Scalable Groups** area.
- Step 6** Click **Save**.
-

Edit or Delete a Group-Based Access Control Policy

You can edit or delete only policies that you created in DNA Center. Policies that were imported from Cisco ISE during the DNA Center and Cisco ISE integration cannot be edited or deleted from DNA Center. You need to edit or delete these policies from Cisco ISE.



Note If you edit a policy, the policy's state changes to **MODIFIED** on the **Policy Administration** page. A modified policy is considered to be stale because it is inconsistent with the policy that was deployed in the network. To resolve this situation, redeploy the policy to the network.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Policy Administration > Group-Based Access Control Policies**.
- Step 2** Check the check box next to the policy that you want to edit or delete.
- Step 3** Do one of the following tasks:
- To make changes, click **Edit**, make the changes, and click **Save**.

Note If you make changes to the policy, deploy the modified policy by checking the check box next to the policy name and clicking **Deploy**.
 - To delete the group, click **Delete**.
-

Traffic Copy Policies

Using DNA Center, you can set up an Encapsulated Remote Switched Port Analyzer (ERSPAN) configuration such that the IP traffic flow between two entities is copied to a specified destination for monitoring or troubleshooting.

To configure ERSPAN using DNA Center, create a traffic copy policy that defines the source and destination of the traffic flow that you want to copy. You can also define a traffic copy contract that specifies the device and interface where the copy of the traffic is sent.



Note Because traffic copy policies can contain either scalable groups or IP network groups, throughout this guide, we use the term *groups* to refer to both scalable groups and IP network groups, unless specified otherwise.

Sources, Destinations, and Traffic Copy Destinations

DNA Center simplifies the process of monitoring traffic. You do not have to know the physical network topology. You only have to define a source and destination of the traffic flow and the traffic copy destination where you want the copied traffic to go.

- **Source**—One or more network device interfaces through which the traffic that you want to monitor flows. The interface might connect to end-point devices, specific users of these devices, or applications. A source group can be comprised of Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or port channel interfaces only.
- **Destination**—The IP subnet through which the traffic that you want to monitor flows. The IP subnet might connect to servers, remote peers, or applications.
- **Traffic Copy Destination**—Layer 2 or Layer 3 LAN interface that receives a copy of the traffic flow for analysis. The interface type can be Ethernet, Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet interfaces only. When configured as a destination, the interface can be used to receive only the copied traffic. The interface can no longer receive any other type of traffic and cannot forward any traffic except that required by the traffic copy feature. You can configure trunk interfaces as destinations. This configuration allows the interfaces to transmit encapsulated traffic.



Note There can be only one traffic copy destination per traffic copy contract.

At the destination, we recommend that you use a network analyzer, such as a Switch Probe device or other Remote Monitoring (RMON) probe, to perform the traffic analysis.

Guidelines and Limitations of Traffic Copy Policy

The traffic copy policy feature has the following limitations:

- You create up to eight traffic copy policies, 16 copy contracts, and 16 copy destinations.
- The same interface cannot be used by more than one traffic copy destination.
- DNA Center does not show a status message to indicate that a traffic copy policy has been changed and is no longer consistent with the one that is deployed in the network. However, if you know that a traffic copy policy has changed since it was deployed, you can redeploy the policy.
- You cannot configure a management interface as a source group or traffic copy destination.

Configure Traffic Copy Policies

The following topics help you create and manage traffic copy policies.

Workflow to Configure a Traffic Copy Policy

Before You Begin

- To be monitored, a source scalable group that is used in a traffic copy policy needs to be statically mapped to the switches and their interfaces. For information about mapping a scalable group to a switch interface, see [Configure Ports Within the Fabric Domain, on page 108](#).
- A traffic copy policy destination group needs to be configured as an IP network group. For more information, see [Create an IP Network Group, on page 96](#).

Procedure

	Command or Action	Purpose
Step 1	Create a traffic copy destination. This is the interface on the device where the traffic flow will be copied for further analysis.	For information, see Create a Traffic Copy Destination, on page 97 .
Step 2	Create a traffic copy contract. The contract defines the copy destination.	For information, see Create a Traffic Copy Contract, on page 98 .
Step 3	Create a traffic copy policy. The policy defines the source and destination of the traffic flow and the traffic copy contract that specifies the destination where the copied traffic is sent.	For information, see Create a Traffic Copy Policy, on page 98 .

Create an IP Network Group

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > Registry > IP Network Groups**.
 - Step 2** Click **Add**.
 - Step 3** In the **Add IP Network Group** dialog box, enter a name and description for the group.
 - Step 4** In the **IP Address or IP/CIDR** field, enter an IP address or an IP address with Classless InterDomain Routing (CIDR) notation. (CIDR allows the assignment of Class C IP addresses in multiple contiguous blocks. It also allows you to add a large number of clients that exist in a subnet range by configuring a single client object.)
 - Step 5** Click **Save**.
-

Edit or Delete an IP Network Group

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Registry > IP Network Groups**.
- Step 2** In the **IP Network Groups** table, check the check box next to the group that you want to edit or delete.
- Step 3** Do one of the following tasks:
- To make changes to the group, click **Edit**. For field definitions, see [Create an IP Network Group](#), on page 96.
 - To delete the group, click **Delete** and then click **Yes** to confirm.
-

Create a Traffic Copy Destination

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Destination**.
- Step 2** Enter a name and description for the traffic copy destination.
- Step 3** Select the device and one or more ports.
- Step 4** Click **Save**.
-

Edit or Delete a Traffic Copy Destination

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Destination**.
- Step 2** Check the check box next to the destination that you want to edit or delete.
- Step 3** Do one of the following:
- To make changes, click **Edit**, make the necessary changes, and click **Save**.
 - To delete the group, click **Delete**.
-

Create a Traffic Copy Contract

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Contracts**.
- Step 2** Click **Add**.
- Step 3** In the dialog box, enter a name and description for the contract.
- Step 4** From the **Copy Destination** drop-down list, choose a copy destination..
- Note** You can have only one destination per traffic copy contract.
- If no copy destinations are available for you to choose, you can create one. For more information, see [Create a Traffic Copy Destination, on page 97](#)
- Step 5** Click **Save**.
-

Edit or Delete a Traffic Copy Contract

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Contracts**.
- Step 2** Check the check box next to the contract that you want to edit or delete.
- Step 3** Do one of the following:
- To make changes, click **Edit**make the necessary changes, and click **Save**.
 - To delete the contract, click **Delete**.
-

Create a Traffic Copy Policy

Procedure

- Step 1** From the DNA Center home page, chooo **Policy > Policy Administration > Traffic Copy Policies**.
- Step 2** Enter the following information:
- **Policy Name**—Name of the policy.
 - **Description**—Word or phrase that identifies the policy.

- Step 3** In the **Contract** field, click **Add Contract**
 - Step 4** Click the radio button next to the contract that you want to use and then click **Save**.
 - Step 5** Drag and drop groups from the **Available Groups** area to the **Source** area.
 - Step 6** Drag and drop groups from the **Available Groups** area to the **Destination** area.
 - Step 7** Click **Save**.
-

Edit or Delete a Traffic Copy Policy

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Policy Administration > Traffic Copy Policies**.
 - Step 2** Check the check box next to the policy that you want to edit or delete.
 - Step 3** Do one of the following:
 - To make changes, click **Edit**, make the necessary changes, and click **Save**.
 - To delete the policy, click **Delete**.
-



Provision Your Network

- [Provisioning, page 101](#)
- [Add Devices to Sites, page 102](#)
- [Provisioning Devices, page 102](#)
- [Delete Devices After Provisioning, page 104](#)
- [Configuring Fabric Domains, page 105](#)

Provisioning

After you have configured policies for your network in the Cisco Digital Network Architecture (DNA) Center, you must provision your devices. In this stage, you deploy the policies across your devices.

There are 3 aspects of provisioning the devices:

- Assign the devices to the inventory and deploy the required policies.
- Add the devices to the sites.
- Create fabric domains and add devices to the fabric.

Add Devices to Sites

Procedure

- Step 1** From the Cisco DNA Center home page, click **Provision**. The Inventory page displays device information gathered during the discovery process.
- Step 2** Check the check box next to the device(s) for which you want to associate to a site.
- Step 3** From the **Action** menu, choose **Add to Site**.
- Step 4** In the **Find Site** field, type the name of the site to which you want to associate the device(s). If you selected multiple devices that you want added to the same site, click the All Same Site option.
- Step 5** Click **Assign**.
-

Provisioning Devices

Provision a Cisco WLC

Before You Begin

- Make sure you have defined the following global network settings before provisioning a Cisco WLC:
 - Network servers, such as AAA, DHCP, and DNS Servers—(See [Configure Global Network Servers](#), on page 19.)
 - Device credentials such as CLI, SNMP, HTTP, and HTTPS credentials—(See [Configure CLI Credentials](#), on page 14, [Configure SNMPv2c Credentials](#), on page 15, [Configure SNMPv3 Credentials](#), on page 16, and [Configure HTTPS Credentials](#), on page 18.)
 - IP address pools—(See [Configure IP Address Pools](#), on page 19.)
 - Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—(See [Configure Global Wireless Settings](#), on page 78.)
- Make sure you have Cisco WLC in your inventory. If not, discover Cisco WLC using the Discovery function. (See [Discover Your Network](#), on page 23.)
- Make sure Cisco WLC is added to a site. (See [Add Devices to Sites](#), on page 102.)

Procedure

- Step 1** From the DNA Center home page, Choose **Provision > Devices** . The **Device Inventory** window appears.

- Step 2** Click the **Device Inventory** tab. All the discovered controllers are displayed.
- Step 3** Check the check box(es) adjacent to the controller device name that you want to provision.
- Step 4** From the **Action** drop-down list, choose **Provision**.
- Step 5** In the **Assign Site** window, assign a site for the controller. In the **Find Site** field, enter the name of the site to which you want to associate the controller. To assign multiple controllers to the same site, check the **All Same Site** check box.
- Step 6** Click **Next**.
The **Configuration** window appears.
- Step 7** In the **Managed AP Locations** field, enter the AP locations managed by controller. Here you have the option to change, remove, or reassign the site.
- Step 8** Click **Next**.
- Step 9** The **Summary** window displays the following information:
- System Details
 - Global Settings
 - SSID
 - Managed Sites
- Step 10** Click **Deploy** to provision the controller.
The **Status** column in the **Device Inventory** window shows **SUCCESS** after a successful deployment.
- Note** After provisioning, if you want to make any changes, click **Design**, change the site profile, and provision the controller again.
-

What to Do Next

- 1 Add Cisco WLC to a fabric domain. See [Add Devices to a Fabric](#), on page 105.
- 2 Configure settings for the various kinds of devices ("hosts") that can access the fabric domain. See [Configure Host Onboarding](#).

Provision a Cisco AP - Day 1 AP Provisioning

Before You Begin

Make sure you have Cisco AP in your inventory. If not, discover APs using the Discovery function. (See [Discover Your Network](#), on page 23.)

Procedure

- Step 1** From the DNA Center home page, choose **Provision > Devices**.
The **Device Inventory** window appears.

- Step 2** Click the **Device Inventory** tab. All the discovered controllers are displayed.
- Step 3** Check the check box(es) adjacent to the AP device name that you want to provision.
- Step 4** From the **Action** drop-down list, choose **Provision**.
- Step 5** In the **Assign Site** window, assign an AP to the site. In the **Find Site** field, enter the name of the site to which you want to associate the AP. To assign multiple APs to the same site, check the **All Same Site** check box.
- Step 6** Click **Next**.
The **Configuration** window appears.
- Step 7** From the **AP Rule** drop-down list, choose the RF profile for the AP. The options are: **High**, **Typical**, and **Low**. The AP group is created based on the RF profile selected.
- Step 8** Click **Deploy** to provision the AP.
You are prompted with message saying that Creation/modification of AP groups in progress. After completion, these devices will go for a reboot.
- Step 9** Click **OK**.
The **Status** column in the **Device Inventory** window shows **SUCCESS** if a deployment is successful.
-

Delete Devices After Provisioning

- If you are deleting a device that is already been added to fabric domain, remove it from the fabric domain and then delete it from the **Provision** menu.
- You cannot delete a device from the **Inventory** window if they have been provisioned. You must delete these devices from the **Provision** menu.

Procedure

- Step 1** From the DNA Center home page, choose **Provision > Devices**.
The **Device Inventory** page appears.
- Step 2** Click the **Inventory** tab, which lists all the discovered and provisioned devices.
- Step 3** Check the check box adjacent to the devices(s) that you want to delete.
Note APs are deleted only when the controller to which they are connected to is deleted.
- Step 4** From the **Action** drop-down list, choose **Delete Device**.
You are prompted with a message **Devices selected will be deleted. Are you sure you want to proceed !**.
- Step 5** Click **OK**.
-

Configuring Fabric Domains

Fabrics Overview

A fabric is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.

The DNA Center allows you to add devices to a fabric network. These devices can be configured to act as control plane or border devices within the fabric network.

Before You Begin

Ensure that your network has been designed, the policies have been retrieved from the Integrated Services Engine (ISE) or created in the DNA Center, and the devices have been inventoried and added to the sites.

Create a Fabric Domain

The DNA Center creates a default fabric domain called *Default LAN Fabric*.

To add a new fabric domain:

Procedure

-
- Step 1** From the DNA Center **Home** page, click **Provision**.
 - Step 2** Click the **New Fabric** tab.
 - Step 3** Enter a name for the fabric.
 - Step 4** From the **Select Auth** field, select an authentication protocol. This determines the type of access that devices can have when connecting to the network. The protocol selected here is applied to all devices in the fabric.
 - Step 5** Click **Add**.
-

Configure a Fabric Domain

You can add devices and associate virtual networks to a fabric domain, and add multicast address pools.

Add Devices to a Fabric

After you have created a fabric domain, you can add devices to this fabric. You can also specify whether the devices should act as a control plane node, a border node, or both.



Note It is optional to designate the devices in a fabric domain as control plane nodes or border nodes. You may have devices that do not play these roles. However, every fabric domain must have at least one control plane node device and one border node device.

There are 3 steps to add and configure devices to a fabric domain:

- 1 Select the devices.
- 2 Specify devices to act as a control plane nodes.
- 3 Specify devices to act as border nodes.

To add a device to the fabric:

Before You Begin

You must provision the device. To provision a device, click on the **Provision** tab and select **Devices**.

Procedure

- Step 1** From the DNA Center **Home** page, click **Provision**. The screen displays all provisioned fabric domains.
- Step 2** From the list of fabric domains, select a fabric. The screen displays all devices in the network that have been inventoried. You can view the devices in topology view or list view. In topology view, any device that is added to the fabric is in blue color.
- Step 3** Click on a device and select one of the options displayed.

Field	Description
Add to Fabric	Add a distribution or access device to the fabric domain.
Add as CP	Add a core or distribution device as a control plane node. This allows the fabric access device to communicate with the control plane device.
Add as Border	Add a core device as a border node. This allows the fabric access device to communicate with the fabric border device. In the pop-up window, enter the following options: <ul style="list-style-type: none"> • Set as default border—Select the check box if you want the device to act as a default border node. • Routing Protocol—Select the routing protocol for the device. • Routing Process—Select the routing process for the device.

Field	Description
Add as CP+Border	<p>Add the selected device as a control plane and a border node.</p> <p>In the pop-up window, enter the following options:</p> <ul style="list-style-type: none"> • Set as default border—Select the check box if you want the device to act as a default border node. • Routing Protocol—Select the routing protocol for the device. • Routing Process—Select the routing process for the device.
View Info	Displays the details of the selected device.
Device Role	Specify the role for the device.

Step 4 After you have added the devices, click **Save**.

Configure Host Onboarding

The **Host Onboarding** tab allows you to configure settings for the various kinds of devices ("hosts") that can access the fabric domain.

In this tab, you can:

- Select an authentication template that will apply to the fabric. These templates are pre-defined configurations that are retrieved from the ISE.
- Associate IP address pools to virtual networks.
- Specify wireless SSIDs within the network that the hosts can access.
- Apply specific configurations for each port for each access device within the fabric domain.

Select Authentication Template

You can select the authentication template that will apply for all devices in the fabric domain.

Procedure

- Step 1** From the **Auth Template** section, select the authentication template.
- Step 2** Click **Save**.

Associate Virtual Networks to the Fabric Domain

IP address pools enable host devices to communicate within the fabric domain.

When an IP address pool is configured, the DNA Center immediately connects to each node to create the appropriate SVI (switch virtual interface) to allow the hosts to communicate.

You cannot add an IP address pool, but you can configure a pool from the ones that are listed. The IP address pools listed here were created when the network was designed.

To associate a virtual network to the fabric domain:

Procedure

Step 1 From the **Virtual Networks** section, click on a virtual network.

Step 2 Configure the virtual network.

Field	Description
Select address pools	From the list of IP address pools, select the ones that should be part of the virtual network.
Choose Auth	From the dropdown, select the authentication type for the virtual network when it is associated with the fabric domain.
Choose Traffic Type	From the dropdown, select whether voice or data traffic should be sent through the virtual network.
Wireless Mgmt Pool	Select whether the virtual network should be part of the wireless management pool of the fabric domain.
AP Provisioning Pool	Select whether the virtual network should be part of the access point provisioning pool.
Flood and Learn	Enable Flood and Learn behaviour for the gateway.

Step 3 Click **Update** to save the settings. The settings you specify here will be deployed to all the devices on the network.

Step 4 When all virtual networks have been configured, click **Save**.

Configure Wireless SSIDs for the Fabric Domain

The **Wireless SSID** section allows you to specify wireless SSIDs within the network that the hosts can access.

Configure Ports Within the Fabric Domain

The **Select Port Assignment** section allows you to configure each access device on the fabric domain. You can specify network behavior settings for each port on each device.



Note The settings you make here for the ports will override the general settings you have made for the device in the **Virtual Networks** section earlier.

To configure the ports:

Procedure

- Step 1** From the **Select Fabric Device** section, select the access device that you want to configure. The ports available on the device are displayed.
- Step 2** Select the ports on the device and specify the allowed IP address pool, the groups that have been provisioned, the voice or data pool, and the authentication type for the port.
- Step 3** When you have specified the settings for the ports, click **Save** to save the settings for the device.

Configure Multicast Settings

After devices have been added to the fabric domain, you can create multicast IP address pools and rendezvous points.

Multicast IP address pools group the endpoints in the fabric domain.

A Rendezvous Point (RP) is a router in a multicast network domain that acts as a shared root for a multicast shared tree. Any number of routers can be configured to work as RPs and they can be configured to cover different group ranges. For correct operation, every multicast router within a Protocol Independent Multicast (PIM) domain must be able to map a particular multicast group address to the same RP.

Create a Multicast IP Address Pool

To create a multicast IP address pool:

Procedure

- Step 1** From the DNA Center **Home** page, click **Provision** . The screen displays all provisioned fabric domains.
- Step 2** From the list of fabric domains, select a fabric. The screen displays the devices in the network. Any device that is added to the fabric is highlighted in blue color.
- Step 3** Go to the **Advanced Settings** tab. The **Select Multicast Address Pool** displays all IP address pools that have been created.
- Step 4** Click the **Add** button. You can now specify the multicast addresses that should form a pool.

Field	Description
Subnet / Mask	Enter the subnet IP address and subnet mask for the multicast pool.

Field	Description
Contexts	Select one or more contexts or VRFs that this multicast pool will become a part of.

Step 5 Click **OK**.

Step 6 Click **Save** on the main screen.

Add a Device as Rendezvous Point

To add a Device as rendezvous point:

Procedure

- Step 1** From the DNA Center **Home** page, click **Provision** . The screen displays all provisioned fabric domains.
- Step 2** From the list of fabric domains, select a fabric. The screen displays the devices in the network. Any device that is added to the fabric is highlighted in blue color.
- Step 3** Go to the **Advanced Settings** tab and scroll down to the **Rendezvous Points** section.
- Step 4** Click on a router that you want to add as a rendezvous point and select **Make Rendezvous Point**.
- Step 5** Click **Save** on the main screen.



Configure Telemetry

- [About Telemetry Collection, page 111](#)
- [Configuring Telemetry Collection, page 111](#)

About Telemetry Collection

DNA Center collects information about user's experience with DNA Center and securely transfers it to the Cisco Clean Access Agent (CAA) infrastructure at Cisco.

This information is collected for the following reasons:

- To proactively identify issues, if any, with DNA Center.
- To better understand the DNA Center features that are most frequently used.
- To improve and enhance the overall user experience.


Telemetry collection is enabled by default, but you can disable it if you want to opt out.

Configuring Telemetry Collection

Before You Begin

You must have successfully deployed the DNA Center and it must be operational.

Procedure

- Step 1** From the DNA Center home page, click .
- Step 2** Choose **System Settings > Settings**.
- Step 3** Click **Telemetry Collection**.

Note Telemetry collection is enabled by default.

Step 4 (Optional) To review the agreement for telemetry collection, click **End User License Agreement**.

Step 5 (Optional) To disable telemetry collection, uncheck the **Telemetry Collection** check box and click **Update**.




Manage Users

- [Change User Password, page 113](#)
- [Edit User Roles, page 113](#)
- [Change Password Policy, page 114](#)
- [Change Authentication Timeout, page 114](#)

Change User Password

You can change the password to log in to the DNA Center server.


Procedure

- Step 1** Click the gear icon  in the upper right corner, then select **System Settings**.
 - Step 2** Click the **User Management** tab, then click **Change Password**.
 - Step 3** Complete the required fields, then click **Update**.
-

Edit User Roles

You can modify user's roles to control which functions they can perform.


Procedure

- Step 1** Click the gear icon  in the upper right corner, then select **System Settings**.
 - Step 2** Click the **User Management** tab, then click **Internal Users**. This list of users and their respective role is displayed.
 - Step 3** Click **Edit** next to the user whose role you want to modify.
 - Step 4** Select a role from the Role pulldown menu, then click **Save**.
-

Change Password Policy

You can change the number of invalid attempts users can make before they are temporarily locked out of the DNA Center server. You can also modify how long users must wait before attempting to log in again.


Procedure

- Step 1** Click the gear icon  in the upper right corner, then select **System Settings**.
 - Step 2** Click the **User Management** tab, then click **Password Policy**.
 - Step 3** Enter a number in the **Number of Invalid Attempts** field. If you enter 0, users can enter as many attempts as necessary without being locked out of the server.
 - Step 4** In the **Temporary Account Lock** field, select a time value in which users are temporarily locked out of the DNA Center server.
 - Step 5** Click **Save**.
-

Change Authentication Timeout

You can specify when DNA Center automatically logs off users.

Procedure

- Step 1** Click the gear icon  in the upper right corner, then select **System Settings**.
 - Step 2** Click the **User Management** tab, then click **Authentication Time Out**.
 - Step 3** In the **Idle Timeout** field, select a time value for which idle users will be automatically logged out if they exceed. The default idle timeout value is 30 minutes.
 - Step 4** In the **Session Timeout** field, select a time value for which users will be automatically logged out if they exceed. The default idle session timeout value is 6 hours.
 - Step 5** Click **Save**.
-



Back Up and Restore Cisco DNA Center

- [About Backup and Restore, page 115](#)
- [Back Up the DNA Center, page 116](#)
- [Restore DNA Center , page 117](#)

About Backup and Restore

The backup and restore procedure for DNA Center can be used for the following purposes:

- To create a single backup file for disaster recovery
- To create a single backup file to restore to a different appliance (if required for your network configuration)

Backup

When you perform a backup, DNA Center creates a copy of the following files as a single file and exports the file to a specific location on the appliance:

- DNA Center database
- DNA Center file system and files
- X.509 certificates and trustpools
- Usernames and passwords
- Any user uploaded files (for example, any Network Plug and Play image files)

The database and files are compressed into a single `.backup` file. The maximum size of the `.backup` file is 30 GB. This number consists of a permitted 20 GB maximum size for a file service backup and a 10 GB permitted maximum size for the database backup.



Note

The `.backup` file should not be modified by the user.

Only a single backup can be performed at a time. Performing multiple backups at once are not permitted. Additionally, only a full backup is supported. Other types of backups (for example, incremental back ups) are not supported.

After saving the backup file, you can download it to another location in your network.

While a backup is being performed, you will be unable to delete any files that have been uploaded to the file service and any changes that you make to files might not be captured by the backup process.

When performing a backup, we recommend the following:

- Perform a backup everyday to maintain a current version of your database and files.
- Perform a backup after making any changes to your configuration. For example, when changing or creating a new policy on a device.
- Only perform a backup during a low impact or maintenance time period.

**Note**

You cannot schedule or automate a backup. In addition, after starting a backup, you cannot manually cancel it.

Restore

When you restore the backup file, DNA Center overwrites the existing database and files with the files contained in the backup file. You can restore the backup file from its default location on the appliance or drag and drop the backup file from its location in your network.

When a restore is being performed, DNA Center is unavailable.

**Note**

You cannot schedule or automate the restore process. In addition, after starting a restore process, you cannot manually cancel it.


Back Up the DNA Center

You can back up and restore the DNA Center database and files. When you perform a backup, DNA Center copies and exports the database and files as a single file to a location on the appliance. When you restore the backup file, DNA Center overwrites the existing database and files with the files contained in the backup file. For more information about the backup and restore process, see [About Backup and Restore](#), on page 115.

Before You Begin

You must have successfully deployed DNA Center and it is operational.

Procedure

-
- Step 1** From the DNA Center home page, click  > **System Settings** > **Backup & Restore**.
- Step 2** Click **Create New Backup**.
The **Backup in Progress** is displayed.

During this process, DNA Center creates a compressed *.backup* file of the database and files. This backup file is also given a time and date stamp that is reflected in its file name. The following file naming convention is used: *yyyy-mm-dd-hh-min-seconds* (year-month-day-hour-seconds).

For example:

backup_2015_08_14-08-35-10

Note If necessary, you can rename the backup file instead of using the default time and date stamp naming convention.

The backup file is saved to a default location on the appliance. Only a single backup file at a time is stored on the appliance. You receive a **Backup done!** notification when the back up process is finished.

Note If the back up process fails, there is no impact to the appliance or its database. 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 appliance and attempt another backup.

Step 3 (Optional) Verify the backup status in the **History** area.

The following information is displayed:

- **Date**—Local date and time of the backup or restore.
- **Operation**—Type of operation, either backup or restore.
- **File Name**—Name of the file that was backed up or restored.
- **File Size**—Size of the file that was backed up or restored.
- **Update Status**—Success or failure status of the operation.

Note Place your cursor over the failure status to display additional details about the failure.

Step 4 (Optional) To download a copy of the backup file to your computer or another location on the network, click [Click here to download a copy of the backup](#).

What to Do Next

When necessary and at the appropriate time, you can restore the backup file to DNA Center.

Restore DNA Center

You can restore the DNA Center database and files from the last known backup file on the appliance or from an archived backup file that was saved and moved to another location on your network. When you restore the backup file, DNA Center overwrites the existing database and files with the files contained in the backup file. For more information about the backup and restore process, see [About Backup and Restore](#), on page 115.



Caution

The 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 network policies that have been created, any new or updated passwords, or any new or updated certificates and trustpool bundles.




Note You can only restore a backup to an appliance that is running the same DNA Center software version as the appliance from which the backup was taken.

Before You Begin

You must have successfully deployed DNA Center and it must be operational.

You must have successfully performed a backup of the DNA Center database and files following the steps in the previous procedure.

Procedure

Step 1 From the DNA Center home page, click  > **System Settings** > **Backup & Restore**.

Step 2 Click **Restore from last Backup**.

Note You can also drag the backup file from its location in your network and drop it onto the **Drag and Drop a backup file** field in the window.

Note The 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 file overwrites the current database. While a restore is in progress, you are not be able to open or access any windows in DNA Center.

If the restore process is successful, you are logged out of DNA Center. You will need to log back in.

If the restore process is unsuccessful, you receive an unsuccessful restore notification. Because the database might be in an inconsistent state, we recommend that you do not use the database and contact technical support for additional actions to take.

Step 3 (Optional) Check whether the restore process was successful. To review the backup and restore history in the **Backup & Restore** window, proceed to Step 4. To review the backup and restore history in Grapevine, follow these steps:

a) Using a Secure Shell (SSH) client, log into the appliance using the IP address that you specified during the initial configuration.

Note 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.

b) When prompted, enter grapevine as your Linux username and the password for SSH access.

c) Enter the **grape backup display** command at the prompt.

Check that the command output shows the restore process was completed and successful. Look for the property operation marked `restore` in the command output, with the latest start time followed by a `success` status.

d) Using the Secure Shell (SSH) client, log out of the appliance.

Step 4 Log back into DNA Center and review the backup and restore history on the **Backup & Restore** window. The following information is displayed:

- **Date**—Local date and time of the backup or restore.
- **Operation**—Type of operation, either backup or restore.
- **File Name**—Name of the file that was backed up or restored.

- **File Size**—Size of the file that was backed up or restored.
- **Update Status**—Success or failure status of the operation.

Note Place your cursor over the failure status to display additional details about the failure.
