



Cisco Digital Network Architecture Center User Guide, Release 1.2.1

First Published: 2018-06-10

Last Modified: 2018-08-02

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 NONINFRINGEMENT 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: <https://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. (1721R)

© 2017–2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Get Started with Cisco DNA Center 1

About Cisco DNA Center 1
Log In 1
Log In for the First Time as a Network Administrator 2
Default Home Page 3
Use Global Search 5
Where to Start 6

CHAPTER 2

Discover Your Network 7

About Discovery 7
Discovery Prerequisites 8
Discovery Credentials 8
Discovery Credentials and Cisco ISE 9
Discovery Credentials Guidelines and Limitations 9
Discovery Credentials Example 10
Preferred Management IP Address 10
Discovery Configuration Guidelines and Limitations 11
Perform Discovery 11
Discover Your Network Using CDP 11
Discover Your Network Using an IP Address Range 16
Discover Your Network Using LLDP 21
Manage Discovery Jobs 27
Stop and Start a Discovery Job 27
Edit a Discovery Job 27
Change Credentials in a Discovery Job 28
Clone a Discovery Job 30

Delete a Discovery Job	31
View Discovery Job Information	31

CHAPTER 3**Onboard Devices with Network Plug and Play 33**

About Network Plug and Play	33
Network Plug and Play Use Cases	35
Manage Plug and Play Devices	36
Devices Overview	36
View Devices	39
Add or Edit a Device	39
Add Devices in Bulk	40
Claim a Device	41
Delete or Reset a Device	43
Manage Plug and Play Workflows	43
Workflows Overview	43
View a Workflow	45
Create or Edit a Workflow	45
Clone a Workflow	48
Delete a Workflow	50
Manage Plug and Play Settings	50
Settings Overview	50
Accept the EULA	50
Manage Cisco Smart Accounts	51
Register or Edit a Virtual Account	51
View, Synchronize, and Deregister Smart Accounts	52

CHAPTER 4**Manage Your Inventory 55**

About Inventory	55
Inventory and Cisco ISE Authentication	56
Display Information About Your Inventory	56
Types of Devices in the DNA Center Inventory	60
Manage Network Devices	61
Add a Network Device	61
Update Network Device Credentials	64

Manage Compute Devices	68
Add a Compute Device	68
Update Compute Device Credentials	68
Manage Meraki Dashboards	69
Integrate Meraki Dashboard	69
Update Meraki Dashboard Credentials	69
Filter Devices	70
Change Devices Layout View	71
Change Device Role (Inventory)	71
Update a Device's Management IP Address	72
Update Device Resync Interval	73
Resync Device Information	73
Delete a Network Device	74
Launch Command Runner (Inventory)	74
Use a CSV File to Import and Export Device Configurations	75
Import Device Configurations From a CSV File	76
Export Device Configurations	76
Export Device Credentials	77

CHAPTER 5**Manage Software Images** 79

About Image Repository	79
Integrity Verification of Software Images	79
Viewing Software Images	80
Using Recommended Software Images	80
Import Software Images	81
About Golden Software Images	81
Creating Golden Software Images	82
Provision Software Images	82

CHAPTER 6**Display Your Network Topology** 85

About Topology	85
Display the Topology of Areas, Sites, Buildings, and Floors	86
Filter Devices on the Topology Map	86
Display Device Information	87

Display Link Information	87
Pin Devices to the Topology Map	88
Save a Topology Map Layout	88
Open a Topology Map Layout	88
Export the Topology Layout	89

CHAPTER 7

Design Network Hierarchy and Settings 91

Design a New Network Infrastructure	91
About Network Hierarchy	92
Guidelines for Preparing Image Files to Use Within Maps	92
Create Sites in the Network Hierarchy	92
Upload Existing Site Hierarchy	93
Search the Network Hierarchy	94
Edit Sites	94
Delete Sites	94
Add Buildings	95
Edit a Building	95
Delete Buildings	95
Add Floors to Buildings	96
Edit Floors	97
Monitor Floor Map	97
Edit Floor Elements and Overlays	100
Guidelines for Placing Access Points	100
Add, Position, and Delete APs	100
Quick View of APs	102
Add, Position, and Delete Sensors	103
Add Coverage Areas	104
Create Obstacles	105
Location Region Creation	106
Guidelines for Placing Inclusion and Exclusion Areas on a Floor Map	106
Define Inclusion Region on a Floor	106
Define Exclusion Region on a Floor	107
Edit Location Regions	107
Delete Location Regions	108

Rail Creation	108
Place Markers	109
Floor View Options	109
View Options for Access Points	109
View Options for Sensors	111
View Options for Overlay Objects	111
Configure Map Properties	111
Configure Global Maps Properties	111
Data Filtering	112
Filtering Access Points Data	112
Filtering Sensors Data	112
Configure Global Wireless Settings	113
Creating SSIDs for an Enterprise Wireless Network	113
Preshared Key Override	115
Creating SSIDs for a Guest Wireless Network	115
Create a Guest Portal Page	118
Create a Wireless Interface	119
Create a Wireless Radio Frequency Profile	120
Create a Wireless Sensor Device Profile	122
Create Network Profiles	123
Create Network Profiles for Routing and NFV	123
About Global Network Settings	125
About Device Credentials	125
CLI Credentials	126
SNMPv2c Credentials	126
SNMPv3 Credentials	126
HTTPS Credentials	127
Configure Global Device Credentials	128
Configure CLI Credentials	128
Configure SNMPv2c Credentials	129
Configure SNMPv3 Credentials	130
Configure HTTPS Credentials	132
Configure IP Address Pools	133
Import IP Address Pools	133

	Configure Service Provider Profiles 134
	Configure Global Network Servers 134
	Add AAA Server 135
	Configure Cisco WLC High Availability from Cisco DNA Center 136
	Prerequisites for Cisco WLC HA 136
	Configuring Cisco WLC HA from Cisco DNA Center 136
	What Happens During or After the High Availability Process is Complete 137
	Commands to Configure and Verify Cisco WLC HA 138
CHAPTER 8	Create Templates to Automate Device Configuration Changes 139
	About Template Editor 139
	Create Projects 139
	Create Templates 140
	Create a Regular Template 140
	Blacklisted Commands 142
	Sample Templates 142
	Create a Composite Template 142
	Edit Templates 144
	Template Simulation 145
	Template Form Editor 146
	Variable Binding 146
	Special Keywords 147
	Create and Associate Templates to Wireless Profiles 148
CHAPTER 9	Run Diagnostic Commands on Devices 151
	About Command Runner 151
	Running Diagnostic Commands on Devices 151
CHAPTER 10	Configure Telemetry Profile 153
	Configure a Telemetry Profile 153
	Apply a Telemetry Profile to the Devices 154
CHAPTER 11	Configure Policies 157
	Policy Overview 157

Policy Dashboard	157
Group-Based Access Control Policies	158
Workflow to Configure a Group-Based Access Control Policy	159
Create a Group-Based Scalable Group	159
Create a Group-Based Access Control Contract	160
Edit or Delete a Group-Based Access Control Contract	161
Create a Group-Based Access Control Policy	161
Edit or Delete a Group-Based Access Control Policy	162
Deploy a Group-Based Access Control Policy	163
IP-Based Access Control Policies	163
Workflow to Configure an IP-Based Access Control Policy	164
Create an IP Network Group	165
Edit or Delete an IP Network Group	165
Create an IP-Based Access Control Contract	165
Edit or Delete an IP-Based Access Control Contract	166
Create an IP-Based Access Control Policy	166
Edit or Delete an IP-Based Access Control Policy	168
Deploy an IP-Based Access Control Policy	168
Application Policies	169
CVD-Based Settings in Application Policies	169
Site Scope	170
Applications and Application Sets	170
Business-Relevance Groups	170
Unidirectional and Bidirectional Application Traffic	171
Consumers and Producers	172
Marking, Queuing, and Dropping Treatments	172
Custom Applications	174
Favorite Applications	175
Service Provider Profiles	175
Queuing Profiles	177
Processing Order for Devices with Limited Resources	178
Policy Drafts	180
Policy Preview	181
Policy Precheck	181

Policy Scheduling	182
Policy Versioning	182
Original Policy Restore	182
Stale Application Policies	183
Application Policy Guidelines and Limitations	183
Configure Applications and Application Sets	184
Change an Application's Settings	184
Create a Server Name-Based Custom Application	184
Create an IP Address and Port-Based Custom Application	185
Create a URL-Based Custom Application	186
Edit or Delete a Custom Application	187
Change the Applications in an Application Set	188
Create a Custom Application Set	188
Edit or Delete a Custom Application Set	189
Mark an Application as Favorite	189
Manage Application Policies	189
Prerequisites	189
Create an Application Policy	190
View Application Policy Information	193
Edit an Application Policy	194
Save a Draft of an Application Policy	194
Deploy an Application Policy	195
Cancel a Policy Deployment	195
Delete an Application Policy	195
Clone an Application Policy	196
Restore an Application Policy	196
Reset the Default CVD Application Policy	197
Preview an Application Policy	197
Precheck an Application Policy	198
Display Application Policy History	198
Roll Back to a Previous Policy Version	199
Manage Queuing Profiles	199
Create a Queuing Profile	199
Edit or Delete a Queuing Profile	200

Manage Application Policies for WAN Interfaces	200
Customize Service Provider Profile SLA Attributes	200
Assign a Service Provider Profile to a WAN Interface	202
Traffic Copy Policies	203
Sources, Destinations, and Traffic Copy Destinations	203
Guidelines and Limitations of Traffic Copy Policy	204
Workflow to Configure a Traffic Copy Policy	204
Create a Traffic Copy Destination	205
Edit or Delete a Traffic Copy Destination	205
Create a Traffic Copy Contract	205
Edit or Delete a Traffic Copy Contract	206
Create a Traffic Copy Policy	206
Edit or Delete a Traffic Copy Policy	206
Virtual Networks	207
Guidelines and Limitations for Virtual Networks	207
Create a Virtual Network	207
Edit or Delete a Virtual Network	208

CHAPTER 12

Provision Your Network	211
Provisioning	211
Add Devices to Sites	211
Provisioning Devices	212
Provision a Cisco WLC	212
Onboard APs with Zero Touch Provisioning - Day 0 Provisioning	213
Provision a Cisco AP—Day 1 AP Provisioning	215
Provision a Brownfield Device	215
Guest Anchor Configuration and Provisioning	217
Provision a Sensor Device	218
Provision LAN Underlay	218
Check the LAN Automation Status	220
Delete Devices After Provisioning	221
Multi-Site Fabric Domain	221
Transit Networks	221
Create a IP Transit Network	222

Create a SDA Transit Network	222
Configuring Fabric Domains	223
Fabrics Overview	223
Create a Fabric Domain	223
Configure a Fabric Domain	223
Add Devices to a Fabric	224
Configure Host Onboarding	226
Select Authentication Template	226
Associate Virtual Networks to the Fabric Domain	226
Configure Wireless SSIDs for the Fabric Domain	227
Configure Ports Within the Fabric Domain	227
Multicast Overview	228
Configure Multicast Settings	228

CHAPTER 13

DNA Center Assurance Overview	233
About DNA Center Assurance	233
About DNA Center Assurance and Analytics	233

CHAPTER 14

Configure DNA Center Assurance	235
Basic Workflow for Configuring DNA Center Assurance	235
DNA Center Assurance and Cisco ISE Integration	236
Generate Keystore File	236
Generate Truststore File	238
Configure DNA Center Assurance for Cisco ISE Integration	240
Assurance Application	240

CHAPTER 15

Assure the Health of Your Enterprise	243
About Enterprise	243
Monitor and Troubleshoot the Overall Health of Your Enterprise	243
Monitor and Troubleshoot the Health of Your Network	246
Global Network Health Summary Score or Site Health Summary Score	251
Device Category Health Score	251
Individual Device Health Score	251
Monitor and Troubleshoot the Health of a Device	252

Enable SNMP Collector Metrics for Fabric Devices	254
Switch Health Score	257
Router Health Score	257
AP Health Score	258
Cisco WLC Health Score	259

CHAPTER 16 Assure Client Health 261

About Clients	261
Monitor and Troubleshoot the Health of All Client Devices	261
Client Health Summary Score	268
Client Category Health Score	268
Client Onboarding Score	268
Client Connectivity Score	269
Monitor and Troubleshoot the Health of a Client Device	270
Individual Client Health Score	273
Trace the Path of a Device	273
About Path Trace	273
Perform a Path Trace	274

CHAPTER 17 Monitor Application Health 277

About Application Experience	277
Enable Cisco NetFlow Collection	277
View the Application Experience of a Client Device	278
Monitor the Health of All Applications	279
Application Health Score	280
Monitor the Health of an Application	281

CHAPTER 18 Manage Sensors and Sensor-Driven Tests 283

About Sensors and Sensor-Driven Tests	283
View Sensor-Driven Tests	284
Add a Sensor-Driven Test	285
Monitor and Troubleshoot the Health of Wireless Sensors	287
Provision the Wireless Cisco Aironet 1800s Active Sensor	289
Enable Cisco Provisioning SSID on the Cisco WLC	290

Edit, Delete, or Run a Sensor-Driven Test **290**

CHAPTER 19 **Manage Dashboards** **293**

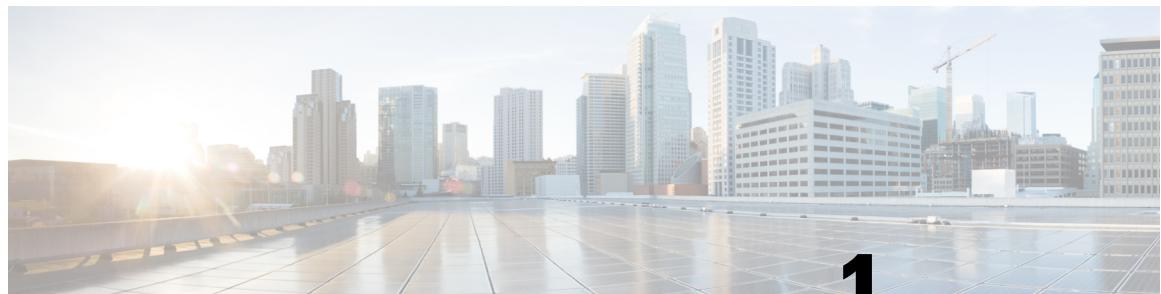
About Dashboards **293**
Create a Custom Dashboard **293**
Create a Dashboard From a Template **294**
View a Dashboard **295**
Edit or Delete a Dashboard **296**
Duplicate a Dashboard **296**
Mark a Dashboard as a Favorite **297**
Change the Position of a Dashlet **297**

CHAPTER 20 **Issues Detected by DNA Center Assurance** **299**

About Issues **299**
View Global Issues **300**
View Issue Catalog **300**
Client Issues **301**
Switch and Fabric Issues **310**
Router Issues **314**
AP and WLC Issues **314**
Sensor Issues **315**

CHAPTER 21 **Troubleshoot DNA Center Using Data Platform** **321**

About Data Platform **321**
Troubleshoot DNA Center Using the Analytics Ops Center **322**
View Collector Status **323**
Configure Data Retention Settings **324**
View Pipeline Status **324**



CHAPTER 1

Get Started with Cisco DNA Center

- [About Cisco DNA Center, on page 1](#)
- [Log In, on page 1](#)
- [Log In for the First Time as a Network Administrator, on page 2](#)
- [Default Home Page, on page 3](#)
- [Use Global Search, on page 5](#)
- [Where to Start, on page 6](#)

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 network environment. The DNA Center GUI provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience. DNA Center allows you to:

- Move faster—Provision thousands of devices across your enterprise network. 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 DNA Center by entering its network IP address in your browser. This IP address connects to the external network and is configured during the DNA Center installation. For more information about installing and configuring DNA Center, see the [Cisco Digital Network Architecture Center Installation Guide](#).

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

Procedure

- Step 1** Enter an address in your web browser's address field in the following format. Here *server-ip* is the IP address (or the hostname) of the server on which you have installed DNA Center:

`https://server-ip`

Example: `https://192.0.2.1`

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

- Step 2** Enter the DNA Center username and password assigned to you by the system administrator. DNA Center displays its Home page.

If your user ID has the NETWORK-ADMIN-ROLE and no other user with the same role has logged in before, you will see a first-time setup wizard instead of the Home page. For details, see [Log In for the First Time as a Network Administrator, on page 2](#).

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

Log In for the First Time as a Network Administrator

If your user ID has the NETWORK-ADMIN-ROLE assigned, and no other user with the same role has logged in before, you will see a "Getting Started" wizard instead of the Home dashboard the first time you log in to DNA Center.

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

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

Before you begin

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

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

- SNMP v2c credentials, including the read community string

Procedure

- Step 1** If you have not already done so, Log in to DNA Center normally, as explained in [Log In, on page 1](#).
- Step 2** With the wizard displayed, click **Get Started**.
- Step 3** In the fields on the following screens, enter the information listed in "Before You Begin", above. Click **Save & Next** to continue, **Back** to return to the previous screen and revise your entries, or **Skip** to cancel the wizard and display the DNA Center Home page.
- Step 4** When you are finished, click **Begin Discovery**. DNA Center displays the Assurance dashboard, which will slowly fill with network health information as discovery completes.
-

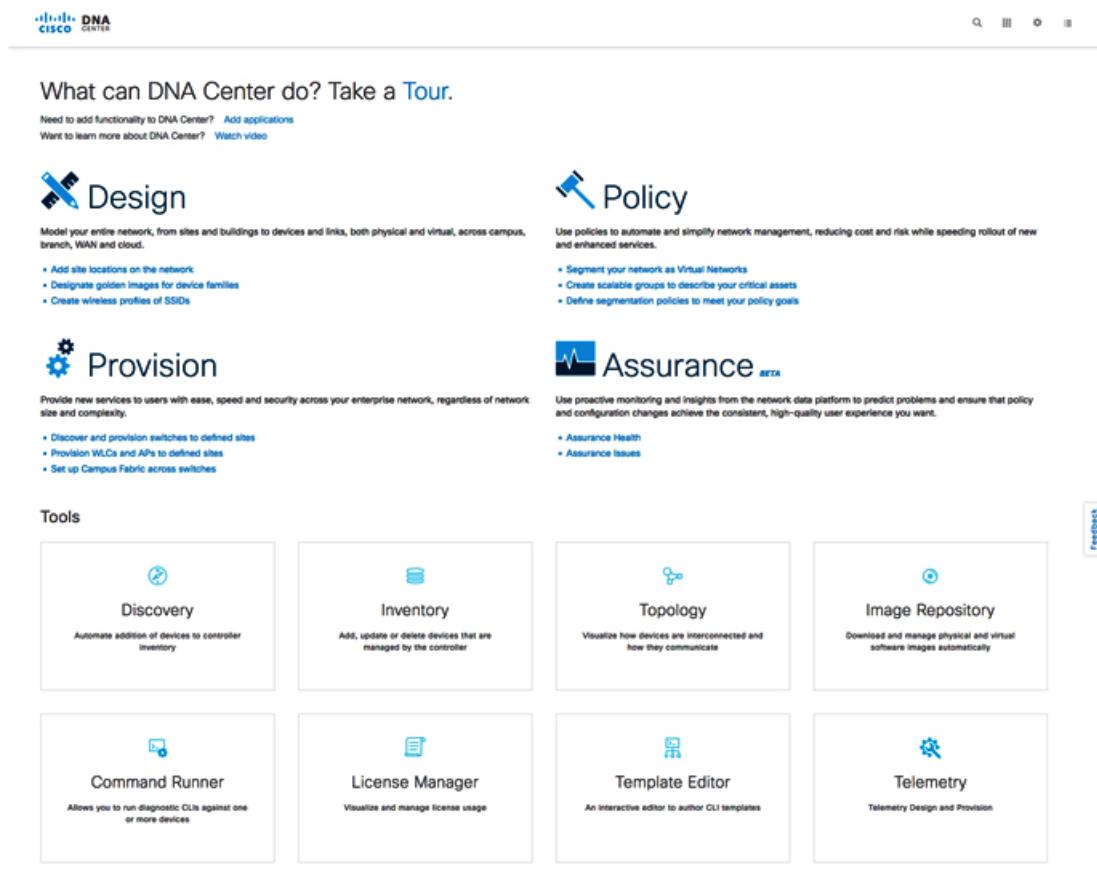
Default Home Page

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**:

The **Applications** area include:

- **Design**—Create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network.
- **Policy**—Create policies that reflect your organization's business intent for a particular aspect of the network, such as network access. DNA Center takes the information collected in a policy and translates it into network-specific and device-specific configurations required by the different types, makes, models, operating systems, roles, and resource constraints of your network devices.
- **Provision**—Prepare and configure devices, including adding devices to sites, assigning devices to the DNA Center inventory, deploying the required settings and policies, creating fabric domains, and adding devices to the fabric.
- **Assurance**—Provides proactive and predictive actionable insights about the performance and health of the network infrastructure, applications, and end-user clients.

Tools—Use the **Tools** area to help you configure and manage your network.

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

423568

Click any of the icons in the two main areas to launch the corresponding application or tool.

In addition to the **Application** and **Tool** icons, you can click any of the icons at the top-right corner of the home page to perform important common tasks:

- Search icon—Lets you search for devices, users, hosts, and other items, anywhere they are stored in the DNA Center database. For tips on using Search, see [Use Global Search, on page 5](#).
- Applications icon—Lets you return to the DNA Center home page from any other page and access the applications and tools. You can do the same thing by clicking on the Cisco DNA Center logo in the upper-left corner of the home page.
- Settings icon—Lets you view audit logs, configure DNA Center system settings, see the DNA Center version you are using, and log out.
- Notifications icon—Lets you see recently scheduled tasks and other notifications.

Finally, you can click the following icons, which appear at the right side of every page in DNA Center:

- Feedback icon—Lets you submit your comments and suggestions to Cisco's DNA Center product team.

-  Help icon—Launches DNA Center's context-sensitive online help in a separate tab in your browser.

If you are new to DNA Center, see [Where to Start, on page 6](#) for tips and suggestions on how to begin using it.

Use Global Search

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

- **Activities:** Search for DNA Center menu items, workflows and features by name.
- **Applications:** Search for them by name.
- **Application Groups:** Search for them by name.
- **Hosts and Endpoints:** Search for them by name, IP address, or MAC address.
- **IP Pools:** Search for them by name or IP address.
- **Network Devices:** Search for them by name, IP address, serial number, software version, platform, product family, or MAC address.
- **Sites:** Search for them by name.
- **Users:** Search for them by user name. Please note that case-insensitivity and substring search are not supported for user names in this release.
- Other items, as new versions of DNA Center are released.

To start a global Search, click the  icon in the upper-right corner of any DNA Center page.

Figure 2: Global Search Icon



When you click the  icon, DNA Center displays a popup global search window, with a search field where you can begin entering identifying information about the item you are looking for.

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

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

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

As you add more characters to the search string, global search will automatically narrow the displayed list of categories and items.

The summary panel includes links to more information. The link will vary as appropriate for each category and item. For example: With Activities, the summary panel shows you links to menu items and workflows elsewhere in the DNA Center system. For Applications, there is the **Application 360** view. You will see links to **Client 360** and **Topology** views for Hosts/Endpoints, and links to **Device 360** and **Topology** views for Network Devices. Click on the link to see the appropriate menu item, workflow, or detail view.

When you are finished, click  to close the global search window.

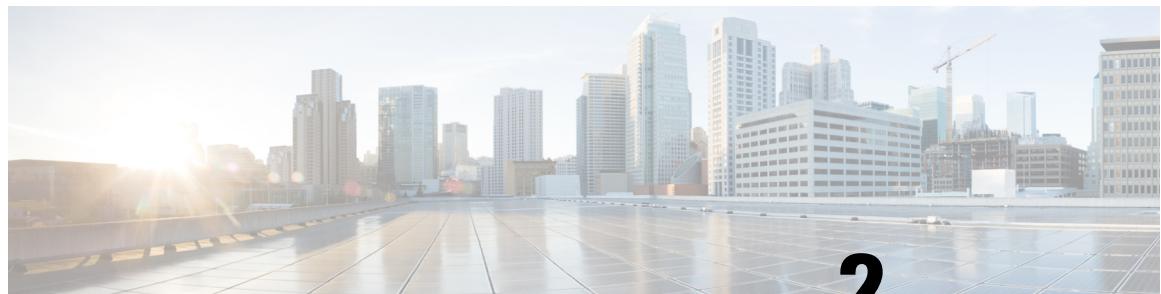
Global search can display a maximum of 500 results at one time.

Where to Start

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

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 (brownfield deployment), start by running Discovery. After running Discovery, all your devices are displayed on the **Inventory** window. For information about running Discovery, see [Discover Your Network, on page 7](#).
- New or nonexisting infrastructure—if you have no existing infrastructure and are starting from scratch, (green field deployment), create a network hierarchy.



CHAPTER 2

Discover Your Network

- [About Discovery, on page 7](#)
- [Discovery Prerequisites, on page 8](#)
- [Discovery Credentials, on page 8](#)
- [Preferred Management IP Address, on page 10](#)
- [Discovery Configuration Guidelines and Limitations, on page 11](#)
- [Perform Discovery, on page 11](#)
- [Manage Discovery Jobs, on page 27](#)

About Discovery

The Discovery feature scans the devices in your network and sends the list of discovered devices to Inventory.

The Discovery feature can also work with the Device Controllability feature to configure required network settings on devices, if these settings are not already present on the device. For more information about Device Controllability, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

There are three ways for you to discover devices:

- Use Cisco Discovery Protocol (CDP) and provide a seed IP address.
- Specify a range of IP addresses. (A maximum range of 4096 devices is supported.)
- Use Link Layer Discovery Protocol (LLDP) and provide a seed IP address.

When configuring the Discovery criteria, remember that there are settings that you can use to help reduce the amount of time it takes to discover your network:

- **CDP Level and LLDP Level**—If you use CDP or LLDP as the discovery method, you can set the CDP or LLDP level to indicate the number of hops from the seed device that you want to scan. The default, level 16, might take a long time on a large network. So, if fewer devices have to be discovered, you can set the level to a lower value.
- **Subnet Filters**—If you use an IP address range, you can specify devices in specific IP subnets for Discovery to ignore.
- **Preferred Management IP**—Whether you use CDP, LLDP, or an IP address range, you can specify whether you want DNA Center to add any of the device's IP addresses or only the device's loopback address.

Regardless of the method you use, you must be able to reach the device from DNA Center and configure specific credentials and protocols in DNA Center to discover your devices. These credentials can be configured and saved in the **Design > Network Settings > Device Credentials** window or on a per-job basis in the **Discovery** window.



Note If a device uses a first hop resolution protocol like Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), the device might be discovered and added to the inventory with its floating IP address. Later, if HSRP or VRRP fails, the IP address might be reassigned to a different device. This situation can cause issues with the data that DNA Center retrieves for analysis.

Discovery Prerequisites

Before you run Discovery, complete the following minimum prerequisites:

- Understand what devices will be discovered by DNA Center by viewing the [DNA Center Supported Devices List](#).
- Ensure at least one SNMP credential is configured on your devices for use by DNA Center. At a minimum, this can be an SNMP v2C read credential. For more information, see [Discovery Credentials, on page 8](#).
- Configure SSH credentials on the devices you want DNA Center to discover and manage. DNA Center discovers and adds a device to its inventory if at least one of the following two criteria are met:
 - The account being used by DNA Center to SSH into your devices has privileged EXEC mode (level 15).
 - You configure the device's enable password as part of the CLI credentials configured in the Discovery job. For more information, see [Discovery Configuration Guidelines and Limitations, on page 11](#).

Discovery Credentials

Discovery credentials are the CLI, SNMPv2c, SNMPv3, HTTP(S), and NETCONF 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(S) credentials.
- Both standard and NFVIS devices—CLI, SNMP, and HTTP(S) credentials

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 that are configured for the discovery job until it finds a set that works for the device.

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

Discovery Credentials and Cisco ISE

If you are using Cisco ISE as an authentication server, discovery authenticates devices using Cisco ISE as part of the discovery process. To make sure that your devices are discovered properly, follow these guidelines:

- Do not use discovery 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 will go 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 will go into a partial collection state.

Discovery Credentials Guidelines and Limitations

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

- To change the device credentials used in a discovery job, you need to edit the discovery job and deselect the credentials that you no longer want to use. Then, you need to add the new credentials and start the discovery. For more information, see [Change Credentials in a Discovery Job, on page 28](#).
- 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.

Discovery Credentials Example

- 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.

Discovery Credentials Example

The devices that compose a typical network can have widely varying discovery requirements. DNA Center lets you create multiple discovery jobs to support these varying requirements. For example, assume that a network of 200 devices form a Cisco Discovery Protocol (CDP) neighborhood. 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, perform the following tasks:

Procedure

- 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 **Inventory** window.
-

Preferred Management IP Address

When DNA Center discovers a device, it logs one of the device's IP addresses as the preferred management IP address for the device. You can configure DNA Center to log the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from DNA Center.

If you choose to use a device's loopback IP address as the preferred management IP address, DNA Center determines the preferred management IP address as follows:

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

After a device is discovered, you can update the management IP address from the **Inventory** window. For more information, see [Update Device Resync Interval, on page 73](#).

Discovery Configuration Guidelines and Limitations

The following are the guidelines and limitations for DNA Center to discover your Cisco Catalyst 3000 Series Switches and Catalyst 6000 Series Switches:

- 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 interfaces for both incoming and outgoing connections. Use the **transport input** and **transport output** commands for this configuration. For information about these commands, see the command reference document for the specific device type.
- Do not change the default login method for a device's console port and the VTY lines. DNA Center cannot discover devices that enforce the AAA login method.
- Cisco WLCs must be discovered using the Management IP address instead of the Service Port IP address. If not, the related WLC 360 and AP 360 pages will not display any data.

Perform Discovery

Discover Your Network Using CDP

You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, or LLDP. This procedure shows you how to discover devices and hosts using CDP. For more information about the other discovery methods, see [Discover Your Network Using an IP Address Range, on page 16](#) and [Discover Your Network Using LLDP, on page 21](#).

**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.
- CLI credentials are not required to discover hosts; hosts are discovered through the network devices that they are connected to.

Before you begin

- Enable CDP on your network devices.
- Configure your network devices, as described in [Discovery Prerequisites, on page 8](#).
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

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 Address/Ranges** area if it is not already visible, and configure the following fields:

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

You can enter addresses either 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.

- Click .

Repeat Steps c and d 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**.

Choose **None** to allow the device use any of its IP addresses or choose **Use Loopback IP** to specify the device's loopback interface 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 10](#).

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 your own credentials, you can save them for only the current job by clicking **Save** or you can save them for the current and future jobs by clicking the **Save as global settings** check box and then clicking **Save**.

- Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.
- To add additional credentials, click **Add Credentials**.
- To configure CLI credentials, configure the following fields:

Table 1: 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.

Field	Description
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>
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>

- d) Click **SNMP v2c** and configure the following fields:

Table 2: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMPv2c 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 SNMPv2c 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>

- e) (Optional) Click **SNMP v3** and configure the following fields:

Table 3: SNMPv3 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. Choose one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv—Does not provide authentication or encryption. • AuthNoPriv—Provides authentication but does not provide encryption. • AuthPriv—Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA—Authentication based on HMAC-SHA. • MD5—Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length. <p>Note</p> <ul style="list-style-type: none"> • Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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	Privacy type. (Enabled if you select AuthPriv as a the authentication mode.) Select one of the following privacy types: <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.

Field	Description
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"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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.

- f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 4: SNMP Properties

Field	Description
Retries	Number of times DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

- g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 5: HTTP(S) 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</p> <p>The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain <>@';:;! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Discover Your Network Using an IP Address Range

Field	Description
Write	<p>You can configure up to five HTTPS 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 The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain <>@', :; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

- h) (Optional) If you have network devices with NETCONF enabled, click **NETCONF** and enter a port number in the **Port** field.

Note For an Evolved Converged Access (eCA) switch, enter the port number 830.

Note If NETCONF is not already enabled on the devices, you can set up Device Controllability to configure NETCONF for you. For more information about Device Controllability, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

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

- 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**.
- 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.

Discover Your Network Using an IP Address Range

You can discover devices using an IP address range, CDP, or LLDP. This procedure shows you how to discover devices and hosts using an IP address range. For more information about the other discovery methods, see [Discover Your Network Using CDP, on page 11](#) and [Discover Your Network Using LLDP, on page 21](#).

Before you begin

Your devices must have the required device configurations, as described in [Discovery Prerequisites](#), on page 8.

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 Address/Ranges** area, if it is not already visible, and configure the following fields:

a) For **Discovery Type**, click **Range**.

b) 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.

Note Cisco WLCs must be discovered using the Management IP address instead of the Service Port IP address. If not, the related WLC 360 and AP 360 pages will not display any data.

c) (Optional) Repeat Step b to enter additional IP address ranges.

d) From the **Preferred Management IP** drop-down list, choose either **None** or **Use Loopback**.

Select **None** to allow the device use any of its IP addresses or **Use Loopback IP** to specify the device's loopback interface 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 10.

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 your own credentials, you can save them for only the current job by clicking **Save** or you can save them for the current and future jobs by clicking the **Save as global settings** check box and then clicking **Save**.

- a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.
- b) To add additional credentials, click **Add Credentials**.
- c) To configure CLI credentials, configure the following fields:

Table 6: 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.

Field	Description
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>
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>

- d) Click **SNMP v2c** and configure the following fields:

Table 7: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMPv2c 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 SNMPv2c 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>

- e) (Optional) Click **SNMP v3** and configure the following fields:

Table 8: SNMPv3 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. Choose one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv—Does not provide authentication or encryption. • AuthNoPriv—Provides authentication but does not provide encryption. • AuthPriv—Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA—Authentication based on HMAC-SHA. • MD5—Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length. <p>Note</p> <ul style="list-style-type: none"> • Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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	Privacy type. (Enabled if you select AuthPriv as a the authentication mode.) Select one of the following privacy types: <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.

Field	Description
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"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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.

- f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 9: SNMP Properties

Field	Description
Retries	Number of times DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

- g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 10: HTTP(S) 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</p> <p>The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain <>@', :; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Field	Description
Write	<p>You can configure up to five HTTPS 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 The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain <>@', :; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

- h) (Optional) If you have network devices with NETCONF enabled, click **NETCONF** and enter a port number in the **Port** field.

Note If NETCONF is not already enabled on the devices, you can set up Device Controllability to configure NETCONF for you. For more information about Device Controllability, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

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**.
- 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 LLDP

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, or an IP address range. This procedure shows you how to discover devices and hosts using LLDP. For more information about the other discovery methods, see [Discover Your Network Using CDP](#), on page 11 and [Discover Your Network Using an IP Address Range](#), on page 16.

**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.
- CLI credentials are not required to discover hosts; hosts are discovered through the network devices that they are connected to.

Before you begin

- Enable LLDP on your network devices.
- Configure your network devices, as described in [Discovery Prerequisites, on page 8](#).
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

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 Address/Range** area if it is not already visible, and configure the following fields:

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

You can enter addresses either 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.

- d) Click

Repeat Steps c and d to exclude multiple subnets from the Discovery job.

- e) (Optional) In the **LLDP 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, LLDP level 3 means that LLDP will scan up to three hops from the seed device.

- f) In the **Preferred Management IP** field, click the drop-down list to select either **None** or **Use Loopback**.

Choose **None** to allow the device use any of its IP addresses or choose **Use Loopback IP** to specify the device's loopback interface 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 10](#).

Note To use the loopback interface IP address as the preferred management IP address, make sure that the LLDP 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 checking the **Save as global settings** check box.

- Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.
- To add additional credentials, click **Add Credentials**.
- For CLI credentials, configure the following fields:

Table 11: 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>
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>

- Click **SNMP v2c** and configure the following fields:

Table 12: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> Name/Description—Name or description of the SNMPv2c 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 SNMPv2c 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>

- e) (Optional) Click **SNMP v3** and configure the following fields:

Table 13: SNMPv3 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. Choose one of the following modes: <ul style="list-style-type: none"> noAuthNoPriv—Does not provide authentication or encryption. AuthNoPriv—Provides authentication but does not provide encryption. AuthPriv—Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> SHA—Authentication based on HMAC-SHA. MD5—Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length. <p>Note</p> <ul style="list-style-type: none"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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.

Field	Description
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"> • Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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.

- f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 14: SNMP Properties

Field	Description
Retries	Number of times DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

- g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 15: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .

Field	Description
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 The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain <>@', :; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<p>You can configure up to five HTTPS 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 The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain <>@', :; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

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.

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:
- From the **Discoveries** pane, select the corresponding discovery job.
 - Click **Stop**.
- Step 3** To restart an inactive discovery job, perform these steps:
- From the **Discoveries** pane, select the corresponding discovery job.
 - Click **Start**.
-

Edit a Discovery Job

You can edit a discovery job and then rerun the job.

Before you begin

You must have created 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 **Edit**.
- Step 4** Depending on the discovery type, you can change the type of discovery job, except for the following fields:
- **CDP**—Discovery name, discovery type, IP address. For more information about the fields you can change, see [Discover Your Network Using CDP, on page 11](#).
 - **IP Range**—Discovery name, discovery type, IP address range (although you can add additional IP address ranges). For more information about the fields you can change, see [Discover Your Network Using an IP Address Range, on page 16](#).
 - **LLDP**—Discovery name, discovery type, IP address. For more information about the fields you can change, see [Discover Your Network Using LLDP, on page 21](#).
- Step 5** Click **Start**.
-

Change Credentials in a Discovery Job

You can change the credentials used in a discovery job and then rerun the job.

Before you begin

You must have created 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 **Edit**.
- Step 4** Expand the **Credentials** area.
- Step 5** Deselect the credentials that you do not want to use.
- Step 6** Configure the credentials that you want to use:
 - a) Click **Add Credentials**.
 - b) To configure CLI credentials, configure the following fields:

Table 16: 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	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. Configure this password only if your network devices require it. For security reasons, enter the enable password again. Note Passwords are encrypted for security reasons and are not displayed in the configuration.

- c) Click **SNMP v2c** and configure the following fields:

Table 17: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMPv2c 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 SNMPv2c 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>

d) (Optional) Click **SNMP v3** and configure the following fields:

Table 18: SNMPv3 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. Choose one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv—Does not provide authentication or encryption. • AuthNoPriv—Provides authentication but does not provide encryption. • AuthPriv—Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA—Authentication based on HMAC-SHA. • MD5—Authentication based on HMAC-MD5.

Clone a Discovery Job

Field	Description
Auth Password	<p>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</p> <p>Note</p> <ul style="list-style-type: none"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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.

Step 7 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.
-

View Discovery Job Information

You can view information about a discovery job, such as the discovery settings and credentials that were used. You can also view the historical information about each discovery that was run, including information about the specific devices that were discovered or that failed to be discovered.

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. Use the **Search** function to find a discovery by device IP address or discovery name.
- Step 3** Click the down-arrow next to one of the following areas for more information:

View Discovery Job Information

- **Discovery Details**—Displays the parameters that were used to run the discovery job. Parameters include attributes such as the CDP or LLDP level, IP address range, and protocol order.
 - **Credentials**—Provides the names of the credentials that were used.
 - **History**—Lists each discovery job that was run, including the status (completed or in progress), the time it was run, its duration, and whether any devices were discovered. You can click **View** to display discovery information per device, such as the status of the device and which device credentials were successful.
User the **Filter** function to display devices by any combination of IP addresses or ICMP, CLI, HTTPS, or NETCOMF values.
-



CHAPTER 3

Onboard Devices with Network Plug and Play

- [About Network Plug and Play, on page 33](#)
- [Network Plug and Play Use Cases, on page 35](#)
- [Manage Plug and Play Devices, on page 36](#)
- [Manage Plug and Play Workflows, on page 43](#)
- [Manage Plug and Play Settings, on page 50](#)

About Network Plug and Play

The Network Plug and Play application provides a way to automatically and remotely provision and onboard new network devices with minimal network administrator and field personnel involvement.

The Network Plug and Play application must be downloaded and installed in DNA Center because it is not installed by default. For more information about installing a package, see the chapter "[Manage Applications](#)" in the *Cisco Digital Network Architecture Center Administrator Guide*. Look for the package named Device Onboarding UI.

Using Network Plug and Play, you can do the following:

- Display the detailed onboarding status of network devices.
- Define provisioning workflows that include a series of actions such as installing a software image, applying a device configuration, and so on.
- Plan devices in advance of their installation by entering device information and associating the device with a workflow. When the device comes online, it contacts DNA Center and the workflow provisions and onboards the device automatically.
- Provision unclaimed network devices, which are new devices that appear on the network without prior planning.
- Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal in a Cisco Smart Account to the Network Plug and Play application, so that all devices appear in DNA Center.

For more information on typical use cases and workflows, see [Network Plug and Play Use Cases, on page 35](#).

To access the Network Plug and Play application after it is installed, from the DNA Center home page, click the **Network Plug and Play** tool. [Table 19: Network Plug and Play Dashboard Elements, on page 34](#) describes the elements in the Network Plug and Play dashboard.

Table 19: Network Plug and Play Dashboard Elements

Element	Description
Add images, or Manage x images	Shows the number of software images that are available in the DNA Center image repository, or shows Add, if there are none. Click the link to go to the image repository. For more information, see Manage Software Images, on page 79 .
Add templates, or Manage x templates	Shows the number of configuration templates that are available in the DNA Center template editor, or shows Add, if there are none. Click the link to go to the template editor. For more information, see Create Templates to Automate Device Configuration Changes, on page 139 .
Add workflows, or Manage x workflows	Shows the number of Network Plug and Play workflows that are defined, or shows Add, if there are none. Click the link to go to the Workflows tab. For more information, see Workflows Overview, on page 43 .
Manage Smart Account Sync	Click Manage to go to Settings > Smart Accounts to manage Smart Account synchronization. For more information, see Manage Cisco Smart Accounts, on page 51 .
Add devices	Click Add to go to the Add Devices dialog where you can add devices. For more information, see Add or Edit a Device, on page 39 or Add Devices in Bulk, on page 40 .
x devices are in error state	Click the number to go to the Devices tab set to filter on devices in the Error state.
x devices called in	Click the number to go to the Devices tab set to filter on devices in the Unclaimed state and that have been contacted.
x planned devices not called in	Click the number to go to the Devices tab set to filter on devices in the Planned state and that have not been contacted.
x devices have been provisioned	Click the number to go to the Devices tab set to filter on devices in the Provisioned state.

Element	Description
Devices States chart	<p>Pie chart showing the number of devices in each of the following states:</p> <ul style="list-style-type: none"> • Error—Device had an error and could not be provisioned. • Unclaimed—Device has not been assigned a workflow. • Planned—Device is added to Network Plug and Play and has been assigned a workflow but has not yet contacted the server. • Provisioned—Device is successfully onboarded and added to inventory.
Device Sources chart	<p>Pie chart showing the number of devices from each of the following sources:</p> <ul style="list-style-type: none"> • User—Devices added by the user. • Network—Devices that appeared on the network and were not added by a user. • SmartAccount—Devices added through synchronization with a Cisco Smart Account. • Migrated—Devices that were migrated from DNA Center 1.1.

Network Plug and Play Use Cases

This section describes typical use cases and workflows for Network Plug and Play.

Planned Provisioning

An administrator can plan the provisioning of a new site or other group of network devices as follows:

1. Upload software images to be deployed to devices, see [Import Software Images](#), on page 81.
2. Define configuration templates or files to be applied to devices, see [Create Templates to Automate Device Configuration Changes](#), on page 139.
3. Create a workflow for different types of devices to be deployed, see [Create or Edit a Workflow](#), on page 45.
4. Add details about planned devices one at a time or in bulk with a CSV file, see [Add or Edit a Device](#), on page 39 or [Add Devices in Bulk](#), on page 40.
5. Devices boot up and are automatically provisioned according to their workflows.

Unclaimed Provisioning

If a new network device is added to the network before it can be planned, it is labeled as an unclaimed device. An administrator can claim it by assigning it a workflow, or directly provisioning it with a software image and a configuration template, as follows:

1. Find the device on the unclaimed devices list, see [View Devices, on page 39](#).
2. Claim the device by assigning a workflow or by directly assigning a software image and configuration template. For more information, see [Claim a Device, on page 41](#).


Note

Only the password is updated by DNA Center in provisioning flow on a firewall and the user name is kept as the default setting in NFV.

The password is updated based on the settings in the Credential Profile assigned to the site in Network Setting, and is configured on the firewall through NFV provisioning flow.

Cisco Smart Account Synchronization and Provisioning

Network devices can be automatically registered through a Cisco Smart Account with the Cisco Plug and Play Connect cloud service. An administrator can synchronize the device inventory from Cisco Plug and Play Connect to Network Plug and Play, so that all devices appear in DNA Center. Then these devices can be claimed and provisioned.

1. Register a Smart Account and virtual account to synchronize with, see [Register or Edit a Virtual Account, on page 51](#).
2. Synchronize the device inventory from the Smart Account, see [View, Synchronize, and Deregister Smart Accounts, on page 52](#).
3. Find the devices on the unclaimed devices list, see [View Devices, on page 39](#).
4. Claim the devices by assigning a workflow or by directly assigning a software image and configuration template. For more information, see [Claim a Device, on page 41](#).
5. Devices boot up and are automatically provisioned according to their workflows.

Manage Plug and Play Devices

Devices Overview

The **Network Plug and Play > Devices** window shows all network devices that the Network Plug and Play tool is onboarding and provisioning. The following tabs are available:

- **All Devices**—Lists all devices, including unclaimed, provisioned, and devices with an error.
- **Unclaimed**—Lists unclaimed devices, which are devices that have not yet been claimed for provisioning.
- **Provisioned**—Lists devices that have completed provisioning successfully.
- **Errors**—Lists devices that have had an error in provisioning.

To manage devices, you can use the controls above the list, shown in [Table 20: Device Controls, on page 37](#).



- Note** Not all options are available from each device tab. For example, the **Edit** and **Claim** options are available only from the **All Devices** and **Unclaimed** tabs. Additionally, some of the options are available from the device details window that opens when you click a device name.

Table 20: Device Controls

Control	Description
Filter	Click Filter to specify one or more filter values and then click Apply . Use the asterisk (*) character as a wildcard anywhere in the string. You can apply multiple filters. To remove a filter, click the x icon next to the corresponding filter value.
Claim	Select one or more devices and click Claim to claim the device. For more information, see Claim a Device, on page 41 .
Edit	Select one device and click Edit to edit the device. For more information, see Add or Edit a Device, on page 39 .
Delete	Select one or more devices and click Delete to delete and reset the devices. For more information, see Delete or Reset a Device, on page 43 .
Reset	Select one or more devices and click Reset to reset the devices. For more information, see Delete or Reset a Device, on page 43 .
Refresh	Click to refresh the device list.
Export	Click to export the list as a CSV file.
Add	Click to add a device. For more information, see Add or Edit a Device, on page 39 or Add Devices in Bulk, on page 40 .
Find	Enter a search term in the Find field to find all devices that have that term in any column. Use the asterisk (*) character as a wildcard anywhere in the search string.
Show entries	Select the number of device entries to show in each page of the table.

The Device table displays the information shown in [Table 21: Device Information, on page 38](#) for each device. All of the columns support sorting. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.



Note Not all columns are used in each device tab. Additionally, some of the columns are hidden in the default column view setting, which can be customized by clicking on the 3 dots () at the right end of the column headings.

Table 21: Device Information

Column	Description
Name	Name of the device. Click this link to open the device details window. For more information, see View Devices, on page 39 . A stack icon indicates a switch stack.
Serial Number	Device serial number
Product ID	Device product ID
Source	Source of the device entry
State	<ul style="list-style-type: none"> • Unclaimed—Device has not been assigned a workflow • Planned—Device has been assigned a workflow but has not yet contacted the server. • Onboarding—Device onboarding is in progress • Provisioned—Device is successfully onboarded and added to inventory • Error—Device had an error and could not be provisioned
Onboarding State	Onboarding state of the device
Last Contact	Last date and time the device contacted Network Plug and Play
Workflow	Workflow that the device is using
Smart Acct	Smart Account with which the device is associated
Virtual Acct	Virtual Account (within the Smart Account) with which the device is associated
Added On	Date and time when the device was added to Network Plug and Play

View Devices

Procedure

Step 1 From the DNA Center home page, choose **Network Plug and Play**.

Step 2 Click the **Devices** tab.

The **All Devices** tab lists all of the devices. You can use the Filter or Find options to find a device, or choose the Unclaimed, Provisioned, or Errors tabs to see just those types of devices.

Step 3 Click the name of a device.

A window with the device details is displayed.

Step 4 Click the **Details**, **History**, **Workflow**, and **Stack** tabs to switch between different types of detailed information for the device. Some tabs have additional links that you can click for more information.

The **Stack** tab appears only for a switch stack device.

Step 5 Click the following actions at the top of the dialog to perform specific tasks on the device. Available actions depend on the device state.

- **Refresh**—Refreshes the device state information.
- **Claim**—Claims the device. For more information, see [Claim a Device, on page 41](#).
- **Edit**—Edits the device. For more information, see [Add or Edit a Device, on page 39](#).
- **Reset**—Resets the device, see [Delete or Reset a Device, on page 43](#).
- **Delete**—Deletes the device, see [Delete or Reset a Device, on page 43](#).

Add or Edit a Device

This procedure shows how to add or edit a device from the **Devices** tab. Alternately, you can add a device from the Dashboard by clicking **Add devices**, and you can edit a device from the device details window by clicking **Edit**.

Table 22: Device Fields

Field	Description
Serial Number	Device serial number (read only if you are editing a device)
Product ID	Device product ID (read only if you are editing a device)
Device Name	Device name
Enable SUDI Authorization	Enables SUDI authorization on devices that support it.

Field	Description
SUDI Serial Numbers	Devices that support SUDI have two serial numbers: the chassis serial number and the SUDI serial number (called the License SN on the device label). Enter one or more comma-separated SUDI serial numbers in this field when adding a device that uses SUDI authentication. This field appears only if Enable SUDI Authorization is checked.
This Device Represents a Stack	Indicates that the device represents a stack (this item is read only if you are editing a device). Applicable only for supported stackable switches that are being planned.

Before you begin

If the device requires credentials, be sure that the global device credentials are set in the **Design > Network Settings > Device Credentials** page. For more information, see [Configure CLI Credentials, on page 128](#).

Procedure

Step 1 From the DNA Center home page, choose **Network Plug and Play**.

Step 2 Click the **Devices** tab.

The **All Devices** tab lists all of the devices. You can use the Filter or Find options to find a device, or choose the Unclaimed tab to see just unclaimed devices.

Step 3 Either add or edit a device, as follows:

- To add a device, click **Add** and the add device dialog is displayed.
- To edit a device, check the check box next to the name of the device you want to edit and click **Edit** in the menu bar above the device table. The edit devices dialog is displayed.

Step 4 Set the fields as needed, referring to [Table 22: Device Fields, on page 39](#) for more information.

Step 5 Save the settings by doing one of the following:

- If you are adding a device and will claim it later, click **Add Device**.
 - If you are adding a device and want to claim it by assigning a workflow to it, click **Add + Claim**. For more information, see [Claim a Device, on page 41](#)
 - If you are editing a device, click **Edit Device**.
-

Add Devices in Bulk

This procedure shows how to add devices in bulk from a CSV file.



Note If you add a device that already exists in Network Plug and Play, there is no change to the existing device.

Procedure

Step 1 From the DNA Center home page, choose **Network Plug and Play**.

Step 2 Click the **Devices** tab.

Step 3 Click **Add**.

The Add Devices dialog is displayed.

Step 4 Click the **Bulk Devices** tab.

Step 5 Click **Download File Template** to download the sample file.

Step 6 Add the information for each device to the file and save the file.

Step 7 Upload the CSV file by doing one of the following actions:

- Drag and drop the file to the drag and drop area.
- Click where it says "click to select" and select the file.

Step 8 Click **Import Devices**.

The devices in the CSV file are listed in a table.

Step 9 Check the box next to each device to import, or click the check box at the top to select all devices.

Step 10 Add the devices by doing one of the following:

- To add the devices and claim them later, click **Add Devices**.
- To add the devices and claim them by assigning one workflow to the whole group, click **Add + Claim**.
For more information, see [Claim a Device, on page 41](#)

Claim a Device

Claiming a device assigns a provisioning workflow to it. If you claim a device that has not yet booted for the first time, then you are planning the device so that it is automatically provisioned when it boots.

This procedure shows how to claim a device from the Devices tab. Alternately, you can claim a device from the device details window by clicking **Claim**.

Before you begin

- Upload to the DNA Center image repository any software images that you want to deploy to devices. For more information, see [Import Software Images, on page 81](#). Alternatively, identify the network location of software images to be deployed by URL.
- Optionally, use the DNA Center Template Editor to define one or more configuration templates that you want to use to provision devices. For more information, see [Create Templates to Automate Device Configuration Changes, on page 139](#). Alternatively, identify the network location of configuration files to be deployed by URL.

- Optionally, define one or more workflows that you want to use to provision devices. For more information, see [Create or Edit a Workflow, on page 45](#)

Procedure

Step 1 From the DNA Center home page, choose **Network Plug and Play**.

Step 2 Click the **Devices** tab.

The **All Devices** tab lists all of the devices. You can use the Filter or Find options to find a device, or choose the Unclaimed tab to see just unclaimed devices.

Step 3 Click the **Unclaimed** tab.

Step 4 Check the check box next to one or more devices that you want to claim.

Step 5 Click **Claim** in the top bar.

The Claim Devices dialog opens.

Step 6 From the Workflow drop-down list, optionally choose a workflow to assign to the devices.

Skip to Step 9 if you selected a workflow, or continue with the next step if you want to directly assign a software image and/or configuration.

Step 7 In the Image area, choose a software image to apply to the devices, by doing one of the following:

- Click **Image** and choose an image that has been uploaded to the DNA Center image repository. After you choose an image, you can view details about it by clicking **Image Details**.
- Click **Import Image** to open the DNA Center image repository in a new tab and import an image. After you import an image, you can view details about it by clicking **Image Details**.
- Click **URL** and specify a TFTP or USB source from which the device can download the software image.

Step 8 In the Configuration area, choose a configuration file or template to apply to the devices, by doing one of the following:

- Click **File** and choose a configuration file that has been previously imported. After you choose a file, you can view it by clicking **View File**.
- Click **Import File** and import a configuration file. After you import a file, you can view it by clicking **View File**.
- Click **Template** and choose a template project and template that has been previously defined in the DNA Center Template Editor tool. After you choose a template, you can view it by clicking **View Template**.
- Click **URL** and specify a TFTP or USB source from which the device can download the configuration file.

Step 9 If a configuration template is part of the selected workflow or was chosen directly, specify the values for the parameters that were defined in the template.

A row for each device is displayed in a table and template parameter names are shown as column names. Enter the values for each parameter in the fields for each device. A red asterisk indicates required fields.

Step 10 Optionally click **Add Workflow** if you want to add a new workflow.

For more information, see [Create or Edit a Workflow, on page 45](#).

- Step 11** Click **Claim** to claim the devices and start the provisioning process.

Delete or Reset a Device

Deleting a device removes it from the Network Plug and Play database but does not reset the device.

Resetting a device resets it to the factory state but does not remove it from the Network Plug and Play database. You can use this option to cause the device to restart the provisioning process.

Procedure

- Step 1** From the DNA Center home page, choose **Network Plug and Play**.

- Step 2** Click the **Devices** tab.

The **All Devices** tab lists all of the devices. You can use the Filter or Find options to find a device, or choose the Unclaimed, Provisioned, or Errors tabs to see just those types of devices.

- Step 3** Check the check box next to one or more devices that you want to delete or reset.

- Step 4** Click **Delete or Reset**.

A confirmation dialog is displayed.

- Step 5** If you are resetting a device, choose one of the following workflow options:

- **Reset and keep current workflow**—Current workflow remains and device goes to Planned state.
- **Reset and remove current workflow**—Workflow is removed and device goes to Unclaimed state.

- Step 6** Click **Delete or Reset**.

Manage Plug and Play Workflows

Workflows Overview

A workflow defines a network device provisioning process that include a series of actions such as installing a software image, applying a device configuration, renumbering a switch stack, and specifying a switch stack license. A workflow is applied to a device when the device is claimed and the workflow executes when the device boots up. After a workflow completes successfully, the device is added to the DNA Center inventory, as long as the device credentials are configured in the global network settings.

The **Network Plug and Play > Workflows** window lists all workflows. To manage workflows, you can use the controls above the list, shown in [Table 23: Workflow Controls, on page 44](#).

Some of the options are also available from the workflow details window that opens when you click a workflow name.

Table 23: Workflow Controls

Control	Description
Filter	Click Filter to specify one or more filter values and then click Apply . Use the asterisk (*) character as a wildcard anywhere in the string. You can apply multiple filters. To remove a filter, click the x icon next to the corresponding filter value.
Clone	Select a workflow and click Clone to copy the workflow. For more information, see Clone a Workflow, on page 48 .
Edit	Select one workflow and click Edit to edit the workflow. For more information, see Create or Edit a Workflow, on page 45 .
Delete	Select a workflow and click Delete to delete the workflow. For more information, see Delete a Workflow, on page 50 .
Refresh	Click to refresh the workflow list.
Add	Click to add a workflow. For more information, see Create or Edit a Workflow, on page 45 .
Find	Enter a search term in the Find field to find all workflows that have that term in any column. Use the asterisk (*) character as a wildcard anywhere in the search string.
Show entries	Select the number of workflow entries to show in each page of the table.

The Workflows table displays the information shown in [Table 24: Workflows Information, on page 44](#) for each workflow. The Worflow 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.



Note Some of the columns are hidden in the default column view setting, which can be customized by clicking on the 3 dots () at the right end of the column headings.

Table 24: Workflows Information

Column	Description
Workflow	Name of the workflow. Click this link to open the workflow details window. For more information, see View a Workflow, on page 45 .
Tasks	Icons depicting the tasks in the workflow

Column	Description
Devices	Number of devices using the workflow
Completes Onboarding	A checkmark indicates that devices that complete this workflow are provisioned and ready for management and no other workflows can be applied.
Created	Date and time when the workflow was created
Modified	Date and time when the workflow was last modified

View a Workflow

Procedure

Step 1 From the DNA Center home page, choose **Network Plug and Play**.

Step 2 Click the **Workflows** tab.

The **Workflows** tab lists all of the workflows. You can use the Filter or Find options to find a workflow.

Step 3 Click the name of a workflow.

A window with the workflow details and tasks is displayed.

Step 4 Click the arrow next to a task to expand the task and display the details.

Step 5 Click the **Devices** tab to see devices that are using the workflow.

Step 6 Click the following actions at the top of the dialog to perform specific tasks on the workflow.

- **Clone**—Clones the workflow. For more information, see [Clone a Workflow, on page 48](#).
 - **Edit**—Edits the workflow. For more information, see [Create or Edit a Workflow, on page 45](#).
 - **Delete**—Deletes the workflow, see [Delete a Workflow, on page 50](#).
-

Create or Edit a Workflow

A workflow is a series of provisioning tasks that are performed on a network device.



Note You cannot edit a workflow that is in use.

Table 25: Workflow Fields

Field	Description
Name	Workflow name
Description	Optional description

Field	Description
Tasks > Image	<p>Installs a software image on the device</p>
	<p>Reload after image upgrade—Reloads the network device following the image installation</p>
	<p>Options:</p> <ul style="list-style-type: none"> • Image—Choose an image that has been uploaded to the DNA Center image repository. • Import Image—Open the DNA Center image repository in a new tab and import an image. • URL—Specify a TFTP or USB source from which the device can download the software image.
Tasks > Configuration	<p>Applies a configuration to the device.</p>
	<p>Save to startup—Saves the new configuration as the startup configuration on the device</p>
	<p>Rollback on connection loss—Roll back the configuration on the device to the previous configuration, if there is a connection loss before the new configuration is successfully applied</p>
	<p>Options:</p> <ul style="list-style-type: none"> • File—Choose a configuration file that has been previously imported. After you choose a file, you can view it by clicking View Configuration. • Import Configuration—Import a configuration file. • Template—Choose a template project and template that has been previously defined in the DNA Center Template Editor tool. • URL—Specify a TFTP or USB source from which the device can download the configuration template.

Field	Description
Tasks > Renumber Stack	<p>Renumerates a switch stack. The user is asked during the claim process to set the device that is the top of the stack. This task applies only to the Cisco Catalyst 3650, 3850, and 9000 Series switches that support stacking, and only if they use the following stack cabling scheme.</p> <p>Figure 3: Stack Cabling Required for Renumbering</p>
Tasks > Stack License	<p>Specifies a switch stack license level. The user is asked during the claim process to specify the license level of the stack. Applies only to the Cisco Catalyst 3650, 3850, and 9000 Series switches that support stacking.</p>

Before you begin

- Upload to the DNA Center image repository any software images that you want to deploy to devices. For more information, see [Import Software Images, on page 81](#). Alternatively, identify the network location of software images to be deployed by URL.
- Optionally, use the DNA Center Template Editor to define one or more configuration templates that you want to use to provision devices. For more information, see [Create a Regular Template, on page 140](#). Alternatively, identify the network location of configuration files to be deployed by URL.

Procedure

- Step 1** From the DNA Center home page, choose **Network Plug and Play**.
- Step 2** Click **Workflows**.
- Step 3** You can add or edit a workflow:
 - To add a new workflow, click **Add**.
 - To edit an existing workflow, click the radio button next to the workflow name and click **Edit**.
- Step 4** Set the fields as needed, referring to [Table 25: Workflow Fields, on page 45](#) for more information.
- Step 5** By default, Image and Configuration tasks are included in a new workflow. If you do not need a task, you can delete it by clicking the trash can icon next to the task.
- Step 6** Click **New Task** and optionally add one or more additional tasks to the workflow.
- Step 7** To change the order of tasks in the workflow, click the up or down arrow icons next to a task to adjust its order.

- Step 8** Click **Add** to create the new workflow or **Update** to save an edited workflow.

Clone a Workflow

Cloning a workflow makes a copy of it and allows you to change the copy.

This procedure shows how to clone a workflow from the Workflows tab. Alternately, you can clone a workflow from the workflow details dialog by clicking **Clone**.

Table 26: Workflow Fields

Field	Description
Name	Workflow name
Description	Optional description
Tasks > Image	<p>Installs a software image on the device</p> <p>Reload after image upgrade—Reloads the network device following the image installation</p> <p>Options:</p> <ul style="list-style-type: none"> • Image—Choose an image that has been uploaded to the DNA Center image repository. • Import Image—Open the DNA Center image repository in a new tab and import an image. • URL—Specify a TFTP or USB source from which the device can download the software image.
Tasks > Configuration	<p>Applies a configuration to the device.</p> <p>Save to startup—Saves the new configuration as the startup configuration on the device</p> <p>Rollback on connection loss—Roll back the configuration on the device to the previous configuration, if there is a connection loss before the new configuration is successfully applied</p> <p>Options:</p> <ul style="list-style-type: none"> • File—Choose a configuration file that has been previously imported. After you choose a file, you can view it by clicking View Configuration. • Import Configuration—Import a configuration file. • Template—Choose a template project and template that has been previously defined in the DNA Center Template Editor tool. • URL—Specify a TFTP or USB source from which the device can download the configuration template.

Field	Description
Tasks > Renumber Stack	<p>Renumerates a switch stack. The user is asked during the claim process to set the device that is the top of the stack. This task applies only to the Cisco Catalyst 3650, 3850, and 9000 Series switches that support stacking, and only if they use the following stack cabling scheme.</p> <p>Figure 4: Stack Cabling Required for Renumbering</p>
Tasks > Stack License	<p>Specifies a switch stack license level. The user is asked during the claim process to specify the license level of the stack. Applies only to the Cisco Catalyst 3650, 3850, and 9000 Series switches that support stacking.</p>

Before you begin

There must be a workflow defined in order to clone it.

Procedure

Step 1 From the DNA Center home page, choose **Network Plug and Play**.

Step 2 Click the **Workflows** tab.

The **Workflows** tab lists all of the workflows. You can use the Filter or Find options to find a workflow.

Step 3 Click the radio button next to the name of a workflow.

Step 4 Click **Clone**.

Step 5 Set the fields as needed, referring to [Table 26: Workflow Fields, on page 48](#) for more information.

Step 6 If you do not need a task, you can delete it by clicking the trash can icon next to the task.

Step 7 Click **New Task** and optionally add one or more additional tasks to the workflow.

Step 8 To change the order of tasks in the workflow, click the up or down arrow icons next to a task to adjust its order.

Step 9 Click **Clone** to save the workflow copy with your changes.

Delete a Workflow

You cannot delete a workflow that has devices assigned to it. You must first assign those devices to a different workflow before deleting it.

Procedure

-
- Step 1** From the DNA Center home page, choose **Network Plug and Play**.
- Step 2** Click **Workflows**.
- Step 3** Click the radio button next to the workflow name and click **Delete**.
- Step 4** Click **Delete** in the confirmation dialog.
-

Manage Plug and Play Settings

Settings Overview

The **Network Plug and Play > Settings** window allows you to do the following configuration tasks that are specific to Network Plug and Play:

- [Accept the EULA, on page 50](#)—Accept the End User License Agreement, which is required for using Network Plug and Play.
- [Manage Cisco Smart Accounts, on page 51](#)—Register DNA Center as a controller for Cisco Plug and Play Connect, in a Cisco Smart Account, for redirection services. This lets you synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Network Plug and Play in DNA Center.

Accept the EULA

You must accept the End User License Agreement (EULA) before using Network Plug and Play.

Procedure

-
- Step 1** From the DNA Center home page, choose **Network Plug and Play**.
- Step 2** Click **Settings > EULA Acceptance**.
- Step 3** To read the EULA, click the [End User License Agreement link](#).
- Step 4** Click the **Accept EULA** check box.
- Step 5** Click **Apply**.
-

Manage Cisco Smart Accounts

The Network Plug and Play > Settings > Smart Accounts window allows you to do the following tasks:

- [Register or Edit a Virtual Account, on page 51](#)—Register DNA Center as a controller for Cisco Plug and Play Connect, in a Cisco Smart Account, for redirection services. This lets you synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Network Plug and Play in DNA Center.
- [View, Synchronize, and Deregister Smart Accounts, on page 52](#)

Register or Edit a Virtual Account

This procedure lets you register the DNA Center controller as a controller for Cisco Plug and Play Connect, in a Cisco Smart Account, for redirection services. Also, this lets you synchronize the device inventory from Cisco Plug and Play Connect to Network Plug and Play.

Table 27: Virtual Account Fields

Field	Description
Select Smart Account	Cisco Smart Account name
Select Virtual Account	Virtual Account name
Use as Default Controller Profile	Check this box to register this DNA Center controller as the default controller in the Cisco Plug and Play Connect cloud portal.
Controller IP	IP address of this DNA Center controller
Profile Name	Controller profile name

Before you begin

Set the Cisco Smart Account credentials in the main DNA Center settings by using **System Settings > Settings > Cisco Credentials**. For more information, see "[Configure Cisco Credentials](#)" in the *Cisco Digital Network Architecture Center Administrator Guide*.

Procedure

Step 1 From the DNA Center home page, choose **Network Plug and Play**.

Step 2 Click **Settings > Smart Accounts**.

The table lists all of the registered virtual account profiles.

Step 3 Either add or edit a virtual account profile, as follows:

- To register a virtual account, click **Add** and the register virtual account dialog is displayed.
- To edit a registered virtual account profile, click the radio button next to the name of the profile that you want to edit and click **Edit Profile** in the menu bar above the table. The edit virtual account dialog is displayed.

View, Synchronize, and Deregister Smart Accounts

- Step 4** Set the fields as needed, referring to [Table 27: Virtual Account Fields, on page 51](#) for more information.
- Step 5** Save the settings by doing one of the following:
- If you are registering a new virtual account profile, click **Register**.
 - If you are editing a virtual account profile, click **Change**.
-

What to do next

Synchronize the device inventory from Cisco Plug and Play Connect to Network Plug and Play. For more information, see [View, Synchronize, and Deregister Smart Accounts, on page 52](#).

View, Synchronize, and Deregister Smart Accounts

The **Network Plug and Play > Settings > Smart Accounts** window lists all registered virtual account profiles. Virtual accounts are sub-accounts within a Cisco Smart Account. To manage virtual account profiles, you can use the controls above the list, shown in [Table 28: Virtual Account Controls, on page 52](#).

Table 28: Virtual Account Controls

Control	Description
Edit Profile	Select a virtual account profile and click Edit Profile to edit it. For more information, see Register or Edit a Virtual Account, on page 51 .
Refresh	Refreshes the virtual account profile list.
Export	Exports the table as a CSV file.
Add	Click to register a virtual account. For more information, see Register or Edit a Virtual Account, on page 51 .
Find	Enter a search term in the Find field to find all virtual account profiles that have that term in any column. Use the asterisk (*) character as a wildcard anywhere in the search string.

The Virtual Accounts table displays the information shown in [Table 29: Virtual Accounts Information, on page 52](#) for each profile.

Table 29: Virtual Accounts Information

Column	Description
Virtual Accounts	Virtual account name
Smart Accounts	Smart account that the virtual account is associated with
Profile	Profile name

Column	Description
Last Sync Time	Last time the device inventory from the virtual account was synchronized with Network Plug and Play
Sync Status	Status of the last synchronization process
Sync Result	Number of devices added, updated, and removed in the last synchronization

Before you begin

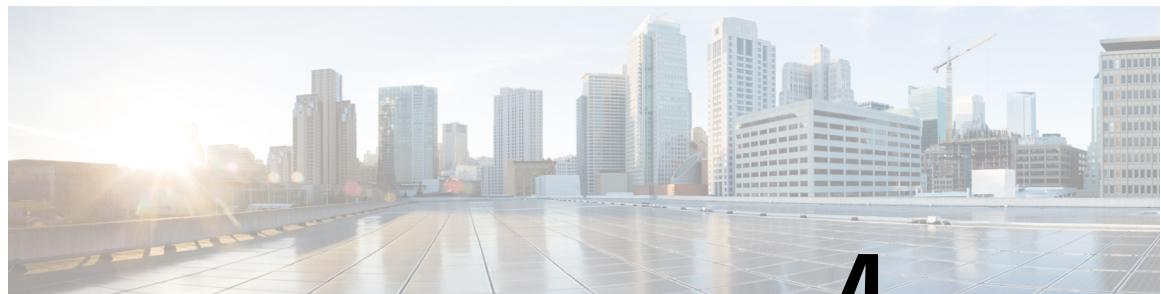
Before you can synchronize the device inventory from the Cisco Plug and Play Connect cloud portal, you must register a virtual account, see [Register or Edit a Virtual Account, on page 51](#).

Procedure

- Step 1** From the DNA Center home page, choose **Network Plug and Play**.
 - Step 2** Click **Settings > Smart Accounts**.
 - Step 3** Click on the name of a virtual account profile to display detailed information.
 - Step 4** Click **Sync** to synchronize the device inventory from Cisco Plug and Play Connect in this virtual account to Network Plug and Play.
 - Step 5** If you want to remove this virtual account profile, click **Deregister**.
 - Step 6** In the confirmation dialog, click **Deregister**.
-

What to do next

Claim the newly synchronized devices by assigning a workflow or by directly assigning a software image and configuration template. For more information, see [Claim a Device, on page 41](#).



CHAPTER 4

Manage Your Inventory

- [About Inventory, on page 55](#)
- [Inventory and Cisco ISE Authentication, on page 56](#)
- [Display Information About Your Inventory, on page 56](#)
- [Types of Devices in the DNA Center Inventory, on page 60](#)
- [Filter Devices, on page 70](#)
- [Change Devices Layout View, on page 71](#)
- [Change Device Role \(Inventory\), on page 71](#)
- [Update a Device's Management IP Address, on page 72](#)
- [Update Device Resync Interval, on page 73](#)
- [Resync Device Information, on page 73](#)
- [Delete a Network Device, on page 74](#)
- [Launch Command Runner \(Inventory\), on page 74](#)
- [Use a CSV File to Import and Export Device Configurations, on page 75](#)

About Inventory

The Inventory function retrieves and saves details, such as host IP addresses, MAC addresses, and network attachment points about devices in its database.

The Inventory feature can also work with the Device Controllability feature to configure required network settings on devices, if these settings are not already present on the device. For more information about Device Controllability, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

Inventory uses the following protocols, as required:

- Link Layer Discovery Protocol (LLDP).
- IP Device Tracking (IPDT) or Switch Integrated Security Features (SISF). (IPDT or SISF must be enabled on the device.)
- LLDP Media Endpoint Discovery. (This protocol is used to discover IP phones and some servers.)
- Network Configuration Protocol (NETCONF). For a list of devices, see [Discovery Prerequisites, on page 8](#).)

After the initial discovery, DNA Center maintains the inventory by polling the devices at regular intervals. The default and minimum interval is every 25 minutes. However, you can change this interval to be from 25

minutes to 24 hours, as required for your network environment. For more information, see [Update Device Resync Interval, on page 73](#).) 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.

Inventory and Cisco ISE Authentication

Cisco ISE has two different use cases in DNA Center:

- If your network uses Cisco ISE for device authentication, you need to configure the Cisco ISE settings in DNA Center. In this way, when provisioning devices, DNA Center configures the devices with the Cisco ISE server information that you defined. In addition, DNA Center configures the devices on the Cisco ISE server and propagates any subsequent updates to the devices to Cisco ISE server as well. For information about configuring Cisco ISE setting in DNA Center, see [Configure Global Network Servers, on page 134](#).

If a device is not configured or updated on the Cisco ISE server as expected due to a network failure or the Cisco ISE server being down, DNA Center automatically retries the operation after a certain wait period. However, DNA Center does not retry the operation if the failure is due to a rejection from Cisco ISE as a input validation error.

When DNA Center configures and updates devices in the Cisco ISE server, the transactions are captured in the DNA Center audit logs. You can use the audit logs to help you troubleshoot issues related to the DNA Center and Cisco ISE inventories. For more information about the DNA Center audit logs, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

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. 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 credentials. Instead, it goes into a partial collection state.

To avoid this situation, make sure that before you provision devices using DNA Center, you have configured the devices in Cisco ISE with the same device credentials that you are using in DNA Center. Also, make sure that you configured valid discovery credentials. For more information, see [Discovery Credentials, on page 8](#).

- If you want, you can use Cisco ISE to enforce access control to groups of devices. For information about this use case, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

Display Information About Your Inventory

The **Inventory** table displays 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.

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 **Inventory** tool.

Table 30: *Inventory*, on page 57 describes the information that is available.

Table 30: Inventory

Column	Description
Device Name	Name of the device. Click the name to display the Device Overview dialog box with the following information: <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 A device name that is displayed in red means that inventory has not polled the device and updated its information for more than 30 minutes.</p>
IP Address	IP address of the device.

Display Information About Your Inventory

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 Sometimes a device is unreachable because the discovery job does not have its credentials or the discovery job has the wrong credentials. If you suspect this might be the case, perform a new discovery job and make sure to specify the device's correct credentials.</p>
MAC Address	MAC address of the device.
OS Version	Cisco IOS software that is currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Uptime	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
Device Role	<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 to unknown.</p> <p>Note If you manually change the device role, the assignment remains static. DNA Center does not update the device role even if it detects a change during a subsequent device resynchronization.</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
Site	The site to which the device is assigned. For more information, see About Network Hierarchy, on page 92 .
Last Updated	Most recent date and time that DNA Center scanned the device and updated the database with new information about the device.
Device Family	Group of related devices, such as routers, switches and hubs, or wireless controllers.
Device Series	Series number of the device, for example, Cisco Catalyst 4500 Series Switches.
Resync Interval	The polling interval for the device. This interval can be set globally in Settings or for a specific device in Inventory. For more information, see the Cisco Digital Network Architecture Center Administrator Guide .

Column	Description
Last Sync 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.

- Step 2** (Optional) To change the layout, click  and choose one of the following layouts or customize your own layout:
- **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**.

Types of Devices in the DNA Center Inventory

Devices show up in inventory one of two ways: by being discovered or by being added manually. DNA Center Inventory supports the following types of devices:



Note For a complete list of supported devices, see the [Cisco Digital Network Architecture Center Supported Devices](#) document.

- **Network Devices**—Supported network devices include Cisco routers, switches, and wireless devices such as wireless controllers (WLCs) and access points (APs).
- **Compute Devices**—Supported compute devices include the Cisco Unified Computing System (UCS), devices running Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS), and other data center devices.

- **Meraki Dashboard**—Dashboard to the Cisco cloud management platform for managing Cisco Meraki products.

Manage Network Devices

Add a Network Device

You can add a network device to your inventory manually.

Procedure

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

Step 2 Click **Add**.

The **Add Device** dialog box is displayed.

Step 3 From the **Type** drop-down list, choose **Network Device**.

Step 4 In the **Device IP / Name** field, enter the IP address or name of the device.

Step 5 Expand the **SNMP** area, if it is not already visible.

Step 6 From the **Version** drop-down list, choose **V2C** (SNMP version 2c) or **V3** (SNMP, version 3).

If you chose **V2C**, configure the following fields:

Table 31: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none">• Name/Description—Name or description of the SNMPv2c 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 SNMPv2c 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 32: SNMPv3 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. Choose one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv—Does not provide authentication or encryption. • AuthNoPriv—Provides authentication but does not provide encryption. • AuthPriv—Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA—Authentication based on HMAC-SHA. • MD5—Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length. <p>Note</p> <ul style="list-style-type: none"> • Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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	Privacy type. (Enabled if you select AuthPriv as the authentication mode.) Select one of the following privacy types: <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.

Field	Description
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"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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.

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

Table 33: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 1 to 3. 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 1 to 300 seconds in intervals of 5 seconds. The default is 5 seconds.

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

Table 34: CLI Credentials

Field	Description
Protocol	<p>Network protocol that enables DNA Center to communicate with remote devices. Valid values are SSH2 or Telnet.</p> <p>If you plan to configure the NETCONF port (see next step), you need to choose SSH2 as the network protocol.</p>
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</p> <p>Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Update Network Device Credentials

Field	Description
Enable Password	<p>Password used to move to a higher privilege level in the CLI.</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 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**.

Related Topics

[Types of Devices in the DNA Center Inventory](#), on page 60

Update Network Device Credentials

You can update the discovery credentials of selected network 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 **Inventory**.
- Step 2** Select the network devices that you want to update.
- Step 3** From the **Actions** drop-down list, choose **Update Credentials**.
- Step 4** From the **Type** drop-down field, select **Network Device** if it is not already selected.
- Step 5** 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 35: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> Name/Description—Name or description of the SNMPv2c 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 SNMPv2c 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 36: SNMPv3 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. Choose one of the following modes: <ul style="list-style-type: none"> noAuthNoPriv—Does not provide authentication or encryption. AuthNoPriv—Provides authentication but does not provide encryption. AuthPriv—Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> SHA—Authentication based on HMAC-SHA. MD5—Authentication based on HMAC-MD5.

Field	Description
Auth Password	<p>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</p> <p>Note</p> <ul style="list-style-type: none"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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 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"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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.

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

Table 37: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 1 to 3. 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 1 to 300 seconds in intervals of 5 seconds. The default is 5 seconds.

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 38: CLI Credentials

Field	Description
Protocol	<p>Network protocol that enables DNA Center to communicate with remote devices. Valid values are SSH2 or Telnet.</p> <p>If you plan to configure the NETCONF port (see next step), you need to choose SSH2 as the network protocol.</p>
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>
Enable Password	<p>Password used to move to a higher privilege level in the CLI.</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 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**.

Related Topics

[Types of Devices in the DNA Center Inventory](#), on page 60

Manage Compute Devices

Add a Compute Device

You can add a compute device to your inventory manually. A compute device includes devices such as the Cisco Unified Computing System (UCS), devices running Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS), and other data center devices.

Procedure

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

Step 2 Click **Add**.

The **Add Device** dialog box is displayed.

Step 3 From the **Type** drop-down list, choose **Compute Device**.

Step 4 In the **Device IP / Name** field, enter the IP address or name of the device.

Step 5 Expand the **HTTP(S)** area, if it is not already visible and configure the following fields:

- **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).

Step 6 Click **Add**.

Related Topics

[Types of Devices in the DNA Center Inventory](#), on page 60

Update Compute Device Credentials

You can update the discovery credentials of selected compute 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 **Inventory**.

Step 2 Select the devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Update Credentials**.

Step 4 From the **Type** drop-down field, select **Compute Device**.

Step 5 Expand the **HTTP(S)** area, if it is not already expanded.

Step 6 In the **Username** and **Password** fields, enter the username and password.

-
- Step 7** In the **Port** field, enter the port number.
- Step 8** Click **Update**.

Related Topics

[Types of Devices in the DNA Center Inventory](#), on page 60

Manage Meraki Dashboards

Integrate Meraki Dashboard

You can integrate your Meraki Dashboard with DNA Center.

Procedure

- Step 1** From the DNA Center home page, click **Inventory**.
- Step 2** Click **Add**.
- Step 3** In the **Add Device** dialog box, from the **Type** drop-down list, select **Meraki Dashboard**.
- Step 4** Expand the **HTTP(S)** area, if it is not already expanded.
- Step 5** In the **API Key / Password** field, enter the API key and password credentials used to access the Meraki dashboard.

DNA Center collects inventory data from the Meraki Dashboard and displays the information.

Related Topics

[Types of Devices in the DNA Center Inventory](#), on page 60

Update Meraki Dashboard Credentials

You can update the Meraki Dashboard 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 **Inventory**.
- Step 2** Select the devices that you want to update.
- Step 3** From the **Actions** drop-down list, choose **Update Credentials**.
- Step 4** From the **Type** drop-down field, select **Meraki Dashboard**.
- Step 5** Expand the **HTTP(S)** area, if it is not already expanded.
- Step 6** In the **API Key / Password** field, enter the API key and password credentials used to access the Meraki dashboard.

Step 7 In the **Port** field, enter the port number.

Step 8 Click **Update**.

Related Topics

[Types of Devices in the DNA Center Inventory](#), on page 60

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 **Inventory**.

Step 2 Click **Filters**.

The following filters are displayed:

- Device Name
- IP Address
- MAC Address
- Reachability Status
- IOS/Firmware
- Platform
- Serial Number
- Up Time
- Last Updated Time
- Resync Interval
- Last Inventory Collection Status
- Device Role
- Location
- Device Family
- Device Series

- 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 **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 (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 and to determine a device's placement on the network topology map in the Topology tool.

Update a Device's Management IP Address

A device can have one of the following roles:

- **Unknown**—Device role is unknown. The device is placed above or beside a border router.
- **Access**—(First tier) Device is located in and performs the tasks required of the access layer or edge of the network.
- **Border Router**—Device performs tasks required of a border router.
- **Distribution**—(Second tier) Device is located in and performs the tasks required of the distribution layer of the network.
- **Core**—(Third tier) Device is located in and performs the tasks required of the core of the network.

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 **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**.

Note If you manually change the device role, the assignment remains static. DNA Center does not update the device role even if it detects a change during a subsequent device resynchronization.

Update a Device's Management IP Address

You can update the management IP address of a devices.



Note You cannot update more than one device at a time. Also, you cannot update a Meraki device's management IP address.

Procedure

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

Step 2 Select the devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Update Management IP**.

The **Update Management IP** dialog box is displayed.

Step 4 In the **Device IP** field, enter the new management IP address.

Note Make sure that the new management IP address is reachable from DNA Center and that the device credentials are correct. Otherwise, the device might enter an unmanaged state.

Update Device Resync Interval

From the **Inventory** window, you can configure device resynchronization in the following ways:

- You can enable and configure a custom resynchronization interval for a specific device.
- You can enable the preconfigured global resynchronization interval that is set for all devices. (This setting is configured in the **Settings > System Settings > Settings > Network Resync Interval** window.)
- You can disable resynchronization.

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 **Inventory**.

Step 2 Select the devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Update Resync Interval**.

The **Update Resync Interval** dialog box is displayed.

Step 4 In the **Select Resync Option** field, select the radio button that corresponds to the type of resynchronization option you want to configure for the device. Valid choices are **Custom**, **Global**, and **Disable**.

Step 5 If you chose **Custom**, in the **Resync Interval (in Mins)** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24-hours).

Step 6 Click **Update**.

Resync Device Information

You can resynchronize device information immediately for selected devices, regardless of their resynchronization interval configuration. A maximum of 40 devices can be resynchronized at the same time.

Procedure

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

Step 2 Select the devices that you want to gather information about.

Step 3 From the **Actions** drop-down list, choose **Resync**.

- Step 4** Confirm the action by clicking **OK**.

Delete a Network Device

You can delete devices from the DNA Center database, as long as they have not already been added to a site.

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 **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** From the **Actions** drop-down list, choose **Delete**.

Launch Command Runner (Inventory)

You can launch the command runner application for selected devices from within the **Inventory** window.

Before you begin

Install the Command Runner application. For more information, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

Procedure

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

- Step 2** Select the devices that you want to run commands on.

- Step 3** From the **Actions** drop-down list, choose **Launch Command Runner**.

For information about the commands you can run and how to run them, see [Running Diagnostic Commands on Devices, on page 151](#).

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) **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

Import Device Configurations From a CSV File

- 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 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 **Inventory**.
 - Step 2** Click **Import Device(s)** to import all of the devices from the CSV file into **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

You can export specific data of selected devices to a CSV file. The CSV file is compressed.



Caution

Handle the CSV file with care because it contains sensitive information about the exported devices. Ensure that only users with special privileges perform a device export.

Procedure

- Step 1** From the DNA Center home page, click **Inventory**.
 - Step 2** To export configuration information about only certain devices, select the check box next to the devices that you want to include. To include all devices, select the check box at the top of the device list.
 - Step 3** Click **Export**.
- The **Export** dialog box appears.
- Step 4** Select the check boxes next to the data that you want to include in the CSV file.

Step 5 Click **Export**.

Note Depending on your browser configuration, you can save or open the compressed file.

Export Device Credentials

You can export device credentials to a CSV file. You are required to configure a password to protect the file from unwanted access. You need to supply the password to the recipient so that the file can be opened.



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 **Inventory**.

Step 2 Select the check box next to the devices that you want to include in the CSV file. To include all devices, select the checkbox at the top of the list.

Step 3 Click **Export** to export the device credentials.

The **Export** dialog box appears.

Step 4 In the **Select Export Type** field, select the **Credentials** radio button.

Step 5 In the **Password** field, enter a password that will be used to encrypt the exported CSV file.

Note The password is required to open the exported file.

Step 6 Confirm the encryption password and click **Export**.

Note Depending on your browser configuration, you can save or open the compressed file.

Export Device Credentials



CHAPTER 5

Manage Software Images

- [About Image Repository, on page 79](#)
- [Integrity Verification of Software Images, on page 79](#)
- [Viewing Software Images, on page 80](#)
- [Using Recommended Software Images, on page 80](#)
- [Import Software Images, on page 81](#)
- [About Golden Software Images, on page 81](#)
- [Creating Golden Software Images, on page 82](#)
- [Provision Software Images, on page 82](#)

About Image Repository

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

- Image Repository—DNA Center stores all the 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.

Before using Image Repository features, you must enable Transport Layer Security protocol (TLS) on older devices such as Catalyst 3K, 4K, and 6K. After any system upgrades, you must re-enable TLS again. For more information, see “Configure Security for Cisco DNA Center” in the [Cisco Digital Network Architecture Center Administrator Guide](#).

Integrity Verification of Software Images

Integrity Verification (IV) monitors software images that are stored in DNA Center for unexpected changes or invalid values that could indicate your devices are compromised. IV compares each device's software, hardware, platform, and configuration settings against an authoritative set of Known Good Values (KGV).

On the **Image Repository** window, a message displays if IV is unable to verify the selected software image using the current KGV file. For more information about IV and importing KGV files, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

Viewing Software Images

After you run Discovery or manually add devices, DNA Center automatically stores information about the software images, SMUs and sub-packages for the devices.

Procedure

- Step 1** From the DNA Center home page, choose **Design > Image Repository** or click **Image Repository**. The software images are organized and displayed based on the device type. By default, software images for physical devices are displayed. You can toggle to Virtual tab to view software images for virtual devices.
 - Step 2** In the **Image Name** column, click the downward arrow to view all the software images for the specified device type family. The **Using Image** column indicates how many devices are using the specific image you selected in the **Image Name** field. Click the number link to view the devices that are using the image.
 - Step 3** In the Version column, click the **Add On** link to view the applicable **SMUs** and **Sub-packages** for the base image. Sub-packages are the additional features that can be added to the existing base image. The sub-package version that is same as the image family and the base image version is displayed here.
 - Note** If you tag any SMU as golden, it will be automatically activated when the base image is installed. You cannot tag a sub-package as golden.
 - Step 4** In the **Device Role** column, select a device role for which you want to indicate this is a "golden" software image. For more information, see [About Golden Software Images, on page 81](#) and [Creating Golden Software Images, on page 82](#).
-

Using Recommended Software Images

DNA Center can display the Cisco-recommended software images for the devices that it manages.

Procedure

- Step 1** From the DNA Center **Home** page, choose  > **System Settings > Settings > Cisco Credentials** and verify that you have entered the correct credentials to connect to Cisco.com.
 - Step 2** Choose **Design > Image Repository** or select **Image Repository** from the DNA Center home page. DNA Center displays the Cisco-recommended software images according to device type.
 - Step 3** Designate the recommended image as golden. See [Creating Golden Software Images, on page 82](#) for more information.

After you designate the Cisco-recommended image as golden, DNA Center automatically downloads the image from cisco.com.
 - Step 4** Push the recommended software image to the devices in your network. See [Provision Software Images, on page 82](#) for more information.
-

Import Software Images

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

Procedure

- Step 1** From the DNA Center home page, choose **Design > Image Repository** or click **Image Repository**.
 - Step 2** Click **Import Image/SMU**.
 - Step 3** Click **Choose File** to navigate to a software image or software image update stored locally or **Enter image URL** to specify an HTTP or FTP source from which to import the software image or software image update.
 - Step 4** If the image you are importing is for a third-party (not Cisco) vendor, select **Third Party** under **Source**. Then select an **Application Type**, describe the device **Family**, and identify the **Vendor**.
 - Step 5** Click **Import**.
A window displays the progress of the import.
 - Step 6** Click **Show Tasks** to verify that the image was imported successfully.
If you imported a SMU, DNA Center automatically applies the SMU to the correct software image, and an **Add-On** link appears below the corresponding software image.
 - Step 7** Click the **Add-On** link to view the SMU.
 - Step 8** In the Device Role field, select the role for which you want to mark this SMU as golden. See [Creating Golden Software Images, on page 82](#) for more information.
Note You can only mark a SMU as golden if you previously marked the corresponding software image as golden.
-

About Golden Software Images

DNA Center allows you to designate software images and SMUs as *golden*. A golden software image or SMU is a validated image that meets the compliance requirements for the 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 an image and a corresponding SMU as golden to create a standardized image. You can also specify a golden image for a specific device role. For example, if you have an image for the Cisco 4431 Integrated Service Routers device family, you can further specify a golden image for those Cisco 4431 devices that have the Access role only.

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

Creating Golden Software Images

You can specify a golden software image for a device family or for a particular device role. The device role is used for identifying and grouping devices according to their responsibilities and placement within the network. For more information, see [About Golden Software Images, on page 81](#).

Procedure

- Step 1** From the DNA Center home page, choose **Design > Image Repository** or click **Image Repository**.
The software images are displayed according to device type.
 - Step 2** From the **Family** column, select a device family for which you want to specify a golden image.
 - Step 3** From the **Image Name** column, select the software image that you want to specify as golden.
 - Step 4** In the **Device Role** column, select a device role for which you want to specify a golden software image. Even if you have devices from the same device family, you can specify a different golden software image for each device role. You can select a device role for physical images only, not virtual images.
-

Provision Software Images

You can push software images to the devices in your network. Before pushing a software image to a device, DNA Center performs pre-checks on the device, such as checking the health of the CPU, disk space, and the route summary. If any pre-checks fail, the software image operation is canceled. After DNA Center pushes a software image to a device, DNA Center repeats these checks to ensure that the state of the network remains unchanged.

DNA Center compares each device's software image with the image that you have designated as golden for that specific device type. If you have not designated a golden image for the device type, then the device's image cannot be updated. See [Creating Golden Software Images, on page 82](#) for more information.

Procedure

- Step 1** From the DNA Center home page, click **Provision**.
- Step 2** Select the device whose image you want to upgrade.
- Step 3** From the **Actions** drop-down list, choose **Update OS Image**.
If any of the pre-checks fail on the device you selected, you cannot update the OS image. Click on the **Outdated** link under the OS image and correct any errors before proceeding.
- Step 4** Select the device whose image you want to upgrade, then click **Update**.
- Step 5** Click **OK** to acknowledge that the device will reload after the image is upgraded.
- Step 6** (Optional) Click **Show Task** to view the progress of the image upgrade.

Note If you have a device between DNA Center and another fabric device, such as an edge router, the software update process might fail if the *in between* device reloads while the software image is being provisioned to the other device.

To continue:

- If you are ready to make the change immediately: Click **Run Now** then click **Confirm**.
 - If you want to update the software image later: Click **Schedule Later** and specify the date and time when you want the change to be applied. Optionally, you can give the change a task name, or specify a different time zone for the schedule. Then click **Confirm**.
-



CHAPTER 6

Display Your Network Topology

- [About Topology, on page 85](#)
- [Display the Topology of Areas, Sites, Buildings, and Floors, on page 86](#)
- [Filter Devices on the Topology Map, on page 86](#)
- [Display Device Information, on page 87](#)
- [Display Link Information, on page 87](#)
- [Pin Devices to the Topology Map, on page 88](#)
- [Save a Topology Map Layout, on page 88](#)
- [Open a Topology Map Layout, on page 88](#)
- [Export the Topology Layout, on page 89](#)

About Topology

The **Topology** window displays a graphical view of your network. Using the discovery settings that you have configured, DNA Center discovers the devices in your network and assigns a device role to them. Based on the device role assigned during discovery (or changed in device inventory), DNA Center creates a physical topology map with detailed device-level data.

Using the topology map, you can do the following:

- Display the topology of a selected area, site, building, or floor.
- Display detailed device information.
- Display detailed link information.
- Filter devices based on a specific Layer 2 VLAN.
- Filter devices based on a Layer 3 protocol (such as Intermediate System - Intermediate System (IS-IS), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), or static routing).
- Filter devices with Virtual Routing and Forwarding (VRF) capability.
- Pin devices to the topology map.
- Save a topology map layout.
- Open a topology map layout.
- Export screen shots of the complete topology layout in Portable Network Graphics (PNG) format.

Display the Topology of Areas, Sites, Buildings, and Floors

You can display the topology of an area, site, building or floor.

Before you begin

- Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.
- You must have defined a network hierarchy and provisioned devices to the buildings or floors within it.

Procedure

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

Step 2 In the tree view menu, select the area, site, building, or floor that you are interested in.

Filter Devices on the Topology Map

You can filter devices based on one of the following attributes:

- VLAN
- Routing
- VRF

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 **Filter**.

Step 3 Do one of the following:

- Click the **VLAN** drop-down field and choose the VLAN that you want to view.
 - Click the **Routing** drop-down field and choose the protocol that interests you.
 - Click the **VRF** drop-down field and choose the VRF that you want to view.
-

Display Device Information

You can display the device name, IP address, and software version of devices.



Note The device information that is accessible in the **Topology** window is also accessible in 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 tree view menu, select the area, site, building, or floor that you are interested in.

Step 3 In the topology area, hover your mouse over the device or device group that interests you.

Note A device group is labeled with the number and types of devices it contains.

Display Link Information

You can display information about the links in the topology map. For simple links, the display shows information for the single link. For aggregated links, the display shows a listing of all underlying links. The information includes the interface name, its speed, and its IP address.

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 tree view menu, select the area, site, building, or floor that you are interested in.

Step 3 Hover your mouse over the link that interests you.

Pin Devices to the Topology Map

Devices can be grouped, or aggregated, so that they take up less room on the map. However, at times, you might want to separate out a device from its group. You can do this by pinning a device to the map.

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 Do one of the following:

- To pin a device, click the device group and, from the slide-out window, click the pin icon to the left of the device name.
 - To pin all devices, click the device group and, from the slide-out dialog box, click **Pin All**.
-

Save a Topology Map Layout

DNA Center has a Cisco recommended topology layout that is displayed by default when you open the topology tool. You can customize multiple layouts and save them to view later. You can also set one of the layouts as the default to be displayed when you open the topology map.

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 **View Options**.

Step 3 Enter a name for your customized map in the **Enter View Title** field.

Step 4 Click **Save**.

Step 5 (Optional) To set your customized map as the default, click **Make Default**.

Open a Topology Map Layout

You can open previously saved topology maps.

Before you begin

You have saved topology map layouts.

Procedure

-
- Step 1** From the DNA Center home page, click **Topology**.
 - Step 2** Click **View Options**.
 - Step 3** Click the name of the map that you want to display.
-

Export the Topology Layout

You can export a screen shot of the full topology layout. The screen shot is downloaded as a PNG file to your local machine.

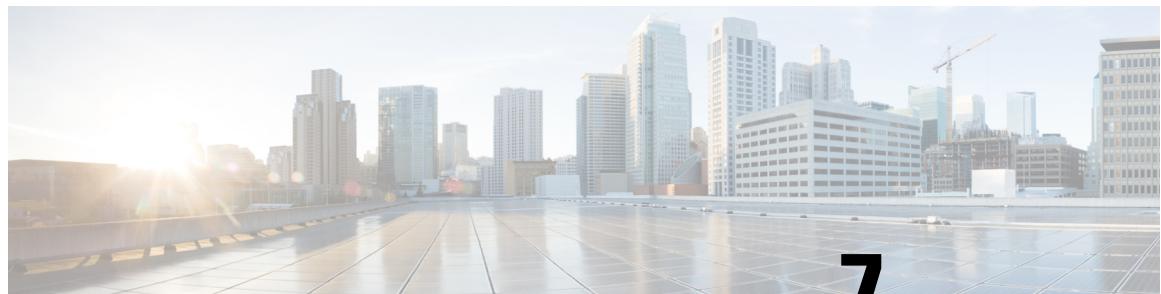
Before you begin

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 .
-

Export the Topology Layout



CHAPTER 7

Design Network Hierarchy and Settings

- [Design a New Network Infrastructure, on page 91](#)
- [About Network Hierarchy, on page 92](#)
- [Monitor Floor Map, on page 97](#)
- [Edit Floor Elements and Overlays, on page 100](#)
- [Floor View Options, on page 109](#)
- [Data Filtering, on page 112](#)
- [Configure Global Wireless Settings, on page 113](#)
- [Create Network Profiles, on page 123](#)
- [About Global Network Settings, on page 125](#)
- [About Device Credentials, on page 125](#)
- [Configure Global Device Credentials, on page 128](#)
- [Configure IP Address Pools, on page 133](#)
- [Import IP Address Pools, on page 133](#)
- [Configure Service Provider Profiles, on page 134](#)
- [Configure Global Network Servers, on page 134](#)
- [Configure Cisco WLC High Availability from Cisco DNA Center, on page 136](#)

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 92](#).
- Step 2** Define global network settings. See [About Global Network Settings, on page 125](#).
- 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. By default, there is one site called **Global**.

- **Areas** or **Sites** do not have a physical address (for example, 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.
- **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.
- **Floors** are within the building which comprises of cubicles, walled offices, wired closet, and so on. You can add floors only to buildings.

You can:

- Create a new network hierarchy. See [Create Sites in the Network Hierarchy](#), on page 92.
- Upload an existing network hierarchy from Cisco Prime Infrastructure. See [Upload Existing Site Hierarchy](#), on page 93.

Guidelines for Preparing Image Files to Use Within Maps

- Use any graphical application that saves to the raster image file formats such as: .jpg, .gif, .png, .dxf, and .dwg.
- Ensure that the dimension of the image is larger than the combined dimension of all buildings and outside areas that you plan to add to the campus map.
- Map image files can be of any size. Cisco DNA Center imports the original image to its database at a full definition, but during display, it automatically resizes them to fit the workspace.
- Gather the horizontal and vertical dimensions of the site in feet or meters before importing. This helps you to specify these dimensions during the map import.

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 more 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 > Network Hierarchy**. A world map is displayed.
- Step 2** On the **Network Hierarchy** page, click **+ Add Site** or click the gear icon  next to the parent site in the left tree pane, and then select the appropriate option.
- Step 3** You can also upload an existing hierarchy. See [Upload Existing Site Hierarchy, on page 93](#).
- Step 4** Enter a name for the site and select a parent node. By default, **Global** is the Parent Node.
- Step 5** Click **Add**. The site is created under the parent node in the left menu.
-

Upload Existing Site Hierarchy

You can upload a CSV file or a map archive 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 Maps Archive, on page 93](#) for information about how to export maps from Prime Infrastructure.

Procedure

-
- Step 1** Choose **Design > Network Hierarchy**, then click **Import > Import Sites**.
- Step 2** Drag and drop your CSV file, or navigate to where your CSV file is located, then click **Import** to import the Prime Infrastructure Groups CSV file. If you do not have an existing CSV file, click **Download Template** to download a CSV file you can edit and then upload.
- Step 3** To import the Prime Infrastructure maps tar.gz archive file, click **Import > Map Import**.
- Drag and drop the map archive file into the boxed area in the **Import Site Hierarchy Archive** dialog box, or click the **click to select** link and browse to the archive file.
 - Click **Save** to upload the file. The **Import Preview** page appears, which shows the imported file.
-

Export Maps Archive

Procedure

-
- Step 1** On the Prime Infrastructure UI, choose **Maps > Wireless Maps > Site Maps (New)** to navigate to this page.
- Step 2** From the **Export** drop-down list, choose **Map Archive**.
- Step 3** The **Export Map Archive** wizard opens.
- Step 4** On the **Select Sites** page, configure the following. You can either select map information or calibration information to be included in the maps archive.
- Map Information**—Turn the **On or Off** toggles to include map information in the archive.
 - Calibration Information**—To export calibration information, turn the **On or Off** toggles. You can either select the **Calibration Information for selected maps** or **All Calibration Information** radio button. If you select **Calibration Information for selected maps**, then the calibration information for the selected site maps is exported. If you select **All Calibration Information**, then the calibration

Search the Network Hierarchy

information for the selected map along with additional calibration information that is available in the system is also exported.

- In the **Sites** left sidebar menu, check one or more check boxes of the site, campus, building floor, or outdoor area that you want to export. Check the **Select All** check box to export all the maps.

Step 5 Select the **Generate Map Archive**. A message saying "Exporting data is in progress" is displayed. A tar file is created and is saved onto your local machine.

Step 6 Click **Done**.

Search the Network Hierarchy

You can search the network hierarchy to quickly find a site, building, or area. This is particularly helpful after you have added many sites, areas, or buildings.

Procedure

To search the tree hierarchy, place your cursor in the **Find Hierarchy** field and enter the text on which you want to search. The tree is filtered on the information you enter in the search window.

Edit Sites

Procedure

Step 1 Choose **Design > Network Hierarchy**.

Step 2 In the left tree pane, navigate to the site that you want to edit.

Step 3 Click the gear icon  next to the site and select **Edit Site**.

Step 4 Make the necessary changes, and click **Update**.

Delete Sites

Procedure

Step 1 Choose **Design > Network Hierarchy**.

Step 2 In the left tree pane, navigate to the site that you want to delete.

Step 3 Click the gear icon  next to the site and select **Delete Site**.

Step 4 Confirm the deletion.

Add Buildings

Procedure

-
- Step 1** Choose **Design > Network Hierarchy**. A world map is displayed.
- Step 2** On the **Network Hierarchy** page, click **+ Add Site** or click the gear icon  next to the parent site in the left tree pane and select **Add Building**.
- Step 3** You can also upload an existing hierarchy. See [Upload Existing Site Hierarchy, on page 93](#).
- Step 4** Enter a name for the building.
- Step 5** Enter an address in the **Address** text box. If you are connected to the Internet, as you enter the address, the Design Application narrows down the known addresses to the one you enter. When you see that the correct address appears 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 building you created is added under the parent site in the left tree menu.
- 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.
-

Edit a Building

Procedure

-
- Step 1** Choose **Design > Network Hierarchy**.
- Step 2** In the left tree pane, navigate to the building that you want to edit.
- Step 3** Click the gear icon  next to the building and select **Edit Building**.
- Step 4** Make the necessary changes in the **Edit Building** window, and click **Update**.
-

Delete Buildings

Procedure

-
- Step 1** Choose **Design > Network Hierarchy**.
- Step 2** In the left tree pane, navigate to the building that you want to delete.
- Step 3** Click the gear icon  next to the building and select **Delete Building**.
- Step 4** Confirm the deletion.

Note Deleting a building deletes all its container maps. APs from the deleted maps are moved to unassigned state.

Add Floors to Buildings

After you add a building, 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** Enter a name for the floor. The floor name 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 (.)
 - Spaces ()
- Step 5** Define the type of floor by selecting the Radio Frequency (RF) model from the **Type (RF Model)** drop-down list: **Indoor High Ceiling**, **Outdoor Open Space**, **Drywall Office Only**, and **Cubes And Walled Offices**. This defines if the floor is an open space or a drywall office, and so on. Based on the RF model selected, the wireless signal strength and the distribution of heatmap is calculated.
- Step 6** You can 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 import a map, make sure that you mark the Overlay Visibility as **On (Floor > View Option > Overlays)**. By default, overlays are not displayed after you import a map.

Figure 5: Example Floor Plan

Step 7 Click Add.

Edit Floors

After you add a floor, you can edit the floor map so that it contains 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** text box.

Step 3 Make necessary changes in the **Edit Floor** pop-up window, and click **Update**.

Monitor Floor Map

- Use the **Find** feature located at the right corner of the page to find specific floor elements like APs, sensors, and clients, and so on. The elements that match the search criteria are displayed on the floor map along with a table in the right pane. When you hover your mouse over the table, it points to the search element on the floor map with a connecting line.



- Click the icon at the right corner of the page to:

- Export floor plan as a PDF.
- Measure distance on the floor map.
- Set scale to modify the floor dimensions.



- Click the icon in the right bottom of the page to zoom in on a location. The zooming levels depend upon the resolution of an image. A high-resolution image may provide more zoom levels. Each zoom level is made of a different style map shown at different scales, each one showing more, or less detail. Some maps are of the same style but at a smaller or larger scale.



- Click the icon to see a map with fewer details.



- Click the icon to view the map icon legend.

Table 39: Map Icons

Icon	Description
Icons	
AP Mode	
L	Local
F	FlexConnect
B	Bridge
Health Score	
	Good Health
	Fair Health
	Poor Health
AP Status	
	Not covered by sensor
	Covered by sensor

Icon	Description
	Issue indicator
Radio Band or Mode	
5	802.11 a/n/ac (5GHZ)
2.4	802.11 b/g/n (2.4GHZ)
n	802.11 a/b/g/n (2.4GHZ)
Se	Sensor
M	Monitor 5 GHz
m	Monitor 2.4 GHz
Mx	Monitor XOR Mode
R	Rogue Detector
...	Other
Radio Status	
5	Ok
5	Minor Fault
5	Down
---	Admin Disable
Icons	
	Access Points
	Sensor
	Markers
Rx Neighbors Line	
---	2.4 GHz
—	5 GHz

Edit Floor Elements and Overlays

With the **Edit** option available on the floor area, you can:

- Add, position, and delete the following floor elements:
 - Access Points
 - Sensors
- Add, edit, and delete the following overlay objects:
 - Coverage Areas
 - Obstacles
 - Location Regions
 - Rails
 - Markers

Guidelines for Placing Access Points

You can follow these guidelines while placing access points on the floor map:

- Place access points along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. Access points placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other APs.
- Location accuracy can be improved by increasing overall AP density and moving APs close to the perimeter of the coverage area.
- In long and narrow coverage areas, avoid placing APs in a straight line. Stagger them so that each AP is more likely to provide a unique snapshot of the device location.
- Although the design provides enough AP density for high-bandwidth applications, location suffers because each AP view of a single device is not varied enough. Hence, location is difficult to determine. Move the APs to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy.

Add, Position, and Delete APs



- Note** Make sure you have Cisco APs in your inventory. If not, then discover APs using the Discovery function. See [About Discovery, on page 7](#).

Procedure

- Step 1** Choose **Design > Network Hierarchy**.
- Step 2** In the left tree view menu, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Floor Elements** panel, next to **Access Points**, click **Add**.
Access points that are not assigned to any floors appear in the list.
- On the **Add APs** page, select check boxes of the access points to bulk select APs, and click **Add Selected** or, click **Add** on the AP row to add the access point.
 - You can search for access points using the search option available. Use the **Filter** to search for access points using the AP name, MAC address, model, or controller. The search is case-insensitive. The search result appears in a table. Click **Add** to add the APs to the floor area.
- Step 5** Close the **Add APs** window after assigning access points to the floor area.
- Step 6** Newly added APs appear on the top-right corner of the floor map. You must position them correctly.
- Step 7** In the **Floor Elements** pane, next to Access Points, click **Position** to place them correctly on the map.
- To position, click the access point and drag and drop it to the appropriate location on the floor map or you can update the x and y coordinates and AP Height in the **Selected AP Details** page. When you drag an access point on the map, its horizontal (x) and vertical (y) position appears in the text box. When selected, the access point details are displayed in the right pane. The **Selected AP Details** page shows the following:
 - **Position by 3 points**—You can draw three points on the floor map and position AP using the points created. To do this:
 - Click **Position by 3 points**.
 - To define the points, click anywhere on the floor map to start drawing the first point. Click again to finish drawing a point. A pop-up appears to set the distance to first point. Enter the distance in meters and click **Set Distance**.
 - Define the second and third points in the similar way and click **Save**.
 - **Position by 2 Walls**—You can define two walls on the floor map and position AP between the defined walls. This helps you to know the position of AP between the two walls. This helps you to understand the AP position between the walls.
 - Click **Position by 2 walls**.
 - To define the first wall, click anywhere on the floor map to start drawing the line. Click again to finish drawing a line. A pop-up appears to set the distance to first wall. Enter the distance in meters and click **Set Distance**.
 - Define the second wall in the similar way and click **Save**.
- The AP is placed automatically as per the defined distance between the walls.
- **AP Name**—Shows the AP Name.
 - **AP Model**—Indicates the AP model for the selected access point.

- **MAC Address**—Displays the MAC address.
- **x**—Enter the horizontal span of the map in feet.
- **y**—Enter the vertical span of the map in feet.
- **AP Height**—Enter the height of the access point.
- **Protocol**—Protocol for this access point: 802.11a/n/ac, 802.11b/g/n (for Hyper Location APs), or 802.11a/b/g/n.
- **Antenna**—Antenna type for this access point.
- **Antenna Image**—Shows the AP image.
- **Antenna Orientation**—Depending on the antenna type, enter the Azimuth and the Elevation orientations in degrees.
- **Azimuth**—This option does not appear for Omnidirectional antennas because their pattern is nondirectional in azimuth.

Step 8 When you have completed placing and adjusting access points, click **Save**.

Clicking **Save** causes the antenna gain on the access point to correspond to the selected antenna. This causes radio to reset.

Heatmap is generated based on the new position of the AP.

Step 9 In the **Floor Elements** panel, next to **Access Points**, click **Delete**.

The **Delete APs** page appears which lists all the assigned and places access points.

- Select check boxes of the access points that you want to delete, and click **Delete Selected**.
- To delete all access points, click **Select All**, and click **Delete Selected**.
- To delete an access point from the floor, click the **Delete** icon.
- Use **Quick Filter** and search using the AP name, MAC address, Model, or Controller. The search is case-insensitive. The search result appears in the table. Click the **Delete** icon to delete from the floor area.

Quick View of APs

Hover your mouse cursor over the AP icon on the floor map to view AP details, Rx Neighbors information, clients information, and device 360 view information.

- Select **Info** to view the following AP details:
 - **Associated**—Indicates whether the AP is associated or not.
 - **Name**—AP Name.
 - **MAC Address**—MAC address of the access point.
 - **Model**—AP Model number.
 - **Admin/Mode**—Administration status of the AP mode.

- **Type**—Radio type.
 - **OP./Admin**—Operational status and the AP mode.
 - **Channel**—Channel number of the access point.
 - **Antenna**—Antenna name.
 - **Azimuth**—Direction of the antenna.
- Select the **Rx Neighbors** radio button to view the immediate Rx neighbors for the selected AP on the map with a connecting line. It also shows whether the AP is associated or not along with the AP name.
 - Click **Device 360** to get a 360° view of a specific network element (router, switch, access point, or Cisco WLC). See [Monitor and Troubleshoot the Health of a Device, on page 252](#). For Device 360 to open, you must have the Assurance application installed.

Add, Position, and Delete Sensors



Note Make sure you have Cisco AP 1800S in your inventory. The AP 1800S sensor needs to be provisioned using PnP for it to show up in the Inventory. See [Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 289](#).

The following modes of sensors are available:

- Dedicated Sensor—An AP is converted into a sensor, and it stays in sensor mode (does not serve clients) unless it is manually converted back into AP mode.



Note Sensor Device—A dedicated AP 1800S sensor. The AP 1800S sensor gets bootstrapped using Plug and Play (PnP). After it obtains Assurance server reachability details, it directly communicates with the Assurance server.

- On-Demand Sensor—An AP is temporarily converted into a sensor to run tests. After the tests complete, the sensor changes back into AP mode.

Procedure

Step 1 Choose **Design > Network Hierarchy**.

Step 2 In the tree view menu, select the floor.

Step 3 Click **Edit**, which is located above the floor plan.

Step 4 In the **Floor Elements** panel, next to **Sensors**, click **Add**.

- On the **Add Sensors** page, select the check boxes of the sensors that you want to add or, click **Add** on the sensors row to add sensors.

Add Coverage Areas

- You can search for sensors using the search option available. Use the **Filter** and search using the Name, MAC address, or Model. The search is case-insensitive. The search result appears in the table. Click **Add** to add sensors to the floor area.

Step 5 Close the **Add Sensors** window after assigning to the floor map.

Step 6 Newly added sensors appear on the top-right corner of the floor map. You must position them correctly.

Step 7 In the **Floor Elements** pane, next to **Sensors**, click **Position** to place them correctly on the map.

Step 8 When you have completed placing and adjusting sensors, click **Save**.

Step 9 In the **Floor Elements** panel, next to **Sensors**, click **Delete**.

The **Delete Sensors** page appears which lists all the assigned and placed sensors.

- Select the check boxes of the sensors that you want to delete, and click **Delete Selected**.
- To delete all sensors, click **Select All**, and click **Delete Selected**.
- To delete a sensor from the floor, click the **Delete** icon.
- Use **Quick Filter** and search using the Name, MAC address, or Model. The search is case-insensitive. The search result appears in the table. Click the **Delete** icon to delete from the floor area.

Add Coverage Areas

Any floor area or outside area defined as part of a building map is by default considered as a wireless coverage area.

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a coverage area or a polygon-shaped area.

Procedure

Step 1 Choose **Design > Network Hierarchy**.

Step 2 In the tree view menu, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Coverage Areas**, click **Add**.

Coverage creation pop-up appears.

Step 5 To draw a coverage area, from the **Type** drop-down list, select **Coverage Area**.

- Enter the name of the area you are defining, and click **Add Coverage**. The coverage area must be a polygon with at least 3 vertices.

- Move the drawing tool to the area you want to outline.

- Click the left mouse button to begin and end drawing a line.

- When you have outlined the area, double-click the left mouse button and the area is highlighted on the page.

The outlined area must be a closed object to appear highlighted on the map.

- Click **Save** to save the newly drawn area.

- Step 6** To draw a polygon-shaped area, from the **Type** drop-down list, choose **Perimeter**.
- Enter the name of the area you are defining, and click **Ok**.
 - Move the drawing tool to the area you want to outline.
 - Click the left mouse button to begin and end drawing a line.
 - When you have outlined the area, double-click the left mouse button and the area is highlighted on the page.
- Step 7** To edit a coverage area, in the **Overlays** panel, next to **Coverage Areas**, click **Edit**.
- The available coverage areas are highlighted on the map.
 - Make the changes and click **Save** after the changes.
- Step 8** To delete a coverage area, in the **Overlays** panel, next to **Coverage Areas**, click **Delete**.
- The available coverage areas are highlighted on the map.
 - Hover your mouse cursor on the coverage area and click to delete.
 - Click **Save** after the deletion.

Create Obstacles

You can create obstacles so that they can be considered while computing RF prediction heatmaps for access points.

Procedure

- Step 1** Choose **Design > Network Hierarchy**.
- Step 2** In the tree view menu, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Overlays** panel, next to **Obstacles**, click **Add**.
- Step 5** In the **Obstacle Creation** pop-up window, select an obstacle type from the **Obstacle Type** drop-down list. The type of obstacles you can create are: **Thick Wall**, **Light Wall**, **Heavy Door**, **Light Door**, **Cubicle**, and **Glass**.
The estimated signal loss for the obstacle type you selected is automatically populated. The signal loss is used to calculate RF signal strength near these objects.
- Step 6** Click **Add Obstacle**.
- Step 7** Move the drawing tool to the area where you want to create an obstacle.
- Click the left mouse button to begin and end drawing a line.
 - When you have outlined the area, double-click the left mouse button and the area is highlighted on the page.
 - Click **Done** in the **Obstacle Creation** window that appears.

- The outlined area must be a closed object to appear highlighted on the map.
- Click **Save** to save the obstacle on the floor map.

Step 8 To edit an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Edit**.

- All the available obstacles are highlighted on the map.
- Click **Save** after the changes.

Step 9 To delete an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Delete**.

- All the available obstacles are highlighted on the map.
 - Hover your mouse cursor on the obstacle and click to delete.
 - Click **Save** after the deletion.
-

Location Region Creation

You can create inclusion and exclusion area to further refine location calculations on a floor. You can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas). For example, you might want to exclude areas such as an atrium or stairwell within a building but include a work area (such as cubicles, labs, or manufacturing floors).

Guidelines for Placing Inclusion and Exclusion Areas on a Floor Map

- Inclusion and exclusion areas can be any polygon shape and must have at least three points.
- You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor area when it is created. The inclusion region is indicated by a solid aqua line, and generally outlines the entire floor area.
- You can define multiple exclusion regions on a floor area.

Define Inclusion Region on a Floor

Area within a floor or outside area map where wireless coverage data, such as signal strength, is either mapped (included) or ignored (excluded).

Procedure

Step 1 Choose **Design > Network Hierarchy**.

Step 2 In the tree view menu, select the floor.

Step 3 In the **Overlays** panel, next to **Location Regions**, click **Add**.

Step 4 In the **Location Region Creation** pop-up window, select **Inclusion Type** from the drop-down list.

Step 5 Click **Add Location Region**. A drawing icon appears to outline the inclusion area.

Step 6 To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

Step 7 Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.

- Step 8** Repeat Step 8 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.
- Step 9** Choose **Save** to save the inclusion region.

Define Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

Procedure

- Step 1** Choose **Design > Network Hierarchy**.
- Step 2** In the tree view menu, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Overlays** panel, next to **Location Regions**, click **Add**.
- Step 5** In the **Location Region Creation** window, select **Exclusion Type** drop-down list.
- Step 6** Click **Location Region**. A drawing icon appears to outline the exclusion area.
- Step 7** To begin defining exclusion area, move the drawing icon to a starting point on the map and click once.
- Step 8** Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.
- Step 9** Repeat Step 8 until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is fully defined. The excluded area is shaded in purple.
- Step 10** To define more exclusion regions, repeat Step 5 to Step 9.
- Step 11** When all exclusion areas are defined, choose **Save** to save the exclusion region.
-

Edit Location Regions

Procedure

In the **Overlays** panel, next to **Location Regions**, click **Edit**.

- The available location regions are highlighted on the map.
 - Make changes, and click **Save**.
-

Delete Location Regions

Procedure

In the **Overlays** panel, next to **Location Regions**, click **Delete**.

- The available location regions are highlighted on the map.
- Hover your mouse cursor on the location region you want to delete, and click to delete.
- Click **Save**.

Rail Creation

You can define a rail line on a floor that represents a conveyor belt. Also, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or outside of the snap-width area (minority).

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

Procedure

Step 1 Choose **Design > Network Hierarchy**.

Step 2 In the tree view menu, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Rails**, click **Add**.

Step 5 Enter a snap-width (feet or meters) for the rail and then click **Add Rail**. A drawing icon appears.

Step 6 Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 7 Click the drawing icon twice when the rail line is drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

Step 8 Click **Save**.

Step 9 In the **Overlays** panel, next to **Rails**, click **Edit**.

- The available rails are highlighted on the map.
- Make changes, and click **Save**.

Step 10 In the **Overlays** panel, next to **Rails**, click **Delete**.

- All the available rail lines are highlighted on the map.
- Hover your mouse cursor on the rail line you want to delete, and click to delete.

Step 11 Click **Save** after the deletion.

Place Markers

Procedure

- Step 1** Choose **Design > Network Hierarchy**.
 - Step 2** In the tree view menu, select the floor.
 - Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
 - Step 4** In the **Overlays** panel, next to **Markers**, click **Add**.
 - Step 5** Enter the name for the markers, and then click **Add Marker**. A drawing icon appears.
 - Step 6** Click the drawing icon and place the marker on the map.
 - Step 7** Click **Save**.
 - Step 8** In the **Overlays** panel, next to **Markers**, click **Edit**.
 - The available markers are highlighted on the map.
 - Make changes, and click **Save**.
 - Step 9** In the **Overlays** panel, next to **Markers**, click **Delete**.
 - All the available markers are highlighted on the map.
 - Hover your mouse cursor on the marker you want to delete, and click to delete.
 - Step 10** Click **Save** after the deletion.
-

Floor View Options

Click **View Options**, which is located above the floor plan in the middle pane. The floor map along with these panels appear in the right pane: **Access Points**, **Sensor**, **Overlay Objects**, **Map Properties**, and **Global Map Properties**.

You can modify the appearance of the floor map by selecting or unselecting various parameters. For example, if you want to view only the access point information on the floor map, check the **Access Point** check box. You can expand each panel to configure various settings available for each floor element.

View Options for Access Points

Click the **On/Off** toggle next to **Access Points** to view access points on the map. Expand the **Access Points** panel to configure these settings:

- **Display Label**—From the drop-down list, choose a text label you want to view on the floor map for the access point. The available display labels are:
 - **None**—No labels are displayed for the selected access point.
 - **Name**—AP name.
 - **AP MAC Address**—AP MAC address.
 - **Controller IP**—IP address of Cisco WLC to which the access point is connected.

- **Radio MAC Address**—Radio MAC address.
- **IP Address**
- **Channel**—Cisco Radio channel number or Unavailable (if the access point is not connected).
- **Coverage Holes**—Percentage of clients whose signal has become weaker until the client lost its connection. It shows **Unavailable** for access points that are not connected and **MonitorOnly** for access points that are in monitor-only mode.
- **TX Power**—Current Cisco Radio transmit power level (with 1 being high) or Unavailable (if the access point is not connected). If you change the radio band, the information on the map changes accordingly.

The power levels differ depending on the type of access point. The 1000 series access points accept a value between 1 and 5, the 1230 access points accept a value between 1 and 7, and the 1240 and 1100 series access points accept a value between 1 and 8.

- **Channel and Tx Power**—Channel and transmit power level (or Unavailable if the access point is not connected).
- **Utilization**—Percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays **Unavailable** for disassociated access points and **MonitorOnly** for access points in monitor-only mode.
- **Tx Utilization**—Transmitted (Tx) utilization for the specified interface.
- **Rx Utilization**—Received (Rx) utilization for the specified interface.
- **Ch Utilization**—Channel utilization for the specified access point.
- **Assoc. Clients**—Total number of clients associated.
- **Dual-Band Radios**—Identifies and marks the XOR dual-band radios on the Cisco Aironet 2800 and 3800 Series Access Points.
- **Health Score**—AP health score.
- **Issue Count**
- **Coverage Issues**
- **AP Down Issues**
- **Heatmap Type**—Heatmap is a graphical representation of Radio Frequency (RF) wireless data where the values taken by variable are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, antenna orientation, and AP transmit power. From the **Heatmap Type** drop-down list, select the heatmap type: **None**, or **Coverage**.
 - **None**
 - **Coverage**—If you have monitor mode access points on the floor plan, you can select coverage heatmap. A coverage heatmap excludes monitor mode access points.
- **Heatmap Opacity (%)**—Drag the slider between 0 to 100 to set the heatmap opacity.
- **RSSI Cut off (dBm)**—Drag the slider to set the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.

- **Map Opacity (%)**—Drag the slider to set the map opacity.

The AP details are reflected on the map immediately. Hover your mouse cursor over the AP icon on the map to view AP details and RX neighbor information.

View Options for Sensors

Click the **Sensors** toggle button to view sensors on the map. Expand the **Sensors** panel to configure these settings:

- **Display Label**—From the drop-down list, choose a text label you want to view on the floor map for the selected access point. The available display labels are:
 - **None**
 - **Name**—Sensors name.
 - **Sensor MAC Address**—Sensors MAC address.
 - **IP Address**—IP address of Cisco WLC to which the sensor is connected.

View Options for Overlay Objects

Expand the **Overlay Objects** panel to configure these settings. Use the **On/Off** toggles to view these overlay objects on the map.

- **Coverage Areas**
- **Location Regions**
- **Obstacles**
- **Rails**
- **Markers**

Configure Map Properties

Expand the **Map Properties** panel to configure:

- **Auto Refresh**—Provides an interval drop-down list to set how often you want to refresh maps data from the database. From the **Auto Refresh** drop-down list, set the time intervals: **None**, **1 min**, **2 mins**, **5 mins**, or **15 mins**.

Configure Global Maps Properties

Expand the **Global Map Properties** panel to configure:

- **Unit of Measure**—From the drop-down list, set the dimension measurements for maps to either **Feet** or **Meters**.

Data Filtering

Filtering Access Points Data

Click **Access Point** under the **Filters** panel in the right pane. The filtering options for access points include the following:

- Choose the radio type from the drop-down list, located above the floor map in the middle pane: **2.4 GHz**, **5 GHz**, or **2.4 GHz & 5 GHz**.
- Click **+ Add Rule** to add a query:
 - Choose the access point identifier you want to view on the map: Name, MAC Address, Tx Power, Channel, Avg Air Quality, Min. Air Quality, Controller IP, Coverage Holes, Tx Utilization, Rx Utilization, Profiles, CleanAir Status, Associated Clients, Dual-Band Radios, Radio, or Bridge Group Name.
 - Choose the parameter by which you want to filter access points.
 - Enter the specific filter criteria in the text box for the applicable parameters, and click **Go**. The search results appear in a tabular format.
 - Click **Apply Filters to List** to view the filter results on the map. To view a particular access point on the map, check the check box of the access point in the table that is displayed, and click **Show Selected on Maps**.

When you hover your mouse cursor over the search result in the table, the location of the AP gets pointed with a line on the map.

Filtering Sensors Data

Click **Sensor** under the **Filters** panel in the right pane. The filtering options for sensor include the following:

- Choose the radio type from the drop-down list, located above the floor map in the middle pane: **2.4 GHz**, **5 GHz**, or **2.4 GHz & 5 GHz**.
- Click **+ Add Rule** to add a query:
 - Choose the sensor identifier you want to view on the map: **Name** and **MAC Address**.
 - Choose the parameter by which you want to filter sensors.
 - Enter the specific filter criteria in the text box for the applicable parameters, and click **Go**. The search results appear in a tabular format.
 - Click **Apply Filters to List** to view the filter results on the map. To view a particular access point on the map, check the check box of the access point in the table that is displayed, and click **Show Selected on Maps**.

When you hover your mouse cursor over the search result in the table, the location of the Sensor gets pointed with a line on the map.

Configure Global Wireless Settings

Global wireless network settings include settings for Service Set Identifier (SSID), wireless interfaces, Wireless Radio Frequency (RF), and Sensor Settings.



- Note** Creating wireless interfaces and wireless radio frequency is applicable only for nonfabric deployments. Creating the wireless sensor device profile is applicable only for the AP 1800S sensor device.

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

- [Creating SSIDs for an Enterprise Wireless Network, on page 113](#)
- [Creating SSIDs for a Guest Wireless Network, on page 115](#)
- [Create a Wireless Interface, on page 119](#)
- [Create a Wireless Radio Frequency Profile, on page 120](#)
- [Create a Wireless Sensor Device Profile, on page 122](#)

Creating SSIDs for an Enterprise Wireless Network

The following procedure describes all the steps for deploying SSIDs for an enterprise wireless network.



- Note** All the SSIDs are created at the Global level. The site, building, and the floor will inherit settings from the Global level.

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:

- Enter an SSID name in the **Wireless Network Name (SSID)** field.
- Select the **Type of Enterprise Network: Voice and Data or Data Only**. This selection defines the quality of service (QoS).
- Check the **Fast Lane** check box to enable fastlane capability on this network.
- Click the **BROADCAST SSID** toggle to turn the broadcast SSID on or off. If you turn the broadcast SSID off, the WLAN will not broadcast the SSID.
- Select one of the **Wireless Option**:
 - **Dual band operation (2.4GHz and 5GHz)**—The WLAN is created for both 2.4 and 5GHz. The band select is disabled by default.

- **Dual band operation with band select**—The WLAN is created for 2.4GHz and 5GHz and band select is enabled.
- **5GHz only**—The WLAN is created for 5GHz and band select is disabled.
- Check the **Fast Transition** check box to enable 802.11r protocol. You can select **Enable** or **Disable** mode. By default, it is in **Adaptive** mode.
- 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**, enter the passphrase in the **Passphrase** text box.
 - **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.

Note You can override a preshared key (PSK) at the site, building, or the floor level. If you override a PSK at the building level, the subsequent floor inherits the new settings. For more information, see [Preshared Key Override, on page 115](#).

- **Open**—Provides no security. Allows any device to access the wireless network without any authentication.
- Under Advanced Security Options, configure the following:
 - Check the **MAC Filtering** check box to enable MAC-based access control on an SSID.
 - Set the **Fast Transition (802.11r)** to: **Enable**, **Adaptive**, or **Disable** mode.

Step 3 Click **Next**. The **Wireless Profiles** window is displayed. You can associate this SSID with the corresponding wireless profile.

Step 4 In the **Wireless Profiles** window, click **+Add** to create a new wireless profile.

Step 5 Configure the following in the **Create a Wireless Profile** window:

- 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**. If you select **No**, configure the following parameters:
 - From the **Select Interface** drop-down list, select the interface. This is the VLAN Id that is associated with the wireless interface.
 - Check the **Flex Connect** check box to enable FlexConnect mode. This is Flex Group profile, where the traffic is split locally, except for traffic that has specific rules. Based on the below configurations, the profile is applied to a site and a flex group is created internally.
 - To assign this profile to a site, enter the full or partial name of the site name in the **Site Selector** text box. The available sites are auto populated and you can select the site you want from the drop-down list.

Step 6 Click **Add**. The created profile appears in the **Wireless Profiles** page.

Step 7 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. For more information, see [Discover Your Network Using CDP, on page 11](#) and [Discover Your Network Using an IP Address Range, on page 16](#).
2. Automatically add and onboard new devices with Network Plug and Play.
3. Configure policies for your network. For more information, see [Configure Policies, on page 157](#).
4. Add Cisco WLC to a site. For more information, see [Add Devices to Sites, on page 211](#).
5. Provisioning Cisco WLCs and Cisco APs. For more information, see [Provision a Cisco WLC, on page 212](#) and [Provision a Cisco AP—Day 1 AP Provisioning, on page 215](#).
6. Add Cisco WLC to a fabric domain. For more information, see [Add Devices to a Fabric, on page 224](#).
7. Configure settings for the various kinds of devices ("hosts") that can access the fabric domain, see [Configure Host Onboarding](#).

Preshared Key Override

The SSIDs are created at the Global hierarchy. The site, building, and the floor inherits settings from the Global hierarchy. You can override a preshared key (PSK) at the site, building, or the floor level. If you override a PSK at the building level, the subsequent floor inherits the new settings.

Procedure

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

Step 2 In the tree menu, select the site, building, or floor to edit the PSK.

Step 3 Under **Enterprise Wireless**, click the **Passphrase** textbox, and enter a new passphrase for the PSK SSID.

Step 4 Click **Save**.

A success message saying "Passphrase for the SSID(s) are updated successfully" is displayed.

Click the Inherit icon next to the SSID to view origin of the settings.

Creating SSIDs for a Guest Wireless Network

This procedure shows how to:

1. Create SSIDs.
2. Create wireless network 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**.

Note For an External Web Authentication (EWA), select **Web Auth** as the **Level of Security** and **External Authentication** as the **Authentication Server**.

Note For a Central Web Authentication (CWA), select **Web Auth** as the **Level of Security** and **ISE Authentication** as the **Authentication Server**.

- **WEB AUTH**—Provides higher level of layer 3 security.
- **Open**—Provides no security. Allows devices to connect to the wireless network without any authentication.

Step 5 If you select **Web Auth**, you must configure the authentication server: **ISE Authentication** or **External Authentication**.

- For **External Authentication**, enter the redirect URL in the **Web Auth URL** text box. For a
- 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. 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 4 to associate an SSID with the existing wireless profile, and 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 not by selecting the **Yes** or **No** radio button next to **Fabric**.
- If you select **No**, configure the following:
- If you want the guest SSID to be a guest anchor, select **Yes** or **No** radio button next to **Do you need a Guest Anchor for this guest SSID**. Select **Yes** for guest anchor configuration.
 - If you select **No**, check the **Flex Connect Local Switching** check box to enable FlexConnect mode. The selection of FlexConnect switches the traffic locally. Based on your configuration, the profile is applied to a site and a flex group is created internally.
 - From the **Select Interface** drop-down list, select the interface or click **+ create a new wireless interface**. This is the VLAN Id that is associated with the wireless interface.
 - To assign this profile to a site, enter the full or partial name of the site name in the **Site Selector** text box. The available sites are auto populated and you can select the site you want from the drop-down list.
 - Click **Save**. The created profile appears on the **Wireless Profiles** page.
- Step 9** To associate the SSID to a wireless profile, do the following:
- On the **Wireless Profiles** page, check the **Profile Name** check boxes 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 on 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. For more information, see [Discover Your Network Using CDP, on page 11](#) and [Discover Your Network Using an IP Address Range, on page 16](#).
 2. Automatically add and onboard new devices with Network Plug and Play. For more information, see [About Network Plug and Play, on page 33](#).
 3. Configure policies for your network. For more information, see [Configure Policies, on page 157](#).

4. Add Cisco WLC to a site. For more information, see [Add Devices to Sites, on page 211](#).
5. Provisioning Cisco WLCs and Cisco APs. For more information, see [Provision a Cisco WLC, on page 212](#) and [Provision a Cisco AP—Day 1 AP Provisioning, on page 215](#).
6. Add Cisco WLC to a fabric domain. For more information, see [Add Devices to a Fabric, on page 224](#).
7. 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 Use the **On/Off** toggle button to select the radio band: **2.4 GHz** or **5 GHz**. If you have disabled one of the radios, the base radio of the AP that you are going to configure this AP profile into will be disabled.

Step 5 Configure the following for **2.4 GHz** radio type:

- Select one of the **Parent Profile** types: **High**, **Medium (Typical)**, **Low**, and **Custom**. The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates profile configurations available in the device for 2.4 GHz. If you change any settings in the populated **Data Rate** and **Tx Configuration**, the **Parent Profile** automatically changes to **Custom**. A new RF Profile is created only for the select custom profile.

Note Low, Medium (Typical), and High are the pre-canned RF profiles. If you select any of the pre-canned RF profiles, the respective RF profiles which are there in the device is used and the new RF profile is not be created on the DNA Center.

- **DCA Channel**—DynamicChannel Assignment (DCA) dynamically manages channel assignment for an RF group and evaluates the assignments on a per AP radio basis.

- Check the **Select All** check box to select DCA channels **1**, **6**, and **11**, or check the check box of the individual channel numbers.

- Click **Show Advanced** to select the DNA channel numbers under the **Advanced Options**. Check the **Select All** check box to select DCA channels that are under advanced options or check the check box of the individual channel numbers. The channel numbers available for B profile: **2**, **3**, **4**, **5**, **7**, **8**, **9**, **10**, **12**, **13**, and **14**.

Note You need to configure these channels globally on Cisco WLC.

- Use the **Data Rate** slider to set the rates at which data can be transmitted between the access point and the client. The available data rates are: **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.

- **Tx Power Configuration**

- **Power Level**—To determine whether the power of an AP needs to be adjusted down. Reducing the power of an AP helps mitigate co-channel interference with another AP on same channel or close proximity. Use the **Power Level** slider to set the minimum or maximum power level. The range is -10dBm to 30dBm and the default is -10dBm.
- **Power Threshold**—It is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP or not. Use the **Power Threshold** slider to increase or decrease the power value which causes the AP to operate at higher or lower transmit power rates. The range is from -50dBm to -80dBm and the default threshold is -70dBm.
- RX SOP—Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. From the RX SOP drop-down list, select the **High**, **Medium**, **Low**, and **Auto** RX SOP threshold values for each 802.11 band.

Step 6 Configure the following for **5 GHz** radio type:

- Select one of the **Parent Profile** types: **High**, **Medium (Typical)**, **Low**, and **Custom**. The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates configurations available in the device for 2.4 GHz. If you change any settings in the populated **Data Rate** and **Tx Configuration**, the **Parent Profile** automatically changes to **Custom**. A new RF Profile is created only for select custom profile.

Note Low, Medium (Typical), and High are the pre-canned RF profiles. If you select any of the pre-canned RF profiles, the respective RF profiles which are already there in the device is used and the new RF profile is not be created on the DNA Center.

- Choose one of the channel bandwidth options from the **Channel Width** drop-down list: **Best**, **20 MHz**, **40 MHz**, **80 MHz**, or **160 MHz**, or **Best**.

- Set the **DCA Channel** to manage channel assignments:

Note You need to configure the DNA channels globally on Cisco WLC.

- **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 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.

- Use the **Data Rate** slider to set the rates at which data can be transmitted between the access point and the client. The available data rates are: **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

- **Tx Power Configuration**

- **Power Level**—To determine whether the power of an AP needs to be adjusted down. Reducing the power of an AP helps mitigate co-channel interference with another AP on same channel or close proximity. Use the **Power Level** slider to set the minimum or maximum power level. The range is -10dBm to 30dBm and the default is -10dBm.

Create a Wireless Sensor Device Profile

proximity. Use the **Power Level** slider to set the minimum or maximum power level. The range is -10dBm to 30dBm and the default is -10dBm.

- **Power Threshold**—It is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP or not. Use the **Power Threshold** slider to increase or decrease the power value which causes the AP to operate at higher or lower transmit power rates. The range is from -50dBm to -80dBm and the default threshold is -70dBm.
- **RX SOP**—Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. From the RX SOP drop-down list, select the **High**, **Medium**, **Low**, and **Auto** RX SOP threshold values for each 802.11 band.

Step 7 Click **Save**.

The profile created gets listed.

Step 8 To mark a profile as default RF profile, check the **Profile Name** check box and click **Mark Default**.

Step 9 Click **OK** in the **Warning** window that appears.

Create a Wireless Sensor Device Profile

Creating the wireless sensor device profile is applicable for the Cisco Aironet 1800s Active Sensor.

Before you begin

If you are using the Cisco Aironet AP 1800S Sensor without an Ethernet module, you must enable Cisco Provisioning SSID on the WLC. See [Enable Cisco Provisioning SSID on the Cisco WLC](#), on page 290.

Procedure

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

Step 2 Under **Sensor Settings**, click **+Add**.

The **Create Sensor SSID Assignment** window appears. Configure the following parameters:

- In the **Settings Name** field, enter a name for the sensor device profile.
- In the **Wireless Network Name (SSID)** field, enter a name for the SSID.
- In the **Level of Security** area, choose a security level, and then enter the appropriate credentials.

Note To provision the Cisco Aironet 1800s Active Sensor with wired connection, enter any proxy name and SSID (for example wired_xyz), and in the **Level of Security** area, choose **Open**.

Step 3 Click **Save**.

Create Network Profiles

From the DNA Center home page, choose **Design > Network Profiles**. Click  **Add Profile** to create network profiles for:

- Routing and NFV—For more information, see [Create Network Profiles for Routing and NFV, on page 123](#).
- Switching
- Wireless—For more information, see [Creating SSIDs for an Enterprise Wireless Network, on page 113](#), [Creating SSIDs for a Guest Wireless Network, on page 115](#), and [Create and Associate Templates to Wireless Profiles, on page 148](#).

Create Network Profiles for Routing and NFV

This workflow shows hows to:

1. Configure router WAN.
2. Configure router LAN.
3. Configure ENCS integrated switch.
4. Create custom configurations.
5. View profile summary.

Procedure

Step 1 Choose **Design > Network Profiles**.

Step 2 Click **+Add Profiles** and choose **Routing & NFV**.

Step 3 The **Router WAN Configuration** window appears.

- Enter the profile name in the **Name** text box.
- Select the number of **Service Providers** and **Devices** from the drop down list. A maximum of three service providers and two devices are supported per profile.
- Select the **Service Provider Profile** from the drop down list. For more information, see [Configure Service Provider Profiles, on page 134](#).
- Select the **Device Family** from the drop down list.
- Enter a unique string in the **Device Tag** to identify the different devices.
- To enable at least one line link for each device to proceed click on **O** and check the check box next to **Connect**. Select the **Line Type** from the drop down list. Click **OK**.
- Click **+Add Services** to add services to the profile. The **Add Services** window appears. Check the check box next to **ISRV vEdge**, **WAN Optimizer**, or **Firewall**. You can also select **+Add Custom** to add custom services to the profile.

To configure the ISRv router, select **Profile** from the drop down list. For more information, see [Import Software Images, on page 81](#). Click **Save**.

To configure vEdge, select **Profile** from the drop down list.

To configure WAN optimizer, select **Services** and **Profile** from the drop down lists.

To configure firewall, select **Services**, **Services** and **Mode** from the drop down lists.

To enable Direct Internet Access (DIA), select **Firewall** and check the check box next to **DIA**.

- Click **Next**.

Step 4 The **Router LAN Configuration** page appears.

- Select **L2** or **L3** services.
- If you select **L2**, select the **Type** from the drop down list, enter the **VLAN ID/Allowed VLAN** and the **Description**.
- If you select **L3**, select the **Protocol Routing** from the drop down list and enter the **Protocol Qualifier**.
- Click **Next**.

Step 5 The **ENCS Integrated Switch Configuration** page appears.

- Click **+Add Row**. Select **Type** from the drop down list and enter the **VLAN ID/Allowed VLAN** and the **Description**.
- Click **Next**.

Step 6 The **Custom Configuration** page appears.

The custom configurations are optional. You may skip the step and apply the configurations any time in the Network Profiles.

If you choose to add the custom configurations

- Select the **Template** from the drop down list.
- Click **Next**.

Step 7 The **Summary** page appears.

This page summarizes the router configurations. Based on the devices and services selected, the hardware recommendation is provided in this page.

- Click **Save**.

Step 8 The **Network Profiles** page appears.

Click **Assign Sites** to assign a site to the network profile. For more information, see [Create Sites in the Network Hierarchy, on page 92](#).

What to do next

1. Add Cisco WLC to a site. See [Add Devices to Sites, on page 211](#).
2. Unclaimed Provisioning. See [Network Plug and Play Use Cases, on page 35](#).

About Global Network Settings

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

- **Global settings**—Settings defined here affect your entire network and include settings for servers such as NTP, Syslog, SNMP Trap, NetFlow Collector, and so on, IP address pools, and device credential profiles.
- **Site settings**—Settings define here override global settings and can include settings for servers, IP address pools, and device credential profiles.

**Note**

Certain network settings can be configured on devices automatically using the Device Controllability feature. When DNA Center configures or updates devices, the transactions are captured in the DNA Center audit logs. You can use the audit logs to help you track changes and troubleshoot issues. For more information about Device Controllability and Audit Logs, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

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

- Network servers, such as AAA, DHCP, and DNS—for more information, see [Configure Global Network Servers, on page 134](#).
- Device credentials, such as CLI, SNMP, and HTTP(S)—For more information, see [Configure CLI Credentials, on page 128](#), [Configure SNMPv2c Credentials, on page 129](#), [Configure SNMPv3 Credentials, on page 130](#), and [Configure HTTPS Credentials, on page 132](#).
- IP address pools—for more information, see [Configure IP Address Pools, on page 133](#).
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—for more information, see [Configure Global Wireless Settings, on page 113](#).

About Device Credentials

Device credentials refer to the CLI, SNMP, and HTTPS credentials that are configured on network devices. DNA Center uses these credentials to discover and collect information about 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. 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.

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



Note In DNA Center's implementation, only the username is provided in cleartext.

SNMPv2c Credentials

Simple Network Management Protocol (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.

SNMPv2c is the community string-based administrative framework for SNMPv2. SNMPv2c 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, 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 the security model and level combinations:

Table 40: 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).
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

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

Device credentials refer to the CLI, SNMP, and HTTPS credentials that DNA Center uses to discover and collect information about the devices in your network.

Configure CLI Credentials

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

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 41: 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>
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 **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Update Now** radio button and click **Apply**.

- To schedule the update for a later time, click the **Schedule Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Configure SNMPv2c Credentials

If you are using SNMPv2c credentials to monitor and manage your network devices, define those SNMPv2c values.

Before you begin

You must have your network's SNMP information.

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 Type, click **SNMP v2c** and enter the following information:

Table 42: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description—Name or description of the SNMPv2c 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 SNMPv2c 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 **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

Configure SNMPv3 Credentials

- To update the new credentials now, click the **Update Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Schedule Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

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 your network's SNMP information.

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 Type, click **SNMP v3** and enter the following information:

Table 43: SNMPv3 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. Choose one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv—Does not provide authentication or encryption. • AuthNoPriv—Provides authentication but does not provide encryption. • AuthPriv—Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA—Authentication based on HMAC-SHA. • MD5—Authentication based on HMAC-MD5.

Field	Description
Auth Password	<p>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</p> <p>Note</p> <ul style="list-style-type: none"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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 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"> Some Cisco Wireless Controllers (WLC) require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your WLCs. Failure to ensure these required minimum character lengths for 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.

Step 4 Click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Update Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Schedule Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

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 44: HTTP(S) 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 The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain <> @ ' , : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<p>You can configure up to five HTTPS 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 The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain <> @ ' , : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Step 4 Click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Update Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Schedule Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Configure IP Address Pools

You can manually create IP address pools.

You can also configure DNA Center to communicate with an external IP address manager. For more information, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

You can also reserve IP address pools for sites. See [Provision LAN Underlay, on page 218](#) for more information.

Procedure

Step 1 From the DNA Center home page, choose **Design > Network Settings > IP Address Pools**.

Step 2 Click **Add IP Pool** and complete the required fields. If you have configured DNA Center to communicate with an external IP address manager, you cannot create an IP pool that overlaps an existing IP address pool in the external IP address manager.

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**.

Import IP Address Pools

You can import IP address pools from Bluecat® or Infoblox®.



Note The IP address pools cannot have subpools and cannot have any assigned IP addresses from the IP address pool.

You must configure DNA Center to communicate with an external IP Address Manager. For more information, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

Procedure

-
- Step 1** From the DNA Center home page, choose **Design > Network Settings > IP Address Pools**.
- Step 2** Click **Import** and complete the required fields.
- Step 3** Enter a CIDR and then click **Retrieve** to get the list of IP pools available to import.
- Step 4** Click **Select All** or chose the IP address pools to import, then click **Import**.
-

Configure Service Provider Profiles

You can create a service provider (SP) profile that defines the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class of service models. After you create a SP profile, you can assign it to an application policy and to the WAN interfaces in the application policy scope, including setting the subline rate on the interface, if needed.

Procedure

-
- Step 1** From the DNA Center home page, select **Design > Network Settings > SP Profiles**.
- Step 2** In the **QoS** area, click **Add**.
- Step 3** In the **Profile Name** field, enter a name for the SP profile.
- Step 4** From the **WAN Provider** drop-down list, choose a service provider.
- Step 5** From the **Model** drop-down list, choose one of four class models: **4 class**, **5 class**, **6 class**, and **8 class**.
For a description of these classes, see [Service Provider Profiles, on page 175](#).
-

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** From the DNA Center home page, choose **Design > Network Settings > Network**.
- Step 2** In the **DHCP Server** field, enter the IP address of a DHCP server.
- Note** You must define at least one DHCP server in order to create IP address pools.
- Step 3** In the **DNS Server** field, enter the domain name of a DNS server.

Note You must define at least one DNS server in order to create IP address pools.

- Step 4** (Optional) You can enter Syslog, SNMP Trap, and NetFlow Collector server information. Click **Add Servers** to add an NTP server.
- Step 5** Click **Save**.
-

Add AAA Server

You can specify AAA servers for network and/or endpoint authentication at the site or global level. You can configure Cisco Identity Services Engine (ISE) and non-ISE AAA servers for network authentication with the support for RADIUS or TACACS. For client and endpoint authentication, only ISE with RADIUS protocol is supported. Only one ISE is supported per Cisco DNA Center.

After you configure a Cisco ISE server for a site, the devices that are assigned to the site are automatically updated on the corresponding Cisco ISE server. Subsequently, any changes to those devices in Cisco ISE are sent automatically to DNA Center.

Procedure

- Step 1** From the DNA Center home page, choose **Design > Network Settings > Network**.
- Step 2** Click **Add Servers** to add a AAA server.
- Step 3** In the **Add Servers** window, check the **AAA** check box, and click **OK**.
- Step 4** You can set the AAA server for network users or client/endpoint users or both.
- Step 5** Check the **Network** and/or **Client/Endpoint** check boxes and configure servers and protocols for AAA server.
- Choose the **Servers** for authentication and authorization: **ISE** or **Non-ISE**.
 - If you select **ISE**, configure the following:
 - Note** AAA settings for a physical and managed site for a particular WLC should match, otherwise the provisioning will fail.

From the **Network** drop-down list, select the IP address of the ISE server. The **Network** drop-down list contains all the IP addresses of the Cisco ISE servers that are registered in **System Settings** on the DNA Center **Home** page. Selecting an ISE IP populates primary and additional IP address drop-down lists with Policy Service Nodes (PSN) IP addresses for the selected ISE. You can either enter an IP address for the AAA server or select the PSN IP address from the **IP Address (Primary)** and **IP Address (Additional)** drop-down lists.

- Note** TACACS protocol is supported only for network users. If TACACS is selected for clients/endpoint users, provisioning will fail.

Choose the **Protocol** for AAA server: **RADIUS** or **TACACS**.

- If you select **Non-ISE**, configure the following:
 - You can either enter an IP address for the AAA server or select the IP addresses from the **IP Address (Primary)** and **IP Address (Additional)** drop-down lists. These drop-down lists contain the non-ISE AAA servers registered in **System Settings**.

- Step 6** Click Save.
-

Configure Cisco WLC High Availability from Cisco DNA Center

Cisco WLC High Availability (HA) can be configured through Cisco DNA Center. In Cisco DNA Center Release 1.2, only the formation of Cisco WLC HA is supported; the breaking of HA and switchover options are not supported.

This section contains information about the following topics:

- [Prerequisites for Cisco WLC HA, on page 136](#)
- [Configuring Cisco WLC HA from Cisco DNA Center, on page 136](#)
- [What Happens During or After the High Availability Process is Complete, on page 137](#)
- [Commands to Configure and Verify Cisco WLC HA, on page 138](#)

Prerequisites for Cisco WLC HA

- The discovery and inventory features of Cisco WLC-1 and WLC-2 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.
- The 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. The redundancy management address of WLC-1 and WLC-2 should also be in the same subnet.

Configuring Cisco WLC HA from Cisco DNA Center

To configure Cisco WLC High Availability from the DNA Center, perform the following tasks:

Procedure

- Step 1** From the DNA Center home page, choose **Provision > Devices**.
- Step 2** Click **WLC-1** since this is being configured as primary controller.
- Step 3** Click the **High Availability** tab.
- Step 4** Choose the **Select Secondary WLC** drop-down list.
- Step 5** Enter the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses in the respective text boxes.
- Note** Ensure that these IP addresses are unused IP addresses.
- Step 6** Click **Configure HA**.

The HA configuration is initiated at the background using the CLI commands. First, the primary controller is configured. On success, the secondary controller is configured. After the configuration is complete, both the controllers will reboot. This process may take up to 2.5 minutes to complete.

Step 7 After the HA is initiated, the **Redundancy Summary** under **High Availability** tab displays the **Sync Status** as **In Progress**. When the DNA Center finds that the HA pairing is successful, **Sync Status** becomes **Complete**.

This is triggered by the inventory poller or by manual resynchronization. By now, the secondary controller (WLC-2) gets deleted from the DNA Center. This flow indicates successful HA configuration in Cisco 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 Cisco WLC before adding Cisco WLC to the connectivity domain. Also ensure that the Sync status is **Complete** before adding Cisco WLC to the connectivity domain.

The following is a list of actions that occur after the process is complete:

- Cisco WLC-1 and Cisco WLC-2 are configured with redundancy management, redundancy units, and Single sign-on (SSO). The Cisco WLCs reboot in order to negotiate their role as an active WLC or a standby WLC. Configuration is synchronized from active to standby.
- On the **Show Redundancy Summary** window, you can see these configurations:
 - SSO is Enabled
 - WLC1 is Active state
 - WLC2 is Hot Stand By state
- The active WLC's management port is shared by both the active and standby WLCs and point to the active WLC. GUI, Telnet, and SSH do not work on the standby WLC. You can use the console and service port interface to control the standby WLC.

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 HA

The following are the configuration commands sent from the DNA Center to configure Cisco WLC HA:

These are the commands sent from the DNA Center to the WLC-1:

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

These are the commands sent from the DNA Center to the WLC-2:

- **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**

Use the following commands to verify HA configurations from the Cisco WLCs:

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



CHAPTER 8

Create Templates to Automate Device Configuration Changes

- [About Template Editor, on page 139](#)
- [Create Projects, on page 139](#)
- [Create Templates, on page 140](#)
- [Template Form Editor, on page 146](#)
- [Create and Associate Templates to Wireless Profiles, on page 148](#)

About Template Editor

Cisco DNA Center provides an interactive editor to author CLI templates. Template Editor is a centralized CLI management tool to help design and provision templates in the DNA Center. The template is used to generate a device deployable configuration by replacing the parameterized elements (variables) with actual values and evaluating the control logic statements. With the Template Editor, you can:

- Create, edit, and delete templates
- Add interactive commands
- Validate errors in the template
- Version control templates for tracking purpose
- Simulate the templates

Create Projects

Projects are a logical grouping to a set of templates.

Procedure

- Step 1** From the Cisco DNA Center home page, choose **Tools > Template Editor**.
- Step 2** In the left pane, click > **Create Project**.

Step 3 In the **Add New Project** window that is displayed, enter a name, description, and tags for the project in the respective text boxes.

Step 4 Click **Add** to add the project.

The created project appears in the left pane.

What to do next

1. Create templates. See [Create a Regular Template, on page 140](#).

Create Templates

Cisco DNA Center provides the following types of configuration templates. CLI templates allow you to choose the elements in the configurations. DNA Center provides variables that you can replace with actual values and logic statements.

- Regular templates
- Composite templates

Create a Regular Template

Before you begin

- Design network hierarchy, with sites, buildings, floors, and so on. For more information, see the [Create Sites in the Network Hierarchy, on page 92](#), [Add Buildings, on page 95](#), and [Add Floors to Buildings, on page 96](#).
- Make sure that you have defined the following global network settings before provisioning a Cisco WLC:
 - Network servers, such as AAA, DHCP, and DNS. For more information, see [Configure Global Network Servers, on page 134](#).
 - Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles. For more information, [Creating SSIDs for an Enterprise Wireless Network, on page 113](#) and [Creating SSIDs for a Guest Wireless Network, on page 115](#).
- Make sure that you have Cisco WLC in your inventory. If not, discover Cisco WLC using the Discovery function. For more information, see [About Discovery, on page 7](#).
- Make sure that Cisco WLC is added to a site. For more information, see [Add Devices to Sites, on page 211](#).

Procedure

Step 1 From the Cisco DNA Center home page, choose **Tools > Template Editor**.

- Step 2** In the tree pane, select the project under which you are creating templates, and click the gear icon > **Add Templates** or click > **Add Templates** located at the top of the left pane.
- Step 3** In the **Add New Template** window that is displayed, click the **Regular Template** radio button.
- Step 4** In the **Name** text box, enter a unique name for the template.
- Step 5** In the **Project Name** text box, enter a unique name for the project.
- The text box is enabled if you are navigating from the > **Add Templates** path. The text box is disabled if you select a project, and click the gear icon > **Add Templates** in the tree pane.
- Step 6** In the **Description** text box, enter a description for the template.
- Step 7** In the **Tags** text box, enter an intuitive name to tag the templates . Tagging a configuration template helps you to:
- Search a template using the tag name in the search field.
 - Use the tagged template as a reference to configure more devices.
- Step 8** If you are creating a template that applies only to a particular device type, from the **Device Type** drop-down list, choose the device. The device types are displayed depending on your selection in the in the **Device Type** drop-down list.
- Step 9** From the **Software Type** drop-down list, choose the software type. You can select the specific software type such as IOS-XE, IOS-XR, or NX-OS if there are commands specific to these software types. If you select the software type as IOS, then the commands are applicable to all software types including IOS-XE, IOS-XR, and NX-OS. This is used at the provisioning time to check whether the selected device is conforming to the selection in the template.
- Step 10** In the **Software Version** text box, enter the software version . During the provisioning, DNA Center checks to see if the selected device has the similar software version as mentioned in the template. If there is a mismatch, then the provision skips the template.
- Step 11** Click **Add** to add the template. The template is created and is listed in the tree view menu under the project you selected.
- Step 12** You can edit the template content by selecting the template that you created in the left menu. To edit the template content, see [Edit Templates, on page 144](#).
- Step 13** The **Template Editor** window opens where you can enter content for the template.
- Step 14** To validate the template, from the **Actions** drop-down list, choose **Check for errors**.
The DNA Center checks for these errors and reports them:
- Velocity syntax error
 - Conflicts with blacklisted commands
- Step 15** To save the template content, from the **Actions** drop-down list, choose **Save**. You can use the Velocity Template Language (VTL) to write the content in the template. For more information about using VTL, see <http://velocity.apache.org/engine-devel/vtl-reference.html>.
After saving the template, DNAC checks for any errors in the template. If there are any velocity syntax errors, then the template content is not saved and all the input variables that are defined in the template is automatically identified during the save process. The local variables (variables that are used in **for** loops, assigned through a set, and so on) are ignored.
- Step 16** To commit the template, from the **Actions** drop-down list, choose **Commit**. You can see only the committed templates in the network profile section.

Blacklisted Commands

Note You can associate only a committed template to a network profile.

Step 17 Click the form editor icon



at the top-right corner of the page to enter additional information to variables in the template.

What to do next

1. Edit Templates. For more information about editing templates, see [Edit Templates, on page 144](#)
2. Assign templates to profiles. For more information on assigning templates to profiles, see [Create and Associate Templates to Wireless Profiles, on page 148](#)

Blacklisted Commands

The blacklisted commands are the ones which are added to the blacklisted category. You can use these commands only through the DNA Center applications. If you use blacklisted commands in your templates, it shows a warning in the template that it may potentially conflict with some of the DNA Center provisioning applications.

Use this query to find out the blacklisted commands which are part of the DNA Center: **select commands from cliconfigtree where sdnconfig_id in (selectid from SDNConfig where classname like '%SPFServiceConfig')**.

Sample Templates**Configure Hostname**

```
hostname $name
```

Configure Interface

```
interface $interfaceName
description $description
```

Configure NTP on Cisco Wireless Controllers

```
config time ntp interval $interval
```

Create a Composite Template

Two or more regular templates are grouped together into a composite sequence template. You can create a composite sequential template for a set of templates, which are applied collectively to devices. For example, when you deploy a branch, you must specify the minimum configurations for the branch router. The templates that you create can be added to a single composite template, which aggregates all the individual templates that you need for the branch router. You must specify the order in which templates that are in the composite template are deployed to devices.

Procedure

- Step 1** From the Cisco DNA Center home page, choose **Tools > Template Editor**.
- Step 2** In the left pane, select the project under which you are creating the templates. Click the gear icon > **Add Templates** or click > **Add Templates** located at the top of the left pane.
- Step 3** In the **Add New Template** window that is displayed, click the **Composite Template** radio button to create composite sequential templates.
- Step 4** In the **Name** text box, enter a unique name for the template.
- Step 5** In the **Project Name** text box, enter a unique name for the project .
The text box is enabled if you are navigating from the > **Add Templates** path. The text box is disabled if you select a project, and click the gear icon > **Add Templates** in the tree pane.
- Step 6** Enter a description for the template in the **Description** text box.
- Step 7** Enter an intuitive name to tag the templates in the **Tags** text box. Tagging a configuration template helps you to:
- Search a template using the tag name in the search field.
 - Use the tagged template as a reference to configure more devices.
- Step 8** If you are creating a template that applies only to a particular device type, from the **Device Type** drop-down list, choose a device. The device types are displayed depending on what you select in the **Device Type** drop-down list.
- Step 9** From the **Software Type** drop-down list, choose the software type. You can select the specific software type such as IOS-XE, IOS-XR, or NX-OS if there are commands specific to these software types. If you select the software type as IOS, then the commands are applicable to all software types including IOS-XE, IOS-XR, and NX-OS. This is used at the provisioning time to check whether the selected device is conforming to the selection in the template.
- Step 10** Enter the software version in the **Software Version** text box. During the provisioning, DNA Center checks to see if the selected device has the similar software version as mentioned in the template. If there is a mismatch, then the provision skips the template.
- Step 11** Click **Add**. The composite template is created and is listed in the left menu under the project you selected.
- Step 12** Click the composite template that you created in the tree view pane.
- Step 13** The **Template Editor** window opens where you can drag and drop templates from the tree view pane to create a sequence. The templates are deployed based on the order in which they are sequenced. You can change the order of templates in the **Template Editor** window.
- Note** You can drag and drop those templates that have the same device type, software type, and software version as that of the composite template.
- Step 14** To abort the deployment process upon failure of the first template, select the first template in the **Template Editor** window and check the **Abort sequence on targets if deployment fails** checkbox.
- Step 15** From the Actions drop-down list, choose **Commit** to commit the template content.

What to do next

1. Assign templates to profiles. See [Create and Associate Templates to Wireless Profiles, on page 148](#).

Edit Templates

After creating a template, you can edit the template to include content to it.

Procedure

Step 1 From the Cisco DNA Center home page, choose **Tools > Template Editor**.

Step 2 Select the template that you want to edit in the left tree pane.

The Template Editor window appears in the right pane.

Step 3 In the **Template Editor** window, enter the template content. You can have a template with a single-line configuration or a multi-select configuration.

Note Velocity template framework restricts the use of variables starting with a number. Hence, you must ensure that the variable name starts with a letter and not with a number.

Step 4 Validate the template by selecting **Check for errors** from the **Actions** drop-down list.

DNA Center checks for these errors and reports them:

- Velocity syntax error
- Conflicts with blacklisted commands

Step 5 Click the Input Form icon



which is located in the top-right corner to bind variables in the template to network settings.

- Select the variables in the **Input Form** pane and click the **Required** check box to bind variables to the network settings.
- From the **Display** drop-down list, choose the type of UI widget you want to create at the time of provisioning: **Text Field**, **Single Select**, or **Multi Select**.
- To bind variables to network settings, select each variable in the **Input Form**, and check the **Bind to Source** check box under **Content** in the right pane.
 - Choose the **Source**, **Entity**, and **Attributes** from the respective drop-down lists.
 - For the source type **CommonSettings**, you can choose one of these entities: **dhcp.server**, **syslog.server**, **snmp.trap.receiver**, **ntp.server**, **timezone.site**, **device.banner**, **dns.server**, **netflow.collector**.
 - For the source type **NetworkProfile**, you can choose the entity type as **SSID**. The SSID entity that is populated is defined under the **Design > Network Profile** page. The binding generates a user-friendly SSID name, which is a combination of SSID name, site, and SSID category. From the

Attributes drop-down list, select the attribute for SSID:**wlanid**. This attribute is used during the advanced CLI configurations at the time of template provisioning.

- For the source type **Inventory**, you can choose one of these entities: **Device** or **Interface**. For the entity type **Device** and **Interface** the **Attribute** drop-down list shows the device or interface attributes.
- For the source type **Inventory**, you can choose one of these entities: **Device**, **Interface**, **APGroup**, or **FlexGroup**. For the entity type **Device** and **Interface** the **Attribute** drop-down list shows the device or interface attributes. The variable resolves to the APGroup and FlexGroup name that is configured on the device to which the template is applied.

After binding variables to a common setting, when you assign templates to a wireless profile and provision the template, whatever network settings that you have defined under **Network Settings > Network**, appears in the drop-down list. You must define these attributes under **Network Settings > Network** at the time of designing your network.

Step 6 From the **Actions** drop-down list, choose **Save** to save the template content.

Step 7 From the **Actions** drop-down list, choose **Commit** to commit the template content.

What to do next

1. Assign templates to profiles and provision the template. See [Create and Associate Templates to Wireless Profiles, on page 148](#).

Template Simulation

The interactive template simulation allows you to simulate the CLI generation of templates by specifying test data for variables before sending them to devices. You can save the test simulation result and use them in future if required.

Procedure

Step 1 Select **Tools > Template Editor**.

Step 2 Select the template you want to edit in the left menu.

The Template Editor window appears in the right pane.

Step 3 Click the Simulator icon



which is located in the top-right corner to run simulation on commands.

- From the **Actions** drop-down list, choose **New Simulation**. In the **New Simulation** window, enter a name for the simulation, and click **Submit**.
 - In the **Simulation Input** form, complete the required fields, and click **Run**. The results are displayed in the **Template Preview** window.
-

Template Form Editor

Procedure

Step 1 Select the template in the left tree pane. The template window opens.

Step 2 Click the **Form Editor** icon that is located in the top-right corner to add additional metadata to the template variables. All the variables that are identified in the template are displayed. You can configure the following metadata:

- Check the **Required** check box if this is a required variable during the provisioning. All the variables by default are marked as Required, which means you must enter the value for this variable at the time of provisioning. You can uncheck the **Required** check box only if the variables are assigned conditionally inside an **if-else** block in the template.
- Enter the field name in the **Field Name** text box. This is the label that is used for the UI widget of each variable during the provisioning.
- Enter the tooltip text that is displayed for each variable in the **Tooltip** text box.
- Enter the default value in the **Default Value** text box. This value appears during the provisioning as the default value.
- Enter any instructional text in the **Instructional Text** text box. Instructional text appears within the UI widget (for example, **Enter the hostname here**). The text within the widget is cleared when the user clicks the widget to enter any text.
- Choose the data type from the **Data Type** drop-down list: **String**, **Integer**, **IP Address**, or **Mac Address**.
- Choose the type of UI widget you want to create at the time of provisioning from the **Display Type** drop-down list: **Text Field**, **Single Select**, or **Multi Select**.
- Enter the number of characters that are allowed in the **Maximum Characters** text box. This is applicable only for string data type.

Step 3 After configuring additional metadata information, from the **Actions** drop-down list, choose **Save**.

Step 4 After saving the template, you must version the template. You must version the template every time you make changes to the template. To do that, from the **Actions** drop-down list, choose **Commit**. The **Commit** window appears. You can enter a commit note in the **Commit Note** text box. However, the version numbers are automatically generated by the system.

Step 5 To view the history, from the **Actions** drop-down list, select **Show History** to view previously created and versioned templates. A pop-up window appears.

- Click **View** in the pop-up window to see the content of the old version.
- Click **Edit** in the pop-up window to edit the template.

Step 6 To view the old versions, from the Actions drop-down list, select

Variable Binding

While creating a template, it is possible to specify variables that are contextually substituted. Many of these variables are available in the drop-down list in the template editor. In Cisco DNA Center Release 1.1, you had to manually enter values for every variable that is defined in the template.

From Release 1.2 onwards, template editor provides an option to bind or use variables in the template with the source object values either while editing or through the input form enhancements. For example, DHCP server, DNS server, Syslog server, and so on.

The pre-defined object values can be one of the following:

- Inventory
- Device object
- Interface object
- **Common Settings**—Settings available under the **Design > Network Settings > Network** page. The common settings variable binding resolves values that are based on the site to which the device belongs.

Special Keywords



Note All commands executed through templates are always in the **config t** mode. Hence, you do not have to specify the **enable** or **config t** commands explicitly in the template.

Enable Mode Commands



Note Specify the **#MODE_ENABLE** command if you want to execute any commands outside of the **config t** command.

Use this syntax to add **enable mode** commands to your CLI templates:

```
#MODE_ENABLE
<<commands>>
#MODE_END_ENABLE
```

Interactive Commands



Note Specify **#INTERACTIVE** if you want to execute a command where a user input is required.

An interactive command contains the input that must be entered following the execution of a command. To enter an interactive command in the CLI Content area, use the following syntax:

```
CLI Command<IQ>interactive question 1 <R> command response 1 <IQ>interactive question
2<R>command response 2
```

Where **<IQ>** and **<R>** tags are case-sensitive and must be entered in uppercase.

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

Combining Interactive Enable Mode Commands

Use this syntax to combine interactive **Enable Mode** commands:

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R> response
#ENDS_INTERACTIVE
#ENDS_END_ENABLE

#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

Multiline Commands



Note If you want multiple lines in the CLI template to be wrapped, use the **MLTCMD** tags. Otherwise, the command is sent line by line to the device. To enter multiline commands in the CLI Content area, use the following syntax:

```
<MLTCMD>first line of multiline command
second line of multiline command
.....
.....
last line of multiline command</MLTCMD>
```

- Where **<MLTCMD>** and **</MLTCMD>** are case-sensitive and must be in uppercase.
- The multiline commands must be inserted between the **<MLTCMD>** and **</MLTCMD>** tags.
- The tags cannot start with a space.
- The **<MLTCMD>** and **</MLTCMD>** tags cannot be used in a single line.

Create and Associate Templates to Wireless Profiles

Before you begin

Before provisioning the template, ensure that the templates are associated with a network profile and the profile is assigned to a site.

During provisioning, when the devices are assigned to the specific sites, the templates associated with the site through the network profile appears in the advanced configuration.

Procedure

Step 1 Choose Design > Network Profiles, and click Add Profile.

There are three types of profiles available:

- **Routing & NFV**—Select this to create a routing and NFV profile. See [Routing & NFC](#) for more information.
- **Switching**—Select this to create a switching profile.
 - Enter the **Profile Name**.
 - Click **+Add** and select the device type and template from the **Device Type** and **Template** drop-down lists.

Note If you do not see the template that you need, create a new template in Template Editor as described in [Create a Regular Template, on page 140](#).

 - Click **Save**.
- **Wireless**—Select this to create a wireless profile. Before assigning wireless network profile to a template, ensure that you have created wireless SSIDs.
 - Enter the **Profile Name**.
 - Click **+ Add SSID**. Those SSIDs that were created under **Network Settings > Wireless** gets populated.
 - Under **Attach Template(s)** area, select the template you want to provision from the **Template** drop-down list.
 - Click **Save** to save the profile.

Step 2 The **Network Profiles** page lists the following:

- **Profile Name**
- **Type**
- **Version**
- **Created By**
- **Sites**—Click **Assign Site** to add sites to the selected profile.

Step 3 Choose **Provision > Devices**. The **Device Inventory** window appears.

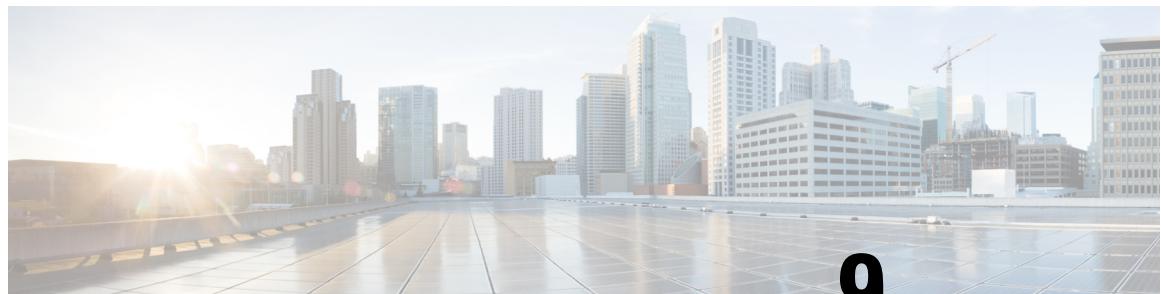
- Check one or more check boxes next to the device name that you want to provision.
- From the **Action** drop-down list, choose **Provision**.
- In the **Assign Site** window, assign a site to which the profiles are attached. In the **Choose a Site** field, enter the name of the site to which you want to associate the controller or select from the **Choose a Site** drop-down list.
- Click **Next**.

The **Configuration** window appears. In the **Managed AP Locations** field, enter the AP locations managed by controller. Here you can change, remove, or reassign the site. This is applicable only for wireless profiles.

- Click **Next**.
- The **Advanced Configuration** window appears. The templates associated with the site through the network profile appears in the advanced configuration.
 - Use the **Find** feature to quickly search for the device by entering the device name or expand the templates folder and select the template in the left pane. In the right pane, select values for those attributes which are bound to source from the drop-down lists .

- To export the template variables into a CSV file while deploying the template, click **Export** in the right pane. You can use the CSV file to make necessary changes in the variable configuration and import it into DNA Center at a later time by clicking **Import** in the right pane.
- Click **Next** to deploy the template. You are prompted to deploy the template now or to schedule it to a later time.
- To deploy the template now, click the **Now** radio button and click **Apply**. To schedule the template deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.

The **Status** column in the **Device Inventory** window shows **SUCCESS** after a successful deployment



CHAPTER 9

Run Diagnostic Commands on Devices

- [About Command Runner, on page 151](#)
- [Running Diagnostic Commands on Devices, on page 151](#)

About Command Runner

The Command Runner tool allows you to send diagnostic CLI commands to selected devices. Currently, show and other read-only commands are permitted.

Running Diagnostic Commands on Devices

Command Runner permits you to run diagnostic CLI commands on selected devices and view the resulting command output.

Before you begin

Perform the following procedures before you begin using Command Runner:

1. First, install the Command Runner application from the **App Management** window. From the DNA Center home page, click the gear icon (⚙), and then choose **System Settings > App Management > Packages & Updates**. Find the Command Runner package in this window and click **Install**.
2. After installation, run a discovery job to populate DNA Center with devices. You will be presented with a list of these devices from which to choose from and run the diagnostic CLI commands.

Procedure

- Step 1** From the DNA Center home page, click **Command Runner** in Tools.

The **Command Runner** window appears.

- Step 2** Place your cursor in the **Select one or more device(s)** field and click.

A list of discovered devices appear.

- Step 3** Select a device from the list to run the diagnostic CLI command or commands on.

A **Device List** with your selection appears. Either select another device to add to the list or click on your selected device in the list to close it.

Note Although the device list will display everything available in inventory, Command Runner is not supported for wireless access points and Cisco Meraki devices. If in a selected list an access point device or Cisco Meraki device is chosen, a warning message appears that states that no commands will be executed on these wireless access points and/or Cisco Meraki devices.

Step 4 In the **Add a Command** field, enter a CLI command and click **Add**.

Step 5 Click **Run Command(s)**.

If successful, a **Command(s) executed successfully** message appears.

Step 6 Click on the command displayed underneath the device in the window to view the command output.

The complete command output then displays in the **Command Runner** window.

Click **Copy CLI** to copy the command output to your clipboard, so that you can paste it to a text file if necessary.

Step 7 Click **Previous Page** to return to the previous window page.

If necessary, click the **x** symbol next to the device name to remove it from the device list. Click the **x** symbol next to the command to remove it from the command list.



CHAPTER 10

Configure Telemetry Profile

The Telemetry tool allows you to configure and apply profiles on devices for monitoring and assessing their health.

- [Configure a Telemetry Profile, on page 153](#)
- [Apply a Telemetry Profile to the Devices, on page 154](#)

Configure a Telemetry Profile

You can create telemetry assessment profiles for your network devices using the Telemetry tool.



Note By default, the **Disable-Telemetry** profile is configured by NDP on all interfaces on all capable devices.

Before you begin

Discover the devices in your network using DNA Center.

Procedure

Step 1 From the DNA Center home page, click **Telemetry** in **Tools**.

The **Telemetry** window appears.

Step 2 Click the **Site View** tab and check to see if network devices are listed in this window.

After configuring telemetry profiles, you will return to this window and apply the telemetry profiles to your devices.

Step 3 Click the **Profile View** tab.

The **Profile View** table displays with the following information:

- **Profile Name**—Name of DNA Center preconfigured profiles and any profiles that you configure.
- **Customized**—Displays whether the profile is one of the DNA Center preconfigured profiles or a user configured profile.

Apply a Telemetry Profile to the Devices

- **Profile Usage**—Number of devices that the telemetry profile is applied to.
- **Icon**—For DNA Center preconfigured profiles, by hovering your cursor over an icon, a definition appears. For example, when you hover your cursor over the following icons the following appears:
 - **Maximal Visibility**—Telemetry profile generated by NDP to enable all possible telemetry on all interfaces on all capable devices.
 - **Optimal Visibility**—Telemetry profile generated by NDP after analyzing the network topology, device capability, PIN, and enabled assurance features, for example, all telemetry will be enabled on WAN router for router 360.
 - **Disable Telemetry**—Disable Telemetry profile configured by NDP on all interfaces on all capable devices.

Step 4 Click **Add Profile**.**Step 5** Enter a profile name in the **Name** field.**Step 6** (Optional) Click **Syslog** and select a **Severity Level** from the drop down menu.**Step 7** (Optional) Click **SNMP** and select an SNMP version.**Step 8** (Optional) Click **SNMP Traps** and select an SNMP version.**Step 9** (Optional) Click **NetFlow** and select a version and profile.**Step 10** Click **Save** to save the profile configuration or click **Cancel** to cancel the profile configuration.**What to do next**

Proceed to apply the telemetry profile or profiles to your network devices. Use the **Telemetry Site View** options and fields to accomplish this task.

Apply a Telemetry Profile to the Devices

You can apply telemetry assessment profiles to your network devices using the Telemetry tool.

Before you begin

Perform the following preliminary tasks:

- Discover the devices in your network using DNA Center.
- Review and/or configure the available telemetry profiles using the **Telemetry Profile View** options and fields.

Procedure**Step 1** From the DNA Center home page, click **Telemetry** in **Tools**.

The **Telemetry** window appears.

Step 2 Click the **Site View** tab.

Step 3 Review the **Site View** table in this tab.

The following information is displayed:

- **Device Name**—Name of the device
- **Address**—IP address of device
- **Type**—Type of device.
- **Family**—Device category. For example, switch, router, access point.
- **Version**—Software version currently running on device.
- **Profile**—Applied telemetry profile on device.
- **Details**—Telemetry assessment of device. This assessment includes information about SNMP, NetFlow, Syslog, and SNMP traps on the device. Additionally, information is provided as to whether the device is capable of sending telemetry data, is actually sending this telemetry data, and/or whether the device is enabled to send this telemetry data.

Step 4 Click the check box next to the **Device Name** of a device to add a telemetry profile to that device.

Step 5 Click the **Actions** button and select a telemetry profile from the drop down list.

Step 6 From the **Show** drop down menu, select the telemetry profile you just applied.

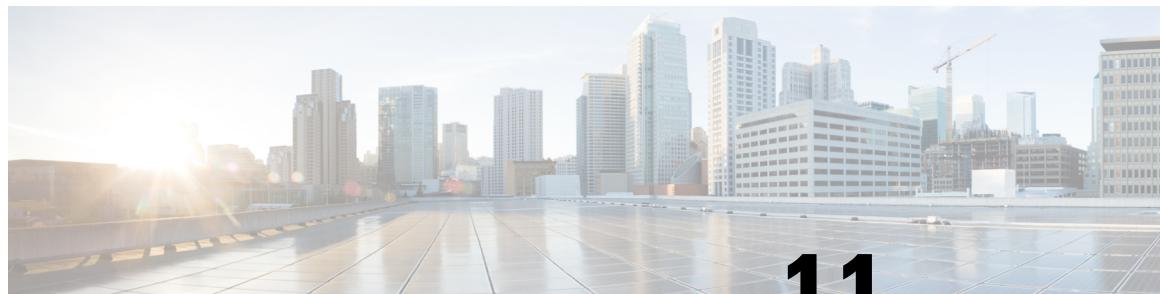
The device should appear in the filtered list, along with any other devices that have also been configured with the same telemetry profile.

What to do next

The telemetry profiles configured in this procedure are used by DNA Center to determine what data types to capture. These data types are then used in monitoring the health of the network devices.

Proceed to access the DNA Center **Assurance** application and review both **Assurance Health** and **Assurance Issues** to check up on the health of your network devices.

Apply a Telemetry Profile to the Devices



CHAPTER 11

Configure Policies

- [Policy Overview](#), on page 157
- [Policy Dashboard](#), on page 157
- [Group-Based Access Control Policies](#), on page 158
- [IP-Based Access Control Policies](#), on page 163
- [Application Policies](#), on page 169
- [Traffic Copy Policies](#), on page 203
- [Virtual Networks](#), on page 207

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, traffic copy policies, and application policies.

Policy Dashboard

The **Policy Dashboard** window shows the number of virtual networks, group-based access control policies, IP-based access control policies, traffic copy policies, scalable groups, and IP network 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.

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. For more information, see the [Cisco Digital Network Architecture Center Installation Guide](#).



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.

A group-based access control policy has two main components:

- **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 Contract**—An access contract is a common building block that is used in both group-based and IP-based access control policies. It defines the rules that make up the access control policies. These rules specify 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.

Before you can create group-based 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 > Group-Based Access Control > Scalable Groups**. You should see scalable groups populated in the **Scalable Groups** tab. 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](#).

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.

Workflow to Configure a Group-Based Access Control Policy

Before you begin

- Make sure that you have integrated Cisco ISE with DNA Center.
- In Cisco ISE, make sure that the work process setting is configured as **Single Matrix** so that there is only one policy matrix for all devices in the TrustSec network.

Procedure

	Command or Action	Purpose
Step 1	(Optional) 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.	For more information, see Create a Virtual Network, on page 207 .
Step 2	(Optional) Create scalable groups. After you integrate with Cisco ISE, the scalable groups that exist in Cisco ISE are propagated to DNA Center. If a scalable group that you need does not exist, you can create it in Cisco ISE.	For more information, see Create a Group-Based Scalable Group, on page 159 .
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 a Group-Based Access Control Contract, on page 160 .
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 161

Create a Group-Based Scalable Group

You can access Cisco ISE through the DNA Center interface to create scalable groups. After you have added a scalable group in Cisco ISE, it is synchronized with the DNA Center database so that you can use it in an access-control policy.



Note

You cannot edit or delete scalable groups from DNA Center; you need to perform these tasks from Cisco ISE. After you delete a scalable group from Cisco ISE, the scalable group name is not removed from the DNA Center policy dashboard. Instead, the DNA Center policy dashboard displays the scalable group in red text to indicate that it has been deleted.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Group-Based Access Control > Scalable Groups**.
All of the scalable groups that have been created in Cisco ISE are displayed.
- Step 2** Click **Add Groups**.
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.

Related Topics

[Workflow to Configure a Group-Based Access Control Policy](#), on page 159

Create a Group-Based Access Control Contract

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Group-Based Access Control > Access Contract**.
- Step 2** Click **Add Contract**.
- Step 3** In the 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 **Action** drop-down list in the table, choose either **Deny** or **Permit**.
- Step 6** From the **Port/Protocol** drop-down list, choose a port or protocol.
- If DNA Center does not have the port or protocol that you need, click **Add Port/Protocol** to create your own.
 - In the **Name** field, enter a name for the port or protocol.
 - From the **Protocol** drop-down list, choose **UDP**, **TDP**, or **TCP/UDP** as the protocol.
 - In the **Port Range** field, enter the port range.
 - If you want DNA Center to configure the port or protocol as defined and not report any conflicts, check the **Ignore Conflict** check box.
- 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 a Group-Based Access Control Contract

**Note**

If you edit a contract that is used in a policy, the policy's state changes to **MODIFIED** in the **Group-Based Access Control Policies** 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 > Group-Based Access Control > 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**. For field definitions, see [Create a Group-Based Access Control Contract, on page 160](#).

Note

If you made changes to a contract that is used in a policy, you need to deploy the modified policy by choosing **Policy > Group-Based Access Control > 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 > Group-Based Access Control > Group-Based Access Control Policies**.

Step 2 Click **Add Policy**.

Step 3 Complete the following fields:

Field	Description
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.

Edit or Delete a Group-Based Access Control Policy

Field	Description
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 **Group-Based Access Control Policies** 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 > Group-Based Access Control > 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**. For field definitions, see [Create a Group-Based Access Control Policy, on page 161](#).

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**.
-

Deploy a Group-Based Access Control Policy

If you make changes that affect a policy's configuration, you need to redeploy the policy to implement these changes.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Group-Based Access Control > Group-Based Access Control**.
- Step 2** Locate the policy that you want to deploy.
- Step 3** Check the check box next to the policy.
- Step 4** Click **Deploy**.
You are prompted to deploy your policy now or to schedule it for a later time.
- Step 5** Do one of the following:
- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
 - To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.

IP-Based Access Control Policies

An IP-based access control policy controls the traffic going into and coming out of a Cisco device in the same way that an Access Control List (ACL) does. As with an ACL, an IP-based access control policy contains lists of permit and deny conditions that are applied to traffic flows based on various criteria including protocol type, source IP address, destination IP address, or destination port number.

IP-based access control policies can be used to filter traffic for various purposes, including security, monitoring, route selection, and network address translation.

An IP-based access control policy has two main components:

- **IP Network Groups**—IP network groups comprise IP subnets that share the same access control requirements. These groups can be defined only in DNA Center. An IP network group may have as few as one IP subnet in it.
- **Access Contract**—An access contract is a common building block that is used in both IP-based and group-based access control policies. It defines the rules that make up the access control policies. These rules specify the actions (permit or deny) performed when traffic matches a specific port or protocol and the implicit actions (permit or deny) performed when no other rules match.

Workflow to Configure an IP-Based Access Control Policy

Before you begin

- To create IP network groups from the **Policy > IP Based Access Control > IP Network Groups** window, make sure that you have integrated Cisco ISE with DNA Center. However, Cisco ISE is not mandatory if you are adding groups within the **Policy > IP Based Access Control > IP Network Groups** window while creating a new IP-based access control policy.



Note Editing an IP network group on the **Policy > IP Based Access Control** page is possible without Cisco ISE. But creation of IP network groups from the **IP Based Access Control** page requires Cisco ISE.

- Make sure you have defined the following global network settings and provision the device.
 - Network servers, such as AAA, DHCP, and DNS Servers—(See [Configure Global Network Servers, on page 134](#).)
 - Device credentials such as CLI, SNMP, HTTP, and HTTPS credentials—(See [Configure Global Device Credentials, on page 128](#).)
 - IP address pools—(See [Configure IP Address Pools, on page 133](#).)
 - Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—(See [Configure Global Wireless Settings, on page 113](#).)
 - Provision devices—(See [Provisioning, on page 211](#).)

Procedure

	Command or Action	Purpose
Step 1	Create IP network groups.	For more information, see Create an IP Network Group, on page 165 .
Step 2	Create an IP-based access control contract. An IP-based access control contract defines a set of rules between the source and destination. These rules dictate the action (allow or deny) that network devices perform based on the traffic that matches the specified protocols or ports. For more information, see Create an IP-Based Access Control Contract, on page 165 .	
Step 3	Create an IP-based access control policy. The access control policy defines the access control contract that governs traffic between the source and destination IP network groups.	For more information, see Create an IP-Based Access Control Policy, on page 166 .

Create an IP Network Group

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > IP Based Access Control > IP Network Groups**.
- Step 2** Click **Add Groups**.
- Step 3** In the **Name** field, enter a name for the IP Network group.
- Step 4** In the **Description**, enter a word or phrase that describes the IP network group.
- Step 5** In the **IP Address or IP/CIDR** field, enter the IP addresses that make up the IP network group.
- Step 6** Click **Save**.
-

Edit or Delete an IP Network Group

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > IP Based Access Control > 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 165](#).
 - To delete the group, click **Delete** and then click **Yes** to confirm.
-

Create an IP-Based Access Control Contract

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > IP Based Access Control > Access Contract**.
- Step 2** Click **Add Contract**.
- Step 3** In the 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 **Action** drop-down list in the table, choose either **Deny** or **Permit**.
- Step 6** From the **Port/Protocol** drop-down list, choose a port or protocol.
- a) If DNA Center does not have the port or protocol that you need, click **Add Port/Protocol** to create your own.
 - b) In the **Name** field, enter a name for the port or protocol.
 - c) From the **Protocol** drop-down list, choose **UDP**, **TDP**, or **TCP/UDP** as the protocol.
 - d) In the **Port Range** field, enter the port range.

- e) If you want DNA Center to configure the port or protocol as defined and not report any conflicts, check the **Ignore Conflict** check box.

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 IP-Based Access Control Contract

**Note**

If you edit a contract that is used in a policy, the policy's state changes to **MODIFIED** in the **IP Based Access Control Policies** 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 > IP-Based Access Control > Access Contract**.

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**. For field definitions, see [Create an IP-Based Access Control Contract, on page 165](#).

Note

If you made changes to a contract that is used in a policy, you need to deploy the modified policy by choosing **Policy > IP-Based Access Control > IP-Based Access Control Policies**, checking the check box next to the policy name, and clicking **Deploy**.

- To delete the contract, click **Delete**.

Create an IP-Based Access Control Policy

You can create an IP-based access control policy to limit traffic between IP network groups.

- Multiple rules can be added to a single policy with different configurations.
- For a given combination of IP groups and contract classifiers, rules are created and pushed to the devices. This count cannot exceed 64 rules as Cisco WLC limits an ACL to have a maximum of 64 rules.
- If a custom contract or the IP group that is used in a **Deployed** policy is modified, the policy is flagged with the status as **Modified** indicating that it is Stale and requires a re-deployment for the new configurations to be pushed to the device.

Procedure

Step 1

From the DNA Center home page, click **Policy > IP Based Access Control > IP Based Access Control Policies**.

Step 2

Click **Add Policy**.

Step 3

Complete the following fields:

Field	Description
Policy Name	Name of the policy.
Description	Word or phrase that identifies the policy.
SSID	<p>Lists FlexConnect SSIDs and non FlexConnect SSIDs that were created during the design of SSIDs. If the selected SSID is configured in a FlexConnect mode, then the access policy is configured in FlexConnect mode. Otherwise, it will be configured in a regular way.</p> <p>Note If an SSID is part of one policy, that SSID will not be available for another policy.</p> <p>Note A valid site-SSID combination is required for policy deployment. You will not be able to deploy a policy if the selected SSID is not provisioned under any devices.</p>
Site Scope	Sites to which a policy is applied. If you configure a wired policy, the policy is applied to all wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope. For more information, see Site Scope, on page 170 .
Source	Origin of the traffic that is affected by the contract. Click the SearchSource field and select an IP network group from the drop-down list. If the IP network that you want is not available, click +Group to create one.
Contract	Rules that govern the network interaction between the source and destination in an access control policy. Click Add Contract to define the 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.
Destination	Target of the traffic that is affected by the contract. Click the SearchDestination field and select an IP network group from the drop-down list. If the IP network that you want is not available, click +Create IP Network Group to create one.
Direction	Configures the relationship of the traffic flow between the source and destination. To enable the contract for traffic flowing from the source to the destination, select One-Way . To enable the contract for traffic flowing in both directions (from the source to the destination and from the destination to the source), select Bi-directional .

Step 4

(Optional) To create an IP network group, click **Create IP Network Group**.

Step 5

(Optional) To add another rule, click the plus sign.

Note To delete a rule, click **x**.

Step 6

(Optional) To reorder the sequence of the rules, drag and drop a rule in the order you want.

Step 7 Click **Deploy**.

The success message "IP-Based Access Control Policy has been created and deployed successfully" displays. Depending on the SSID selected, either a FlexConnect policy or a standard policy is created with different level of mapping information and deployed. The **Status** of the policy is shown as **DEPLOYED**. A wireless icon next to the **Policy Name** shows that the deployed access policy is a wireless policy.

Edit or Delete an IP-Based Access Control Policy

If you need to, you can change or delete an IP-based access control policy.



Note If you edit a policy, the policy's state changes to **MODIFIED** on the **IP Based Access Control Policies** 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, you need to redeploy the policy to the network.

Procedure

Step 1 From the DNA Center home page, click **Policy > IP Based Access Control > IP Based Access Control Policies**.

Step 2 Select 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**. When you are done, click **Save**.
- To delete the policy, click **Delete**.

Step 4 If you made changes to the policy, deploy the modified policy by selecting the check box next to the policy name and clicking **Deploy**.

Deploy an IP-Based Access Control Policy

If you make changes that affect a policy's configuration, you need to redeploy the policy to implement these changes.

Procedure

Step 1 From the DNA Center home page, choose **Policy > IP Based Access Control > IP Based Access Control Policy**.

Step 2 Locate the policy that you want to deploy.

Step 3 Check the check box next to the policy.

Step 4 Click **Deploy**.

You are prompted to deploy your policy now or to schedule it for a later time.

Step 5 Do one of the following:

- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
- To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.

Application Policies

Quality of service (QoS) refers to the ability of a network to provide preferential or deferential service to selected network traffic. By configuring QoS, you can ensure that network traffic is handled in such a way that makes the most efficient use of network resources while still adhering to the objectives of the business, such as guaranteeing voice quality meets enterprise standards or ensuring a high Quality of Experience (QoE) for video.

You can configure QoS in your network using application policies in DNA Center. Application policies comprise these basic parameters:

- **Application Sets**—Set of applications with similar network traffic needs. Each application set is assigned a business relevance group (business relevant, default, or business irrelevant) that defines the priority of its traffic. QoS parameters in each of the three groups are defined based on Cisco Validated Design (CVD). You can modify some of these parameters to more closely align with your objectives. For more information, see [Applications and Application Sets, on page 170](#).
- **Site Scope**—Sites to which an application policy is applied. If you configure a wired policy, the policy is applied to all wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope. For more information, see [Site Scope, on page 170](#).

DNA Center takes all of these parameters and translates them into the proper device command line interface (CLI) commands. When you deploy the policy, DNA Center configures these commands on the devices defined in the site scope.



Note DNA Center configures quality of service policies on devices based on the QoS feature set available on the device. For more information about a device's QoS implementation, see the device product documentation.

CVD-Based Settings in Application Policies

The default QoS trust and queuing settings in application policies are based on the Cisco Validated Design (CVD) for Enterprise Medianet Quality of Service Design. CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by Cisco engineers to ensure faster, more reliable, and fully predictable deployment.

The latest validated designs related to quality of service are published in the Cisco Press book, *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition, available at:

<http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694>. For additional information, see the following Cisco documentation:

- [Cisco Validated Designs](#)
- [Enterprise Medianet Quality of Service Design 4.0](#)
- [Medianet Campus QoS Design 4.0](#)
- [Medianet WAN Aggregation QoS Design 4.0](#)

Site Scope

A site scope defines the sites to which an application policy is applied. When defining a policy, you configure whether a policy is for wired or wireless devices. You also configure a site scope. If you configure a wired policy, the policy is applied to all wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices in the site scope with the SSID defined in the scope.

This allows you to make tradeoffs as necessary to compensate for differences in the behaviors between wired and wireless network segments. For example, wireless networks typically have lower bandwidth, lower speed, and increased packet loss in comparison to wired networks. Individual wireless segments may exhibit further variation due to local conditions of RF interference, congestion, and other factors, such as the varying capabilities of network devices. The ability to apply per-segment policies to individual wireless segments enables the adjustment of traffic-handling rules to ensure that the highest-priority traffic is least affected by degradation of the wireless network.

Applications and Application Sets

Applications are the software programs or network signaling protocols that are being used in your network. DNA Center supports all of the applications in the Cisco Next Generation Network-Based Application Recognition (NBAR2) library of approximately 1400 distinct applications.

Applications are grouped into logical groups called application sets. An application set can be assigned a business relevance within a policy.

Applications are also mapped into industry standard-based traffic classes, as defined in RFC 4594, that have similar traffic treatment requirements. The traffic classes define the treatments (such as DSCP marking, queuing and dropping) that will be applied to the application traffic, based on the business relevance group that it is assigned.

If you have additional applications that are not included in DNA Center, you can add them as custom applications and assign them to application sets. For more information, see [Custom Applications, on page 174](#). You can also create custom application sets to contain any applications that you want.

For more information about NBAR2, see the following URL: <https://www.cisco.com/c/en/us/products/ios-nx-os-software/network-based-application-recognition-nbar/index.html>.

Business-Relevance Groups

A business-relevance group classifies a given application set according to how relevant it is to your business and operations.

The business-relevance groups are business relevant, default, and business irrelevant, and they essentially map to three types of traffic: high priority, neutral, and low priority.

- **Business Relevant**—(High-priority traffic) The applications in this group directly contribute to organizational objectives and, as such, may include a variety of applications, including voice, video, streaming and collaborative multimedia applications, database applications, enterprise resource applications, email, file-transfers, content distribution, and so on. Applications designated as business-relevant are treated according to industry best-practice recommendations, as prescribed in Internet Engineering Task Force (IETF) RFC 4594.
- **Default**—(Neutral traffic) This group is intended for applications that may or may not be business-relevant. For example, generic HTTP/HTTPS traffic may contribute to organizational objectives at times, while at other times such traffic may not. You may not have insight into the purpose of some applications (for instance, legacy applications or even newly deployed applications), so the traffic flows for these applications should be treated with the Default Forwarding service, as described in IETF RFC 2747 and 4594.
- **Business Irrelevant**—(Low-priority traffic) This group is intended for applications that have been identified to have no contribution towards achieving organizational objectives. They are primarily consumer- and/or entertainment-oriented in nature. We recommend that this type of traffic be treated as a "Scavenger" service, as described in IETF RFC 3662 and 4594.

Applications are grouped into application sets and sorted into business-relevance groups. You can include an application set in a policy as-is, or you can modify it to meet the needs of your business objectives and your network configuration.

For example, YouTube is member of the consumer-media application set, which is business-irrelevant (by default), because most customers typically classify this application this way. However, this classification may not be the true for all companies; for example, some businesses may be using YouTube for training purposes. In such cases, an administrator can move the YouTube application into the streaming-video application set, which is business relevant by default.

Unidirectional and Bidirectional Application Traffic

Some applications are completely symmetrical and require identical bandwidth provisioning on both ends of the connection. Traffic for such applications is described as bidirectional. For example, if 100 kbps of Low-Latency Queuing (LLQ) are assigned to voice traffic in one direction, 100 kbps of LLQ also must be provisioned for voice traffic in the opposite direction. This scenario assumes that the same Voice over IP (VoIP) coder-decoders (codecs) are being used in both directions and does not account for multicast Music-on-Hold (MoH) provisioning. However, certain applications, such as Streaming Video and multicast MoH, are most often unidirectional. Therefore, it might be unnecessary and even inefficient to provision any bandwidth guarantees for such traffic on a branch router for the branch-to-campus direction of traffic flow.

DNA Center allows you to specify whether an application is unidirectional or bidirectional for a particular policy.

On switches and wireless controllers, NBAR2 and custom applications are unidirectional by default. However, on routers, NBAR2 applications are bidirectional by default.

Consumers and Producers

You can configure relationships between applications such that when traffic from one application is sent to another application (thus creating a specific a-to-b traffic flow), the traffic is handled in a specific way. The applications in this relationship are called producers and consumers and are defined as follows:

- **Producer**—Sender of the application traffic. For example, in a client/server architecture, the application-server would be considered the producer, as the traffic primarily flows in the server-to-client direction. In the case of a peer-to-peer application, the remote peer is considered the producer.
- **Consumer**—Receiver of the application traffic. The consumer may be a client endpoint in a client/server architecture or it may be the local device in a peer-to-peer application. Consumers may be endpoint devices but may, at times, be specific users of such devices (typically identified by IP Addresses or specific subnets). There may also be times when an application is the consumer of another application's traffic flows.

Setting up this relationship allows you to configure specific service levels for traffic matching this scenario.

Marking, Queuing, and Dropping Treatments

DNA Center bases its marking, queuing, and dropping treatments on IETF RFC 4594 and the business relevance category that you have assigned to the application. DNA Center assigns all of the applications in the Default category to the Default Forwarding application class and all of the applications in the Irrelevant Business category to the Scavenger application class. For applications in the Relevant Business category, DNA Center assigns traffic classes to applications based on the type of application. See the table below for a list of application classes and their treatments.

Table 45: Marking, Queuing, and Dropping Treatments

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
Relevant	VoIP 1	Expedited Forwarding (EF)	Priority Queueing (PQ)	VoIP telephony (bearer-only) traffic, for example, Cisco IP Phones.
	Broadcast Video	Class Selector (CS) 5	PQ	Broadcast TV, live events, video surveillance flows, and similar inelastic streaming media flows, for example Cisco IP Video Surveillance and Cisco Enterprise TV. (Inelastic flows refer to flows that are highly drop sensitive and have no retransmission and/or flow-control capabilities.)
	Realtime Interactive	CS4	PQ	Inelastic high-definition interactive video applications and audio and video components of these applications, for example, Cisco TelePresence.
	Multimedia Conferencing	Assured Forwarding (AF) 41	Bandwidth (BW) Queue and Differentiated Services Code Point (DSCP) Weighted Random Early Detect (WRED)	Desktop software multimedia collaboration applications and audio and video components of these applications, for example, Cisco Jabber and Cisco WebEx.
	Multimedia Streaming	AF31	BW Queue and DSCP WRED	Video-on-Demand (VoD) streaming video flows and desktop virtualization applications, such as Cisco Digital Media System.
	Network Control	CS6	BW Queue only 2	Network control plane traffic, which is required for reliable operation of the enterprise network, such as EIGRP, OSPF, BGP, HSRP, IKE, and so on.
	Signaling	CS3	BW Queue and DSCP	Control-plane traffic for the IP voice and video telephony infrastructure.
	Operations, Administration, and Management (OAM)	CS2	BW Queue and DSCP 3	Network operations, administration, and management traffic, such as SSH, SNMP, syslog, and so on.
		AF21	BW Queue and DSCP WRED	

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
	Transactional Data (Low-Latency Data)			Interactive (foreground) data applications, such as enterprise resource planning (ERP), customer relationship management (CRM), and other database applications.
	Bulk Data (High-Throughput Data)	AF11	BW Queue and DSCP WRED	Non-interactive (background) data applications, such as E-mail, file transfer protocol (FTP), and backup applications.
Default	Default Forwarding (Best Effort)	DF	Default Queue and RED	Default applications and applications assigned to the default business-relevant group. Because only a small minority of applications are assigned to priority, guaranteed-bandwidth, or even to differential service classes, the vast majority of applications continue to default to this best-effort service.
Irrelevant	Scavenger	CS1	Minimum BW Queue (Differential) and DSCP	Non-business related traffic flows and applications assigned to the business-irrelevant group, such as data or media applications that are entertainment-oriented. Examples include YouTube, Netflix, iTunes, and Xbox Live.

¹ VoIP signaling traffic is assigned to the Call Signaling class.

² WRED is not be enabled on this class, as network control traffic should not be dropped.

³ WRED is not enabled on this class, as OAM traffic should not be dropped.

Custom Applications

Custom applications are applications that you add to DNA Center. An orange bar is displayed next to custom applications to distinguish them from the standard NBAR2 applications and application sets. For wired devices, you can define applications based on server name, IP address and port, or URL. You cannot define custom applications for wireless devices.

When you define an application according to its IP address and port, you can also define a Differentiated Services Code Point (DSCP) value and port classification.

To simplify the configuration process, you can define an application based on another application that has similar traffic and service-level requirements. DNA Center copies the other application's traffic class settings to the application that you are defining.

DNA Center does not configure Access Control Lists (ACLs) for port numbers 80, 443, and 8080, even if they are defined as part of a custom application. If the custom application has a transport IP defined, DNA Center configures the application on the devices.

**Note**

For a custom application to be programmed on devices when a policy is deployed, you must assign the custom application to one of the application sets defined in the policy.

Favorite Applications

DNA Center allows you to flag applications that you want to configure on devices before all other applications, except custom applications. Flagging an application as a favorite helps to ensure that the QoS policies for your favorite applications get configured on devices. For more information, see [Processing Order for Devices with Limited Resources, on page 178](#).

Although there is no limit to the number of applications that you can mark as favorite, designating only a small number of favorite applications (for example, less than 25) helps to ensure that these applications are treated correctly from a business-relevance perspective in deployments with network devices that have limited Ternary Content-Addressable Memory (TCAM).

Favorite applications can belong to any business-relevance group or traffic class and are configured system-wide, not on a per-policy basis. For example, if you flag the cisco-jabber-video application as a favorite, the application is flagged as a favorite in all policies.

Keep in mind that not only business-relevant applications may be flagged as favorites, but even business-irrelevant applications may be flagged as such. For example, if an administrator notices a lot of unwanted Netflix traffic on his network, he may chose to flag Netflix as a favorite application (despite its being assigned as business-irrelevant). In this case, Netflix would be programmed into the device policies before other business-irrelevant applications, ensuring that the business-intent of controlling this application is realized.

Service Provider Profiles

Service provider (SP) profiles define the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class models.

When application policies are deployed on the devices, each SP profile is assigned a certain service-level agreement (SLA) that maps each SP class to a Differentiated Services Code Point (DSCP) value and a percentage of bandwidth allocation. See the table below.

You can customize the DSCP values and the percentage of bandwidth allocation in a SP profile when configuring an application policy.

After you create the SP profile, you need to configure it on the WAN interfaces. To configure WAN interfaces, see [Configure Service Provider Profiles on WAN Interfaces](#).

Table 46: Default SLA Attributes for SP Profiles with 4-Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Class 2 Data	AF21	—	—	25
Default	0	—	—	31

Table 47: Default SLA Attributes for SP Profiles with 5-Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Class 3 Data	AF11	—	—	1
Default	Best Effort	—	—	30

Table 48: Default SLA Attributes for SP Profiles with 6-Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Class 1 Data	AF31	—	—	10
Class 3 Data	AF11	—	—	1
Video	AF41	—	—	34
Voice	EF	Yes	10	—
Default	0	—	—	30
Class 2 Data	AF21	—	—	25

Table 49: Default SLA Attributes for SP Profiles with 8-Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Network-Control Management	CS6	—	—	5

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Streaming Video	AF31	—	—	10
Call Signalling	CS3	—	—	4
Scavenger	CS1	—	—	1
Interactive Video	AF41	—	—	30
Voice	EF	Yes	10	—
Default	0	—	—	25
Critical Data	AF21	—	—	25

Queuing Profiles

Queuing profiles allow you to define an interface's bandwidth allocation based on the interface speed and the traffic class.



Important Queueing profiles do not apply to WAN-facing interfaces that are connected to a service provider profile.

The following interface speeds are supported:

- 100 Gbps
- 10/40 Gbps
- 1 Gbps
- 100 Mbps
- 10 Mbps
- 1 Mbps

If the speed of an interface falls between two interface speeds, DNA Center treats the interface at the lower interface speed.



Note DNA Center attempts to detect the operational speed of the interface in order to apply the correct policy. However, if a switch port is administratively down, DNA Center cannot detect the speed. In this case, DNA Center uses the interface's supported speed.

You define a queuing policy as part of an application policy. When you deploy the application policy, the devices in the sites that are selected in the site scope are configured with the assigned LAN queuing policy.

If no LAN queuing policy is assigned, the application policy uses the default, Cisco Validated Design (CVD) queuing policy.

If you change the queuing policy in an application policy that has already been deployed, the policy becomes stale, and you need to redeploy the policy for the changes to be configured on the devices.

Note the following additional guidelines and limitations of queuing policies:

- You cannot delete a LAN queuing profile if it is used in a policy.
- If you update a queuing profile that is associated with a policy, the policy is marked as stale. You need to redeploy the policy to provision the latest changes.
- Traffic class queuing customization does not affect interfaces on Cisco service provider switches and routers. You need to continue to configure these interfaces without using DNA Center.

Table 50: Default CVD LAN Queuing Policy

Traffic Class	Default Bandwidth (Total = 100%)
	⁴
Voice	10%
Broadcast Video	10%
Real-Time Interactive	13%
Multimedia Conferencing	10%
Network control	3%
Signaling	2%
OAM	2%
Transactional Data	10%
Bulk Data	4%
Scavenger	1%
Best Effort	25%

⁴ We recommend that the total bandwidth for Voice, Broadcast Video, and Real-Time Interactive traffic classes equals no more than 33%.

Processing Order for Devices with Limited Resources

Some network devices have a limited memory (called Ternary Content Addressable Memory or TCAM) for storing network access control lists (ACLs) and access control entries (ACEs). So, as ACLs and ACEs for applications are configured on these devices, the available TCAM space is used. When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

To ensure that QoS policies for the most important applications get configured on these devices, DNA Center allocates TCAM space based on the following order:

1. **Rank**—Number assigned to custom and favorite applications, but not to existing, default NBAR applications. The lower the rank number, the higher the priority. For example, an application with rank 1 has a higher priority than an application with rank 2, and so on. Having no rank is the lowest priority.
 - Custom applications are assigned rank 1 by default.
 - Default NBAR applications are not assigned a rank until you mark them as favorites, at which point they are assigned rank 10,000.
2. **Traffic Class**—Priority based on the following order: Signaling, Bulk Data, Network Control, Operations Administration Management (Ops Admin Mgmt), Transactional Data, Scavenger, Multimedia Streaming, Multimedia Conferencing, Real Time Interactive, Broadcast Video, and VoIP Telephony
3. **Popularity**—Number (1–10) that is based on Cisco Validated Design (CVD) criteria. The popularity number cannot be changed. An application with a popularity of 10 has a higher priority than an application with a popularity of 9, and so on.
 - Custom applications are assigned popularity 10 by default.
 - Default NBAR applications are assigned a popularity number (1–10) that is based on Cisco Validated Design (CVD) criteria. When you mark an application as a favorite, this does not change the popularity number (only rank is changed).
4. **Alphabetization**—If two or more applications have the same rank and popularity number, they are sorted alphabetically by the application’s name, and assigned a priority accordingly.

For example, you define a policy that has the following applications:

- Custom application, custom_realtime, which has been assigned rank 1 and popularity 10 by default.
- Custom application, custom_salesforce, which has been assigned rank 1 and popularity 10 by default.
- Application named corba-iiop, which is in the transactional data traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 9 (based on CVD).
- Application named gss-http, which is in the Ops Admin Mgmt traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 10 (based on CVD).
- All other, default NBAR applications, which have no rank, but will be processed according to their traffic class and default popularity (based on CVD).

According to the prioritization rules, the applications are configured on the device in this order:

Application Configuration Order	Reason
1. Custom application, custom_realtime	Custom applications are given highest priority. Given that the custom_salesforce and custom_realtime applications have the same rank and popularity, they are sorted alphabetically, custom_realtime before custom_salesforce.
2. Custom application, custom_salesforce	

Application Configuration Order	Reason
3. Favorite application, gss- <i>http</i>	Because both of these applications have been designated as favorites, they have the same application ranking. So, DNA Center evaluates them according to their traffic class. Because gss- <i>http</i> is in the Ops Admin Mgmt traffic class, it is processed first, followed by the corba-iiop application, which is in the Transactional Data traffic class. Their popularity does not come into play because the processing order has been determined by their traffic class.
4. Favorite application, corba-iiop	
5. All other, default NBAR applications	All other applications are next and are prioritized according to traffic class and then popularity, with any applications having the same popularity being alphabetized according to the application's name.

Policy Drafts

When you create a policy, you can save it as a draft without having to deploy it. Saving it as a draft allows you open the policy later and make changes to it. You can also make changes to a deployed policy, and save it as a draft.



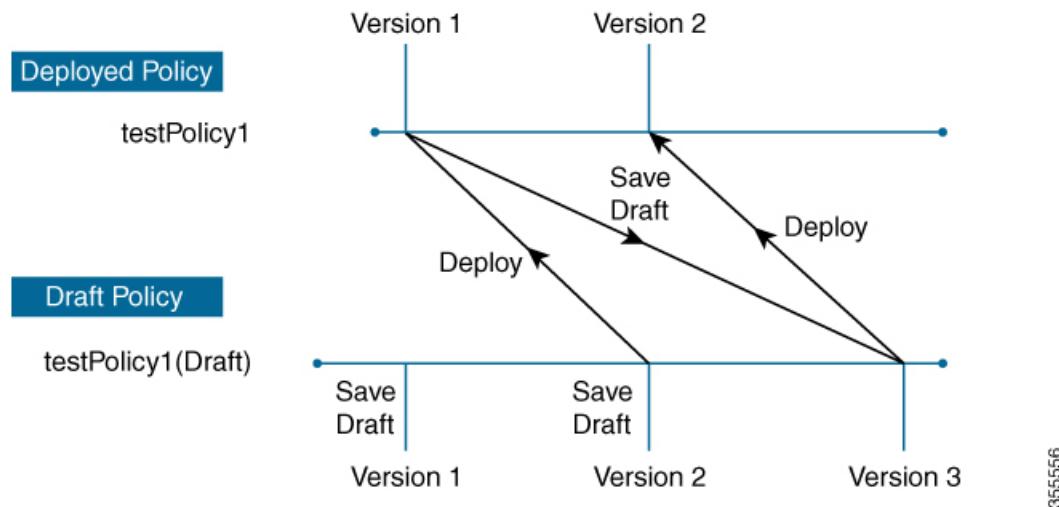
Note After you save or deploy a policy, you cannot change its name.

Draft policies and deployed policies are related to one another, but they have their own versioning, as follows:

When you save a policy as a draft, DNA Center appends the policy name with (Draft), and increments the version number. When you deploy a policy, DNA Center increments the version number of the deployed policy.

For example, as shown in the figure below, you create a policy named testPolicy1 and save it as a draft. The policy is saved as testPolicy1 (Draft), version number 1. You make a change to the draft and save it again. The policy has the same name, testPolicy1 (Draft), but its version number is incremented to 2.

You decide you like the policy so you deploy it to the network. The policy is deployed with the name testPolicy1 and its version number is 1. You make a change to the deployed policy and save it as a draft. The draft policy, testPolicy1 (Draft) is incremented to version number 3. When you ultimately deploy that version, testPolicy1 is incremented to version 2.

Figure 6: Deployed Policy and Draft Policy Versioning

Any time you modify and save either a draft policy or a deployed policy, the draft policy version number is incremented. Similarly, any time you deploy either a draft policy or a modified deployed policy, the deployed policy version is incremented.

Just as with deployed policies, you can display the history of draft policies and roll them back to previous versions.

For more information about viewing the history of policy versions and rolling back to a previous version, see [Policy Versioning, on page 182](#).

Policy Preview

Before you deploy a policy, you can generate the command line interface (CLI) that will be applied to a device.

The Preview operation generates the CLI commands for the policy, compares them with the CLI commands in the running configuration on the device and returns only the remaining CLI commands that are required to configure the policy on the device.

After reviewing the preview output, you can deploy the policy to all of the devices in the scope, or you can continue to make changes to the policy.

Policy Precheck

When you create an application policy, you can check that it will be supported on the devices in the site scope before you deploy it. The precheck function checks that the device type, model, line cards, and software images support the application policy that you created. If any of these components are not supported, DNA Center reports a failure for the device. DNA Center also provides possible ways to correct the failures. If these remedies do not fix the failure, you can remove the device from the site scope.

If you deploy the application policy as-is, the policy will fail to deploy on the devices that reported a failure during the precheck process. To avoid the failure, you can remove the device from the site scope or update the device components to a level that the application policy supports. For a list of supported devices, see the [Cisco Digital Network Architecture Center Supported Devices](#) document.

Related Topics

[Precheck an Application Policy](#), on page 198

Policy Scheduling

After you create or change a policy, you can deploy or redeploy the policy to the devices associated with it. You can deploy or redeploy a policy immediately or at a specific date and time, for example, on a weekend during off-peak hours. You can schedule a policy deployment for wired or wireless devices.

After you have scheduled a policy to be deployed, the policy and site scope are locked. You can view the policy, but you cannot edit it. If you change your mind about deploying the policy, you can cancel it.



-
- Note** When the schedule event occurs, the policy is validated against the various policy components, for example, applications, application sets, and queuing profiles. If this validation fails, the policy changes are lost.
-

Policy Versioning

Policies are versioned. Policy versioning allows you to do the following tasks:

- Compare a previous version to the current (latest) one to see the differences.
- Display previous versions of a policy and select a version to reapply to the devices in a site scope.

Editing one version of a policy does not affect other versions of that policy or the components of the policy, such as the application sets that the policy manages. For example, deleting an application set from a policy does not delete the application set from DNA Center, other versions of that policy, or even other policies. Because policies and application sets exist independent of each other, it's possible to have a policy version that contains application sets that no longer exist. If you attempt to deploy or rollback to an older version of a policy that references an application set that no longer exists, an error occurs.



-
- Note** Policy versioning does not capture changes to applications (such as rank, port, and protocol), application set members, LAN queuing profiles, and sites.
-

Original Policy Restore

The first time that you deploy a policy to devices, DNA Center detaches the device's original Cisco Modular QoS CLI (MQC) policy configurations, but leaves them on the device. DNA Center stores the device's original NBAR configurations in DNA Center. This action allows you to restore the original MQC policies and NBAR configuration onto the devices later, if needed.



-
- Note** Because the MQC policies are not deleted from the device, if you remove these policies, you will not be able to restore them using the DNA Center original policy restore feature.
-

When you restore the original policy configuration onto a device, DNA Center removes the existing policy configuration that you deployed and reverts to the original configuration that was on the device.

Any MQC policy configurations that existed before you deployed application policies are reattached to the interfaces. However, queuing policies, such as multilayer switching (MLS) configurations, are not restored; instead, the devices retain the MLS configurations that were last applied through DNA Center.

After you restore the original policy configuration to the device, the policy that is stored in DNA Center is deleted.

Note the following additional guidelines and limitations for this feature:

- If the first attempt to deploy a policy to a device fails, DNA Center automatically attempts to restore the original policy configurations onto the devices.
- If a device is removed from an application policy after that policy has been applied to the device, the policy remains on the device. DNA Center does not automatically delete the policy or restore the QoS configuration on the device to its original (pre-DNA Center) configuration.

Stale Application Policies

An application policy can become stale if you change the configuration of something that is referenced in the policy. If an application policy becomes stale, you need to redeploy it for the changes to take affect.

An application policy can become stale for any of the following reasons:

- Change to applications referenced in an application set.
- Change to interfaces, such as SP Profile assignment, WAN sub-line rate, or WAN or LAN marking.
- Change to the Queuing profile.
- New site added under a parent site in the policy.
- Device added to a site that is referenced by the policy.
- Devices moved between sites in the same policy.

Application Policy Guidelines and Limitations

- DNAC cannot learn multiple Wireless LANs (WLANs) with the same SSID name on a Wireless Controller (WLC). At any point, DNAC will have only one entry for a WLAN with a unique name although it is possible for the WLC to contain multiple entries with the same name and different WLAN Profile Names.

You might have duplicate SSID names per WLC by design, or you might have inadvertently added a WLC with a duplicate SSID name using DNAC. In either case, having duplicate SSID names per WLC is problematic for several DNAC features:

- **Learn Config**—DNAC learns only one randomly chosen SSID name per WLC and discards any remaining duplicate SSID names. (**Learn Config** is typically used in a brownfield scenario.)
- **Application Policy**—When deploying an application policy, DNAC randomly applies the policy to only one of the duplicate SSID names and not the others. In addition, policy restore, CLI preview, EasyQoS Fastlane, and PSK override features either fail or have unexpected outcomes.

- **Multiscale Network**—In a multiscale network, multiple duplicate SSID names on multiple devices can also cause issues. For example, one device has a WLAN configured as a non-fabric SSID, and a second device has the same WLAN, but it is configured as a fabric SSID. When you perform a **Learn Config**, only one SSID name is learned. The other SSID name from the other device is discarded. This behavior can cause conflicts especially if the second device supports only fabric SSID names, but DNA Center is trying to perform operations on the device with non-fabric SSID names.
- **IPACL Policy**—When deploying an IPACL policy, DNAC randomly applies the policy to only one of the duplicate SSIDs. In addition, scenarios involving Flex Connect are also impacted.
- DNA Center does not recommend Out of Band (OOB) changes to device configurations. If you make OOB changes, the policy in DNA Center and the one configured on the device become inconsistent. The two policies remain inconsistent until you deploy the policy from DNA Center to the device again.
- The QoS trust functionality cannot be changed.

Configure Applications and Application Sets

Change an Application's Settings

You can change the application set or traffic class of an existing NBAR application.

Procedure

Step 1

From the DNA Center home page, choose **Policy > Application > Applications**.

Step 2

Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.

Step 3

Click the application name.

Step 4

In the dialog box, change one or both settings:

- **Traffic Class**—Choose a traffic class from the drop-down list. Valid traffic classes are BROADCAST_VIDEO, BULK_DATA, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, NETWORK_CONTROL, OPS_ADMIN_MGMT, REAL_TIME_INTERACTIVE, SIGNALING, TRANSACTIONAL_DATA, VOIP_TELEPHONY.
- **Application Set**—Choose an application set from the drop-down list. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, generic-tunneling, intranet-apps, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 5

Click **Save**.

Create a Server Name-Based Custom Application

If you have applications that are not in DNA Center, you can add them as custom applications.

Procedure

Step 1 From the DNA Center home page, click **Policy > Application > Applications**.

Step 2 Click **Add Application**.

Step 3 In the dialog box, complete the following fields:

Field	Description
Application name	Name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.
Type	Method by which users access the application. Choose Server Name for applications that are accessible through a server.
Server Name	Name of the server that hosts the application.
Similar To	Application with the similar traffic-handling requirements. Click the radio-button to select this option, then select an application from the drop-down field. DNA Center copies the other application's traffic class to the application that you are defining.
Traffic Class	Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
Application Set	Application set that you want the application to reside. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, generic-tunneling, intranet-apps, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 4 Click **OK**.

Create an IP Address and Port-Based Custom Application

If you have applications that are not in DNA Center, you can add them as custom applications.

Procedure

Step 1 From the DNA Center home page, click **Policy > Application > Applications**.

Step 2 Click **Add Application**.

Step 3 In the dialog box, complete the following fields:

Create a URL-Based Custom Application

Field	Description
Application name	Name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.
Type	Method by which users access the application. Choose Server IP/Port for applications that are accessible through an IP address and port.
DSCP	Differentiated Services Code Point (DSCP) value. Check the DSCP check box and define a DSCP value. If you do not define a value, the default value is Best Effort. Best-effort service is essentially the default behavior of the network device without any QoS.
IP/Port Classifiers	Classification of traffic based on IP address, protocol, and port number. Check the IP/Port Classifiers check box to define the IP address or subnet, protocol, and port or port range for an application. Valid protocols are IP, TCP, UDP, and TCP/UDP. If you select the IP protocol, you do not define a port number or range. Click to add more classifiers.
Similar To	Application with the similar traffic-handling requirements. Click the radio-button to select this option, then select an application from the drop-down field. DNA Center copies the other application's traffic class to the application that you are defining.
Traffic Class	Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
Application Set	Application set that you want the application to reside. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, generic-tunneling, intranet-apps, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

- Step 4** Click **OK**.
-

Create a URL-Based Custom Application

If you have applications that are not in DNA Center, you can add them as custom applications.

Procedure

- Step 1** From the DNA Center home page, click **Policy > Application > Applications**.

Step 2

Click **Add Application**.

Step 3

In the dialog box, complete the following fields:

Field	Description
Application name	Name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.
Type	Method by which users access the application. Choose URL for applications that are accessible through a URL.
URL	URL used to reach the application.
Similar To	Application with the similar traffic-handling requirements. Click the radio-button to select this option, then select an application from the drop-down field. DNA Center copies the other application's traffic class to the application that you are defining.
Traffic Class	Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
Application Set	Application set that you want the application to reside. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, generic-tunneling, intranet-apps, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 4

Click **OK**.

Edit or Delete a Custom Application

If you need to, you can change or delete a custom application.

**Note**

You cannot delete a custom application that is directly referenced by an application policy. Application policies typically reference application sets and not individual applications. However if a policy has special definitions for an application (such as a consumer or producer assignment or bidirectional bandwidth provisioning), the policy has a direct reference to the application. As such, you must remove the special definitions or remove the reference to the application entirely before you can delete the application.

Change the Applications in an Application Set

Procedure

-
- Step 1** From the DNA Center home page, click **Policy > Application > Applications**.
- Step 2** Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.
- Step 3** Do one of the following:
- a) To edit the application, click the application name, make your changes, and click **OK**. For information about the fields, see [Create a Server Name-Based Custom Application, on page 184](#), [Create an IP Address and Port-Based Custom Application, on page 185](#), or [Create a URL-Based Custom Application, on page 186](#).
 - b) To delete the application, click  in the application box and then click **OK** to confirm.
-

Change the Applications in an Application Set

You can move applications from one application set to another application set.

Procedure

-
- Step 1** From the DNA Center home page, click **Policy > Application > Application Sets**.
- Step 2** Use the **Search**, **Show**, or **View By** fields to locate the applications or application sets that you want to change.
- Step 3** Click the down arrow to display the applications in the set. Use the scroll bar to view all of the applications.
- Step 4** Drag and drop applications from one application set to another.

Note You can select, drag, and drop multiple applications at a time.

Create a Custom Application Set

If none of the application sets fit your needs, you can create a custom application set.

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > Application > Application Sets**.
- Step 2** Click **Add Application Set**.
- Step 3** In the dialog box, enter a name for the new application set.
DNA Center creates the new application set; however, it has no applications in it.
- Step 4** Click **OK**.
- Step 5** Use the **Search**, **Show**, or **View By** fields to locate the application set.
- Step 6** Locate the applications that you want to move into the new application set.
- Step 7** Check the check box next to the applications that you want to move.

- Step 8** Drag and drop the applications into the new application set.

Edit or Delete a Custom Application Set

If you need to, you can change or delete a custom application set.

**Note**

You cannot delete a custom application set that is referenced by an application policy. You must remove the application set from the policy before you can delete the application set.

Procedure

- Step 1** From the DNA Center **Home** page, choose **Policy > Application > Application Sets**.
- Step 2** Use the **Search**, **Show**, or **View By** fields to locate the application set that you want to change.
- Step 3** Do one of the following:
- To edit the application set, drag and drop applications into or out of the application set. Click **OK** to confirm each change.
 - To delete the application set, click in the application set box and then click **OK** to confirm.

Mark an Application as Favorite

You can mark an application as a favorite to designate that the application's QoS configuration must be deployed to devices before other applications' QoS configuration. Applications are configured system-wide, not on a per-policy basis. For more information, see [Favorite Applications, on page 175](#).

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Application > Applications**.
- Step 2** Locate the application that you want to mark as a favorite.
- Step 3** Click .

Manage Application Policies

Prerequisites

To configure QoS policies, make sure that you address the following requirements:

- DNA Center supports most of the Cisco LAN, WAN, WLAN devices. To verify whether the devices and software versions in your network are supported, see the *Cisco Digital Network Architecture Center Supported Devices* document.

Create an Application Policy

- Make sure that your Cisco network devices, such as the ISR-G2, the ASR 1000, and Wireless LAN Controller, have the AVC (Application Visibility and Control) feature license installed. For information, see the *NBAR2 (Next Generation NBAR) Protocol Pack FAQ* at the following URL: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/network-based-application-recognition-nbar/qa_C67-723689.html.
- For DNA Center to identify the WAN interfaces that need policies, you must specify the interface type (WAN) and (optionally) its subline rate and service-provider Class-of-Service model. For more information, see [Assign a Service Provider Profile to a WAN Interface, on page 202](#).
- Verify that the device roles that were assigned to devices during the discovery process are appropriate for your network. If necessary, change any of the device roles that are not appropriate. For more information, see [Change Device Role \(Inventory\), on page 71](#).

Create an Application Policy

Before you begin

- Define your business objectives. For example, your business objective might be to improve user productivity by minimizing network response times or to identify and deprioritize non-business applications. Based on these objectives, decide which business relevance category your applications fall into.
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.
- Verify that the device roles that were assigned to devices during the discovery process are appropriate for your network. If necessary, change any of the device roles that are not appropriate. For more information, see [Change Device Role \(Inventory\), on page 71](#).
- Add devices to sites. For more information, see [Add Devices to Sites, on page 211](#).
- If you have applications that are not defined in DNA Center, you can add them and define their QoS attributes. For more information, see [Custom Applications, on page 174](#).
- If you plan to configure this policy with a service provider profile for traffic that is destined for a service provider, make sure that you have configured a SP Profile. After creating the application policy, you can return to the SP Profile and customize its SLA attributes and assign the SP Profile to WAN interfaces. For more information, see [Configure Service Provider Profiles, on page 134](#).
- If you want some applications configured before others on devices, mark these applications as favorites. For more information, see [Mark an Application as Favorite, on page 189](#).

Procedure

Step 1 From the DNA Center home page, choose **Policy > Application > Application Policies**.

Step 2 Click **Add Policy**.

Step 3 In the **Application Policy Name** field, enter a name for the policy.

Step 4 Select the **Wired** or **Wireless** radio button.

Step 5 Click **Site Scope** and click the check box next to the sites where you want to deploy the policy.

Note For policies of wired devices, you cannot select a site that is already assigned to another policy. For policies of wireless devices, you cannot select a site that is already assigned to another policy with the same SSID.

Step 6 For policies of wired devices, you can exclude devices or specific interfaces from being configured with the policy.

- a) From the **Site Scope** pane, click  next to the site you are interested in.
A list of devices in the selected scope is displayed.
- b) Locate the device that you want to exclude and click the toggle button in the corresponding **Policy Exclusions** column.
- c) To exclude specific interfaces, click **Exclude Interfaces** and .
- d) From the list of interfaces, click the toggle button in the **Exclude from Policy** column next to the interfaces that you want to exclude.
- e) Click < **Back to Devices in Site-Name**.
- f) Click < **Back to Site Scope**.

Step 7 For WAN devices, you can configure specific interfaces.

- a) From the **Site Scope** pane, click  next to the site you are interested in.
- b) From the list of devices in the site, click **Configure** in the **SP Profile Settings** column next to the device you are interested in.

Note This option is only available for routers.

- c) In the **WAN Interface** column, click the **Select Interface** drop-down field and choose an interface.
- d) In the **Role** column, click the **Select Role** drop-down field and choose a role according to the type of interface you are configuring:
 - **Physical interface**—Choose **WAN**. This role is the only valid role for a physical interface.
 - **Tunnel interface**—Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.

Note Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.

- e) In the **Service Provider Profile** column, click the **Select Profile** drop-down field and choose an SP profile.
- f) (Optional) If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.
- g) (Optional) To configure additional WAN interfaces, click + and repeat Step c through Step f.
- h) Click **Save**.
- i) Click < **Back to Site Scope**.

Step 8 From the **Site Scope** pane, click **OK**.

Step 9 (Optional) If the Cisco Validated Design (CVD) queuing profile (CVD_QUEUEING_PROFILE) does not meet your needs, create a custom queuing profile.

- a) Click **Queuing Profiles**.
- b) Select a queuing profile from the list in the left pane.
- c) Click **Select**.

- Step 10** (Optional) If this policy is for traffic that is destined for a service provider, customize the service provider profile SLA attributes.
- Click **SP Profile**.
 - Choose a SP profile.
 - Customize the SLA attributes (**DSCP**, **SP Bandwidth %**, and **Queueing Bandwidth %**).
- Step 11** (Optional) Configure the business relevance of the application sets used in your network.
- DNA Center comes with application sets that are preconfigured into business-relevancy groups. You can keep this configuration or modify it by dragging and dropping an application set from one business-relevancy group to another.
- Step 12** (Optional) Customize applications by creating consumers and assigning them to applications or by marking an application as bidirectional.
- Expand the application group.
 - Click the gear icon  next to the application that you are interested in.
 - From the **Traffic Direction** field, select the **Unidirectional** or **Bi-directional** radio button.
 - To choose an existing consumer, click the **Consumer** field and choose the consumer that you want to configure. To create a new consumer, click **+ Add Consumer** and define the **Consumer Name**, **IP/Subnet**, **Protocol**, and **Port/Range**.
 - Click **OK**.
- Step 13** Configure host tracking. Click the **Host Tracking** toggle to turn host tracking on or off.
- When deploying an application policy, DNA Center automatically applies Access Control List (ACL) entries (ACEs) to the switches to which collaboration end points (such as telepresence units or Cisco phones) are connected.
- The ACE matches voice and video traffic generated by the collaboration end point, ensuring that the voice and video traffic are correctly marked.
- When host tracking is turned on, DNA Center tracks the connectivity of the collaboration end points within the site-scope and to automatically reconfigure the ACL entries when the collaboration end points connect to the network or move from one interface to another.
- When host tracking is turned off, DNA Center does not automatically deploy policies to the devices when a collaboration end point moves or connects to a new interface. Instead, you need to redeploy the policy for the ACLs to be configured correctly for the collaboration end points.
- Step 14** (Optional) Preview the CLI commands that will be sent to devices. For more information, see [Preview an Application Policy, on page 197](#).
- Step 15** (Optional) Precheck the devices on which you plan to deploy the policy. For more information, see [Precheck an Application Policy, on page 198](#).
- Step 16** Do one of the following tasks:
- Save the policy as a draft by clicking **Save Draft**. For more information, see [Policy Drafts, on page 180](#).
 - Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.
- To deploy the policy now, click the **Now** radio button and click **Apply**.
- To schedule the policy deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment. For more information, see [Policy Scheduling, on page 182](#).

Note The site time zone setting is not supported for scheduling application policy deployments.

Related Topics

[Queuing Profiles](#), on page 177

[Service Provider Profiles](#), on page 175

[Business-Relevance Groups](#), on page 170

View Application Policy Information

You can display various information about application policies that you have created and deployed.

Before you begin

You must deploy at least one application policy

Procedure

Step 1 From the DNA Center home page, choose **Policy > Application > Application Policies**.

Step 2 Sort the policies by name or filter them by name, status, or queuing profile.

Step 3 View the list of policies and the following information about each:

- **Policy Name**—Name of the policy.
- **Version**—Iteration of the policy. Each time a policy is deployed or saved as a draft, it is incremented by one version. For example, you create a policy and deploy it. The policy is at version 1. If you change the policy and deploy it again, the version of the policy is incremented to version 2. For more information, see [Policy Drafts](#), on page 180 and [Policy Versioning](#), on page 182
- **Policy Status**—State of the policy.
- **Deployment Status**—State of the last deployment (per device). Presents a summary of the following
 - Devices that were successfully provisioned
 - Devices that failed to be provisioned
 - Devices that were not provisioned due to the deployment being aborted.

Clicking the state of the last deployment displays the policy deployment window, which provides a filterable list of the devices on which the policy was deployed. For each device, the following information is displayed:

- Device details (name, site, type , role, and IP address)
- Success deployment status. Clicking on the gear icon next to the status displays the details of the effective marking policy that was deployed to the device. For devices that have limited TCAM resources or an old NBAR protocol pack, only a subset of the applications that are included in the policy can be provisioned, and they are shown in the view.
- Failure status shows the reason for the failure.

- **Scope**—Number of sites (not devices) that are assigned to the policy. For policies of wireless devices, the name of the SSID to which the policy applies is included.
 - **LAN Queuing Profile**—Name of the LAN queuing profile that is assigned to the policy.
-

Edit an Application Policy

You can edit an application policy.

Before you begin

You must have created at least one policy.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Application > Application Policies**.
- Step 2** Use the **Filter** field to locate the policy that you want to edit.
- Step 3** Click the radio button next to the policy.
- Step 4** From the **Actions** drop-down list, choose **Edit**.
- Step 5** Make changes to the application policy as needed. For information about the application policy settings, see [Create an Application Policy, on page 190](#).
- Step 6** Do one of the following tasks:
 - Save the policy as a draft by clicking **Save Draft**. For more information, see [Policy Drafts, on page 180](#).
 - Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.
To deploy the policy now, click the **Run Now** radio button and click **Apply**.
To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see [Policy Scheduling, on page 182](#).

Note The site time zone setting is not supported for scheduling application policy deployments.

Save a Draft of an Application Policy

When creating, editing, or cloning a policy, you can save it as a draft so that you can continue to modify it later. You can also make changes to a deployed policy and save it as a draft.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Application > Application Policies**.
- Step 2** Create, edit, or clone a policy.
- Step 3** Click **Save Draft**.

For more information, see [Policy Drafts, on page 180](#).

Deploy an Application Policy

If you make changes that affect a policy's configuration, such as adding a new application or marking an application as a favorite, you need to redeploy the policy to implement these changes.

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > Application > Application Policies**.
- Step 2** Use the **Filter** field to locate the policy that you want to deploy.
- Step 3** Click the radio button next to the policy that you want to deploy.
- Step 4** From the **Actions** drop-down list, choose **Deploy**.
You are prompted to deploy your policy now or to schedule it for a later time.
- Step 5** Do one of the following:
- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
 - To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.
- Note** The site time zone setting is not supported for scheduling application policy deployments.

Cancel a Policy Deployment

After you click **Deploy**, DNA Center begins to configure the policy on the devices in the site scope. If you realize that you have made a mistake, you can cancel the policy deployment.

The policy configuration process is performed as a bulk process in that it configures 40 devices at a time. So, if you have fewer than 40 devices, canceling the process has no real effect. However, if you have hundreds of devices, canceling the policy deployment can be useful when needed.

When you click **Abort**, DNA Center cancels the configuration process on devices that have not started to be configured and changes the device status to **Policy Aborted**. DNA Center does not cancel the deployments that are in the process of being completed or have been completed. These devices retain the updated policy configuration and reflect the state of the policy configuration, whether it is configuring, successful, or failed.

Procedure

During a policy deployment, click **Abort** to cancel the policy configuration process.

Delete an Application Policy

You can delete an application policy if it is no longer needed.

Procedure

- Step 1** From the DNA Center home page, click **Policy > Application > Application Policies**.
 - Step 2** Use the **Filter** field to locate the policy that you want to delete.
 - Step 3** Click the radio button next to the policy that you want to delete.
 - Step 4** From the **Actions** drop-down list, choose **Delete**.
 - Step 5** To confirm the deletion, click **Ok**. Otherwise, click **Cancel**.
 - Step 6** When the deletion confirmation message appears, click **Ok** again.
-

Clone an Application Policy

If an existing application policy has most of the settings that you want in a new policy, you can save time by cloning the existing policy, changing it, and then deploying it to a different scope.

Before you begin

You must have created at least one policy.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Application > Application Policies**.
 - Step 2** Use the **Filter** field to locate the policy that you want to clone.
 - Step 3** Click the radio button next to the policy that you want to clone.
 - Step 4** From the **Actions** drop-down list, choose **Clone**.
 - Step 5** Configure the application policy as needed. For information about the application policy settings, see [Create an Application Policy, on page 190](#).
 - Step 6** Do one of the following tasks:
 - Save the policy as a draft by clicking **Save Draft**. For more information, see [Policy Drafts, on page 180](#).
 - Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.
 - To deploy the policy now, click the **Run Now** radio button and click **Apply**.
 - To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see [Policy Scheduling, on page 182](#).
- Note** The site time zone setting is not supported for scheduling application policy deployments.
-

Restore an Application Policy

If you create or make changes to a policy and then decide that you want to start over, you can restore the original QoS configuration that was on the device before you configured it using DNA Center.

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > Application > Application Policies**.
- Step 2** Use the **Filter** field to locate the policy that you want to reset.
- Step 3** Click the radio button next to the policy.
- Step 4** From the **Actions** drop-down list, choose **Restore**.
- Step 5** Click **OK** to confirm the change or **Cancel** to abort it.
-

Reset the Default CVD Application Policy

The Cisco Validated Design (CVD) configuration is the default configuration for applications. If you create or make changes to a policy and then decide that you want to start over, you can reset the applications to the Cisco Validated Design (CVD) configuration. For more information about the CVD configuration, see [Application Policies, on page 169](#).

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > Application > Application Policies**.
- Step 2** Use the **Filter** field to locate the policy that you want to reset.
- Step 3** Click the radio button next to the policy.
- Step 4** From the **Actions** drop-down list, choose **Edit**.
- Step 5** Click **Reset to Cisco Validated Design**.
- Step 6** Click **OK** to confirm the change or **Cancel** to abort it.
- Step 7** Do one of the following tasks:
- To save a draft of the policy, click **Save Draft**.
 - To deploy the policy, click **Deploy**.
-

Preview an Application Policy

Before you deploy a policy, you can generate the CLI that will be applied to a device and preview the configuration.

Procedure

-
- Step 1** From the DNA Center home page, click **Policy > Application > Application Policies**.
- Step 2** Create or edit a policy, as described in [Create an Application Policy, on page 190](#) or [Edit an Application Policy, on page 194](#).
- Step 3** Before deploying the policy, click **Preview**.
A list of the devices in the scope appears.
- Step 4** Next to the device that you are interested in, click **Generate**.

Precheck an Application Policy

DNA Center generates the CLIs for the policy.

- Step 5** Click **View** to view the CLIs or copy them to the clipboard.

Related Topics

[Policy Preview](#), on page 181

Precheck an Application Policy

Before you deploy an application policy, you can check whether the devices in the site scope are supported. The precheck process includes validating a device's model, line cards, and software image.

Procedure

- Step 1** From the DNA Center home page, click **Policy > Application > Application Policies**.

- Step 2** Create or edit a policy, as described in [Create an Application Policy](#), on page 190 or [Edit an Application Policy](#), on page 194.

- Step 3** Before deploying the policy, click **Preview**.

A list of the devices in the scope appears.

- Step 4** Click **Pre-check**.

DNA Center checks the devices and reports any failures in the **Pre-Check Result** column. You can still deploy the policy even if there are failures reported on some devices. To resolve the failures, you need to bring the devices into compliance with the specifications listed in the [Cisco Digital Network Architecture Center Supported Devices](#).

Related Topics

[Policy Precheck](#), on page 181

Display Application Policy History

You can display the version history of an application policy. The version history includes the series number (iteration) of the policy and the date and time that the version was saved.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Application > Application Policies**.

- Step 2** Click the radio button next to the policy that interests you.

- Step 3** From the **Actions** drop-down list, choose **History**.

- Step 4** From the **Policy History** dialog box, you can do the following:

- To compare a version with the current version, click **Difference** next to the version that interests you.
- To roll back to a previous version of the policy, click **Rollback** next to the version that you want to roll back to.

Roll Back to a Previous Policy Version

If you change a policy configuration, and then realize that it is incorrect, or it is not having the desired affect in your network, you can revert to a policy that is up to five versions back.

Before you begin

You must have created at least two versions of the policy to roll back to a previous policy version.

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > Application > Application Policies**.
- Step 2** Click the radio button next to the policy that interests you.
- Step 3** From the **Actions** drop-down list, choose **Show History**.
Previous versions of the selected policy are listed in descending order with the newest version (highest number) at the top of the list and the oldest version (lowest number) at the bottom.
- Step 4** (Optional) To view the differences between the selected version and the latest version of a policy, click **Difference** in the **View** column.
- Step 5** When you determine the policy version that you want to rollback to, click **Rollback** for that policy version.
Note If the selected site scope changed between policy versions, the rollback is not done on the current (latest) selected site. Only the policy content is rolled back.
- Step 6** Click **Ok** to confirm the rollback procedure.
The rolled back version becomes the newest version.
-

Manage Queuing Profiles

Create a Queuing Profile

DNA Center provides a default Cisco Validated Design (CVD) queuing profile (CVD_QUEUEING_PROFILE). If this queuing profile does not meet your needs, you can create a custom queuing profile.

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > Application > Queuing Profile**.
- Step 2** Click **Add Profile**.
- Step 3** In the **Profile Name** field, enter a name for the profile.
- Step 4** Configure the bandwidth for each traffic class by using the slider, clicking the plus (+) or minus (-) sign, or entering a specific number in the field.

The number indicates the percentage of the total interface bandwidth that will be dedicated to the selected application class. Because the total bandwidth equals 100, adding bandwidth to one application class subtracts bandwidth from another application class.

Edit or Delete a Queuing Profile

An open lock icon indicates that you can edit the bandwidth for the application class. A closed lock indicates that you cannot edit it.

If you make a mistake, you can return to the Cisco Validated Design (CVD) settings by clicking **Reset to Cisco Validated Design**.

The graph in the middle helps you visualize the amount of bandwidth that you are setting for each application class.

Step 5 (For advanced users) To customize the DSCP code points that DNA Center uses for each of the traffic classes, in the **Show** drop-down list, choose **DSCP Values** and configure the value for each application class by clicking the field next to each and entering a specific number in the field.

To customize DSCP code points required within a service provider cloud, configure a service provider profile.

Step 6 Click **Save**.

Related Topics

[Queuing Profiles](#), on page 177

[Marking, Queuing, and Dropping Treatments](#), on page 172

[Customize Service Provider Profile SLA Attributes](#), on page 200

Edit or Delete a Queuing Profile**Procedure**

Step 1 From the DNA Center home page, choose **Policy > Application > Queuing Profile**.

Step 2 From the **Queuing Profile** pane, click the radio button next to the queuing profile that you want to edit or delete.

Step 3 Do one of the following tasks:

- To edit the application set, change any of the field values except the profile name and click **Save**. For information about the fields, see [Create a Queuing Profile](#), on page 199.
- To delete the profile, click **Delete**.

Note You cannot delete a queuing profile if it is referenced in an application policy.

Related Topics

[Queuing Profiles](#), on page 177

[Marking, Queuing, and Dropping Treatments](#), on page 172

Manage Application Policies for WAN Interfaces**Customize Service Provider Profile SLA Attributes**

If you do not want to use the default SLA attributes assigned to your SP profile by its class model, you can customize the SP Profile SLA attributes to fit your requirements. For more information about the default SP Profile SLA Attributes see [Service Provider Profiles](#), on page 175.

**Note**

After creating your custom SP profile, you need to configure the WAN interfaces with the SP profile. For information, see [Configure Service Provider Profiles on WAN Interfaces](#).

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, choose **Policy > Application > Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to change.

Step 3 Select the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Click **SP Profiles** and select a SP profile.

Step 6 You can modify the information in the following fields:

- **DSCP**—Differentiated Services Code Point (DSCP) value. Valid values are from 0 to 63.

- Expedited Forwarding (EF)
- Class Selector (CS)—CS1, CS2, CS3, CS4, CS5, CS6
- Assured Forwarding—AF11, AF21, AF41
- Default Forwarding (DF)

For more information about these DSCP values, see [Marking, Queuing, and Dropping Treatments, on page 172](#).

- **SP Bandwidth %**—Percentage of bandwidth allocated to a specific class of service.

- **Queuing Bandwidth %**—Percentage of bandwidth allocated to each of the traffic classes. You can make one of the following changes:

- To customize the queuing bandwidth, unlock the bandwidth settings by clicking the lock icon and adjust the bandwidth percentages.
- To calculate the queuing bandwidth automatically from the SP bandwidth, lock the queuing bandwidth settings by clicking the lock icon and then clicking **OK** to confirm. By default, DNA Center automatically distributes the queuing bandwidth percentage such that the sum of the queuing bandwidth for all of the traffic classes in a SP class aligns with the SP bandwidth percentage of that class.

Step 7 Click **OK**.

Assign a Service Provider Profile to a WAN Interface

If you have already created an application policy and now want to assign SP profiles to WAN interfaces, you can edit the policy and perform this configuration, including setting the subline rate on the interface, if needed.

Before you begin

If you have not created the policy, you can create the policy and assign SP profiles to WAN interfaces at the same time. For more information, see [Create an Application Policy, on page 190](#).

Procedure

- Step 1** From the DNA Center home page, click **Policy > Application > Application Policies**.
- Step 2** Use the **Filter** field to locate the policy that you want to edit.
- Step 3** Click the radio button next to the policy.
- Step 4** From the **Actions** drop-down list, choose **Edit**.
- Step 5** From the **Site Scopepane**, click  next to the site you are interested in.
- Step 6** From the list of devices in the site, click **Configure** in the **SP Profile Settings** column for the device you are interested in.
- Step 7** In the **WAN Interface** column, click the **Select Interface** drop-down field and choose an interface.
- Step 8** In the **Role** column, click the **Select Role** drop-down field and choose a role according to the type of interface you are configuring:
 - **Physical interface**—Choose **WAN**. This role is the only valid role for a physical interface.
 - **Tunnel interface**—Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.

Note Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.
- Step 9** In the **Service Provider Profile** column, click the **Select Profile** drop-down field and choose an SP profile.
- Step 10** If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.
- Step 11** To configure additional WAN interfaces, click **+** and repeat Step 7 through Step 10.
- Step 12** Click **Save**.
- Step 13** Click **< Back to Site Scope**.
- Step 14** Click **OK**.
- Step 15** Click **Deploy**.
- You are prompted to deploy your policy now or to schedule it for a later time.
- Step 16** Do one of the following:
 - To deploy the policy now, click the **Run Now** radio button and click **Apply**.
 - To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.

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 on a device that will receive, process, and analyze the ERSPAN data. The device is typically a packet capture or network analysis tool that receives a copy of the traffic flow for analysis.



Note 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.

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.

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.

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 [#unique_264](#).
- 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 165](#).

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 205 .
Step 2	Create a traffic copy contract. The contract defines the copy destination.	For information, see Create a Traffic Copy Contract, on page 205 .
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 206 .

Create a Traffic Copy Destination

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Traffic Copy > 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 > Traffic Copy > 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 > Traffic Copy > 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 205](#)
- Step 5** Click **Save**.
-

Edit or Delete a Traffic Copy Contract

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > Traffic Copy > 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, choose **Policy > Traffic Copy > 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 > Traffic Copy > 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**.
-

Virtual Networks

Virtual networks are isolated routing and switching environments. You can use virtual networks to segment your physical network into multiple logical networks.

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.

A typical use case is building management, where the user community needs to be segmented from building systems, such as lighting; heating, ventilation, and air conditioning (HVAC) systems; and security systems. In this case, you segment the user community and the building systems into two or more virtual networks to block unauthorized access of the building systems.

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

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 guidelines and limitations:

- You can create only one guest virtual network.
- VRFs are common across all domains. The maximum number of VRFs is based on the device with the fewest VRFs in the domain.

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:

Table 51: Virtual Network Fields

Field	Description
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.

Related Topics

[Edit or Delete a Virtual Network](#), on page 208

[Guidelines and Limitations for Virtual Networks](#), on page 207

[Virtual Networks](#), on page 207

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:

- To edit the virtual network, click the name of the virtual network from the left navigation pane and modify the information in any of the fields in the following table, except the virtual network name:

Table 52: Virtual Network Fields

Field	Description
Network Name	Name of the virtual network. (Cannot be modified.)
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.

Field	Description
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.

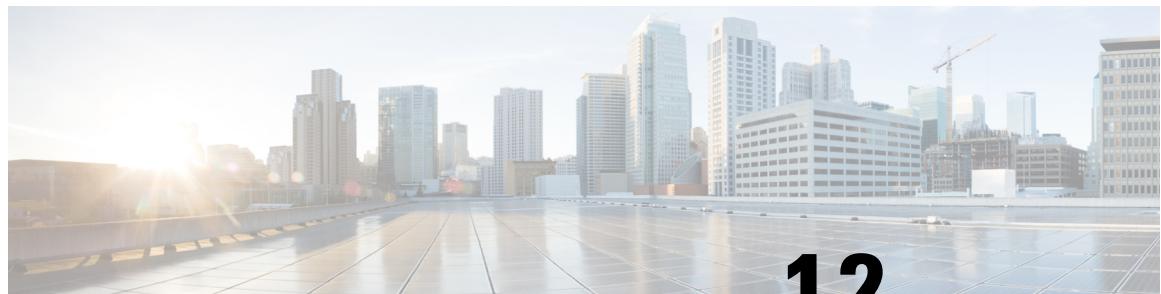
- To delete the virtual network, click  and confirm the deletion.

Related Topics

[Create a Virtual Network](#), on page 207

[Guidelines and Limitations for Virtual Networks](#), on page 207

[Virtual Networks](#), on page 207



CHAPTER 12

Provision Your Network

- Provisioning, on page 211
- Add Devices to Sites, on page 211
- Provisioning Devices, on page 212
- Check the LAN Automation Status, on page 220
- Delete Devices After Provisioning, on page 221
- Multi-Site Fabric Domain, on page 221
- Transit Networks, on page 221
- Configuring Fabric Domains, on page 223

Provisioning

After you have configured policies for your network in DNA Center, you can provision your devices. In this stage, you deploy the policies across your devices.

There are 3 aspects of provisioning the devices:

- Assign devices to the inventory and deploy the required settings and policies.
- Add devices to 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 that you have defined the following global network settings before provisioning a Cisco WLC:
 - Network servers, such as AAA, DHCP, and DNS. For more information, see [Configure Global Network Servers, on page 134](#).
 - Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see [Configure CLI Credentials, on page 128](#), [Configure SNMPv2c Credentials, on page 129](#), [Configure SNMPv3 Credentials, on page 130](#), and [Configure HTTPS Credentials, on page 132](#).
 - IP address pools. For more information, see [Configure IP Address Pools, on page 133](#).
 - Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles. For more information, see [Configure Global Wireless Settings, on page 113](#).
- Make sure that you have Cisco WLC in your inventory. If not, discover Cisco WLC using the Discovery function. For more information, see [Discover Your Network, on page 7](#).
- Make sure that Cisco WLC is added to a site. For more information, see [Add Devices to Sites, on page 211](#).

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 Cisco WLCs are listed.

Step 3 Check the check box adjacent the controller device name that you want to provision.

Step 4 From the **Action** drop-down list, choose **Provision**.

Step 5 The **Assign Site** window appears. Assign a site for the controller.

Step 6 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 7 Click **Next**.

The **Configuration** window appears.

Step 8 Select a role for Cisco WLC: **Active Main WLC** or **Guest Anchor**.

- Step 9** In the **Managed AP Locations** field, enter the AP locations managed by the controller. Here you have the option to change, remove, or reassign the site.
Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that particular site. One site can be managed by only one WLC.
- Step 10** For Active Main WLC, you can configure the following
- Step 11** If you have selected the **WLC Role** as **Active Main WLC**, under **Interface and VLAN Configuration**, click **+ Add** and configure the interface and the VLAN.
- Step 12** In the **Configure Interface and VLAN** window, configure the following:
- Step 13** From the **Interface Name** drop-down list, select the interface name.
- Step 14** Enter the **VLAN ID**.
- Step 15** Enter the **Interface IP Address**.
- Step 16** Enter the **Interface Net Mask (in bits)**.
- Step 17** Enter the gateway **Gateway IP Address**.
- Step 18** Enter the **LAG/Port Number**.
- Step 19** Click **OK**.
- Step 20** For a guest anchor WLC, you can change the VLAN ID configuration by changing the **VLAN ID** under **Assign Guest SSIDs to DMZ site**.
- Step 21** Click **Next**.
- Step 22** The **Summary** window displays the following information:
- **System Details**
 - **Global Setting**
 - **SSID**
 - **Managed Sites**
 - **Interfaces**
- Step 23** 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 224](#).
2. Configure settings for the various kinds of devices (hosts) that can access the fabric domain. See [Configure Host Onboarding](#).

Onboard APs with Zero Touch Provisioning - Day 0 Provisioning

Follow this workflow for Zero Touch Provisioning of APs.

Before you begin

- Design network hierarchy, with sites, buildings, floors, and so on. For more information, see the [Create Sites in the Network Hierarchy, on page 92](#), [Add Buildings, on page 95](#), and [Add Floors to Buildings, on page 96](#).
- Create a network profile. For more information, see the [Create a Wireless Sensor Device Profile, on page 122](#).
- Provision a Cisco WLC. For more information, see the [Provision a Cisco WLC, on page 212](#).
- Configure a DHCP server, with Option #43 or Option #60, which is the DNAC PnP server's IP address. This helps the AP to contact PnP server to download configurations. For more information, see the [About Global Network Settings, on page 125](#).
- APs should be in the factory reset state without any WLC configurations.

Procedure

Step 1 The AP that is connected to a switch contacts the DHCP server and connect to a PnP server.

Step 2 The DHCP server allocates IP address with Option #43, which is the DNAC PnP server's IP address.

Step 3 The AP starts the PnP agent and contacts the PnP server.

Step 4 Find the AP on the **DNAC > Provision > Unclaimed Devices** tab.

The **Device Status** shows as **Unclaimed**.

Step 5 Claim the device:

- Check the check box adjacent to the AP device name, and click **Claim Device**.
- Enter a **Device Name**.
- From the **Choose a site** drop-down list, select a site for the AP.
- By default, the customer RF profile that you marked as default under **Network Settings > Wireless > Wireless Radio Frequency Profile** is selected in the **Choose a RF Profile** drop-down list. You can change the default RF Profile value for an AP by selecting a value from the **Choose a RF Profile** drop-down list. The options are: **High**, **Typical**, and **Low**. The AP group is created based on the RF profile selected.
- Click **Apply**.

Step 6 The AP gets the PnP configurations with WLC details and joins Cisco WLC successfully. At this stage, the **Onboarding Status** on the **Provision > Unclaimed** of the AP will be **Executed Workflow** and the **Device Status** under **Provision > Unclaimed Device** page will be **Onboarding**.

Step 7 Once the AP is provisioned, the **Provision Status** on the **Device Inventory > Inventory** page changes to **Success** and the **Onboarding Status** on the **Provision > Unclaimed** will be **Executed Workflow**.

Provision a Cisco AP—Day 1 AP Provisioning

Before you begin

Make sure that you have Cisco AP in your inventory. If you do not, discover APs using the Discovery function. See [Discover Your Network, on page 7](#).

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 adjacent the AP device name that you want to provision.
- Step 4** From the **Action** drop-down list, choose **Provision**.
- Step 5** The **Assign Site** window appears. Assign an AP to the site .
- Step 6** 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 7** Click **Next**.
The **Configuration** window appears.
- Step 8** By default, the customer RF profile that you is marked as default under **Network Settings > Wireless > Wireless Radio Frequency Profile** is selected in the RF Profile drop-down list . You can change the default RF Profile value for an AP by selecting a value from the **RF Profile** drop-down list. The options are:**High**, **Typical**, and **Low**. The AP group is created based on the RF profile selected.
- Step 9** Click **Deploy** to provision the AP.
You are prompted with message stating that creation/modification of an AP group in progress.
- Note** After completion, these devices will get rebooted.
- Step 10** Click **OK**.
The **Status** column in the **Device Inventory** window shows **SUCCESS** if a deployment is successful.
-

Provision a Brownfield Device

Before you begin

With Cisco DNA Center, you can add and provision brownfield devices such as Cisco WLC to the network. Brownfield refers to devices that belong to existing sites with pre-existing infrastructure.

- Start by running a discovery on the device. After running a discovery, all your devices are displayed on the Inventory page. For more information, see [Discover Your Network, on page 7](#), and [About Inventory, on page 55](#).

- Cisco WLC is reachable and in managed state and is on the Inventory page. For more information, see [About Inventory, on page 55](#).

Procedure

- Step 1** From the DNA Center home page, choose **Provision > Devices**.
The **Device Inventory** window appears.
- Step 2** Click the **Inventory** tab.
All the discovered Cisco WLCs are listed.
- Step 3** Click **Filter** and enter the appropriate values in the selected filter field. For example, for the **Device Name** filter, enter the name of the device.
The data that is displayed in the **Devices** table is automatically updated according to your filter selection.
- Step 4** Check the check box adjacent the controller device name that you want to provision.
- Step 5** From the **Action** drop-down list, choose **Learn Device Config**.
- Step 6** The **Assign Site** window appears. Assign a site for the controller.
- Step 7** From the **Choose a site** drop-down list, select the site to which you want to associate the controller.
- Step 8** Click **Next**.
- Step 9** On the **Learnt Configurations** window, all the learned configurations are listed.
- Click **Network** in the left pane. The right pane displays configurations that were learned as part of device configuration learning. It shows:
 - **AAA Server** details, which were learned as part of the device learning.
 - **Systems Settings**, with details about IP address and protocol of the AAA server. Enter the **Shared Secret** for the AAA server.
 - Click **Wireless** in the left pane. The right pane lists all the enterprise and guest SSIDs that are present on the device. For an SSID with a preshared key (PSK), you must provide the **passphrase key**.
 - Click **Discarded Config** in the left pane. The right pane lists the conflicting or the existing configurations on the DNA Center. The discarded config entries are categorized as:
 - Duplicate design entity
 - Unknown device configuration for Radio Policy
 - Threshold entities
- Step 10** Click **Next**.
The **Network Profile** window appears.
- Step 11** The **Network Profile** window lists network profile or site profile created based on the AP and WLAN combination.
- Step 12** Click **Save**.
A message saying "Brownfield Configuration is Successful" is displayed.

- Step 13** Choose **Design > Network Profiles**, to assign a site to the network profile.
- Step 14** On the **Network Profiles** page, click **Assign Site** to add sites to the selected profile.
- Step 15** In the **Add Sites to Profile** window, select a site from the drop-down list, and click **Save**.
- Step 16** Click the **Provision** tab.
- Step 17** Click **Filter** and enter the appropriate values in the selected filter field.
The data that is displayed in the **Devices** table is automatically updated according to your filter selection.
- Step 18** Check the check box adjacent the controller device name that you want to provision.
- Step 19** From the **Action** drop-down list, choose **Provision**.
- Step 20** Review details on the **Assign Site** window, and click **Next**.
The **Configurations** window appears.
- Step 21** Under **Interface and VLAN Configuration**, click **+Add** to configure interface and VLAN details.
- Step 22** On the **Configure Interface and VLAN** window, configure the required fields, and click **OK**.
- Step 23** Click **Next**.
- Step 24** The **Summary** window displays the following information:
- **Device Details**
 - **Network Settings**
 - **SSID**
 - **Managed Sites**
 - **Interfaces**
- Step 25** Click **Deploy** to provision the device.
The **Provision Status** column in the **Device Inventory** window shows **SUCCESS** after a successful deployment.

Guest Anchor Configuration and Provisioning

Follow these steps to configure a guest anchor WLC:

Procedure

- Step 1** Design network hierarchy, with sites, buildings, floors, and so on. For more information, see [Create Sites in the Network Hierarchy, on page 92](#), [Add Buildings, on page 95](#), and [Add Floors to Buildings, on page 96](#).
- Step 2** Network servers, such as AAA, DHCP, and DNS servers. For more information, see [Configure Global Network Servers, on page 134](#) and [Add AAA Server, on page 135](#).
- Step 3** Create SSIDs for guest wireless network with external web authentication and central web authentication with Cisco ISE. For more information, see [Creating SSIDs for a Guest Wireless Network, on page 115](#).
- Step 4** Discover Cisco WLC using the Cisco Discovery Protocol (CDP) or an IP address range and ensure that the devices are in Inventory and should be in the managed state. For more information, see [About Discovery, on page 7](#).
- Step 5** Provision foreign Cisco WLC as the active main WLC. See [Provision a Cisco WLC, on page 212](#).

- Step 6** Select the role for Cisco WLC as guest anchor and provision the guest anchor controllers. For more information, see [Provision a Cisco WLC, on page 212](#).
- Step 7** Device credentials such as CLI, SNMP, HTTP, and HTTPS credentials—See [Configure CLI Credentials, on page 128](#), [Configure SNMPv2c Credentials, on page 129](#), [Configure SNMPv3 Credentials, on page 130](#), and [Configure HTTPS Credentials, on page 132](#).
-

Provision a Sensor Device

Provisioning a sensor device is applicable for Cisco Aironet 1800s Active Sensors.

Before you begin

- Make sure you have the sensor device in your inventory in an UNCLAIMED state.
- Make sure you have created a profile for the sensor device. See [Create a Wireless Sensor Device Profile, on page 122](#).
- In DHCP server, make sure to configure the NTP server (option #42) and the vendor-specific option #43 with ascii value "5A1D;B2;K4;I172.23.104.31;J80".

Procedure

- Step 1** From the DNA Center home page, choose **Provision > Devices**.
The **Device Inventory** window appears.
- Step 2** Click the **Unclaimed Devices** tab. All the unclaimed devices are displayed.
- Step 3** Check the check box(es) adjacent to the sensor device that you want to provision.
Three tabs appear above the list of unclaimed devices.
- Step 4** Click the **Sensor Provision** tab.
The **Sensor Provision** window appears providing the serial number and device information.
- Step 5** From the **Sensor Select SSID Profile** drop-down list, choose the profile name to associate to the sensor device.
- Step 6** Click **Assign**.
Provisioning starts and the sensor device appears in the device inventory.
If the provisioning is successful, the **Provision Status** column in the **Device Inventory** window shows **Success**.
-

Provision LAN Underlay

Use LAN automation to provision a LAN underlay.

Before you begin

- Configure your network hierarchy. (See [Add Devices to Sites, on page 211](#).)

- Make sure you have defined the following global network settings:
 - Network servers, such as AAA, DHCP, and DNS Servers—(See [Configure Global Network Servers, on page 134](#).)
 - Device credentials such as CLI, SNMP, HTTP, and HTTPS credentials—(See [Configure CLI Credentials, on page 128](#), [Configure SNMPv2c Credentials, on page 129](#), [Configure SNMPv3 Credentials, on page 130](#), and [Configure HTTPS Credentials, on page 132](#).)
 - IP address pools—(See [Configure IP Address Pools, on page 133](#).)
- Make sure that you have at least one device in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 Reserve an IP address pool for the site that you will be provisioning.

Note The size of the LAN Automation pool must be /25 or larger.

- a) From the DNA Center home page, choose **Design > Network Settings > IP Address Pools**.
- b) From the **Network Hierarchy** pane, select a site.
- c) Click **Reserve IP Pool** and complete the following fields to reserve all or part of an available global IP address pool for the specific site:
 - **IP Pool Name**—Unique name for the reserved IP address pool.
 - **Type**—Type of IP address pool. For LAN automation, select **LAN**.
 - **Global IP Pool**—IP address pool from which you want to reserve all or part of the IP addresses.
 - **CIDR Notation/No. of IP Addresses**—IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses you want to reserve.
 - **Gateway IP Address**—Gateway IP address.
 - **DHCP Servers**—DHCP Server(s) IP address(es).

d) Click **Reserve**.

Step 2 Discover and provision devices.

- a) From the DNA Center home page, choose **Provision > Devices > Inventory**.
All the discovered devices are displayed.
- b) Click the **Topology View** icon.
- c) Right click one of the discovered devices and select **Discover and Provision New Devices**.
- d) From the **LAN Automation** slide-in dialog box, complete the following fields:
 - **Site ID**—Site ID and associated settings that DNA Center uses for LAN automation.
 - **Seed Device(s)**—IP address of the device that DNA Center uses as the starting point to discover and provision new devices.

Note If DNA Center cannot access the primary seed device, it uses the secondary seed device.

Check the LAN Automation Status

- **LAN Pool**—IP address pool that was reserved for LAN automation. (See Step 1.)
- **Name Prefix**—Text that describes the devices being provisioned. As DNA Center provisions each device, it names the device with the text that you provide and adds a unique number to the end. For example, if you enter **Access** as the name prefix, as each device is provisioned, it is named Access-1, Access-2, Access-3, and so on.
- **Discover Ports**—Ports to be used to discover and provision new devices.

e) Click **Start**.

DNA Center begins to discover and provision the new devices.

Step 3 Monitor and review the progress of devices being provisioned.a) From the **Topology View** page, click **Status**.

The **LAN Automation Status** dialog box displays the progress of the devices being provisioned.

Note The process can take several minutes for all of the new devices to be provisioned.

b) After all of the devices have been discovered and provisioned, click **Stop**.

The LAN automation process is complete, and the new devices are added to the Device Inventory.

What to do next

To review the LAN automation configurations, from the DNA Center home page, choose **Network Plug and Play > Configurations**.

Check the LAN Automation Status

You can view the status of LAN automation jobs that are in progress.

Before you begin

You must have created and started a LAN automation job.

Procedure**Step 1** From the DNA Center home page, choose **Provision > Devices**.**Step 2** Click the **Inventory** tab. All the discovered devices are displayed.**Step 3** Click **LAN Auto Status**.

The status of any running or completed LAN automation jobs is displayed.

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**.

Multi-Site Fabric Domain

A Multi-site Fabric domain is a collection of Fabric sites interconnected via a Transit Area. A Fabric site is a portion of the fabric which has its own set of Control Plane Nodes, Border Nodes and Edge Nodes based on geography or size. A Fabric site is in principle autonomous from other Fabric sites from the connectivity perspective.

Multiple Fabric sites corresponding to a single Fabric domain are interconnected by a Transit Area. The Transit Area may be defined as a portion of the Fabric that has its own Control Plane Nodes, Border Nodes, but does not have Edge Nodes. Furthermore, the Transit Area shares at least one Border Node with each Fabric Site it interconnects.

An Software Defined Access (SDA) Fabric comprises of multiple sites. Each site has the benefits of scale, resiliency, survivability and mobility. The overall aggregation of sites (i.e. the Fabric domain) must also be able to accommodate a very large number of end-points and scale modularly or horizontally by aggregating sites contained within each site.

Transit Networks

Transit Network is a network that connects two or more Fabric sites with each other or connects the Fabric site with External Networks (Internet, Data Center etc). There are two types of transit networks.

- IP Transit

Create a IP Transit Network

IP Transit represents if we are using regular IP network to connect to external network or between two or more Fabric sites.

IP Transit of BGP type is supported.

- SDA Transit

SDA Transit represents if we are using LISP/VxLAN encapsulation to connect two Fabric sites.

Using SDA Transit provides an advantage of carrying the same Policy tag across different Fabric sites.

Create a IP Transit Network

To add a new IP Transit network:

Procedure

-
- Step 1** From the DNA Center **Home** page, click **Provision**.
 - Step 2** Click the **Fabric** tab.
 - Step 3** Click the **Add Fabric Domain or Transit** tab.
 - Step 4** Select **Add Transit** from the pop-up.
 - Step 5** Enter a **Transit Name** for the network.
 - Step 6** Select the Transit type as **IP-Based**
 - Step 7** Routing protocol is set as default to BGP.
 - Step 8** Enter the **Autonomous System Number** for this Transit network.
 - Step 9** Click **Save**
-

Create a SDA Transit Network

To add a new SDA Transit network:

Before you begin

Procedure

-
- Step 1** From the DNA Center **Home** page, click **Provision**.
 - Step 2** Click the **Fabric** tab.
 - Step 3** Click the **Add Fabric Domain or Transit** tab.
 - Step 4** Select **Add Transit** from the pop-up.
 - Step 5** Enter a **Transit Name** for the network.
 - Step 6** Select the Transit type as **SD-Access**
 - Step 7** Enter the **Site for the Transit Control Plane** for this Transit network. Select at least one Transit Map-Server.

-
- Step 8** Enter the **Transit Control Plane** for this Transit network.
 - Step 9** Repeat steps 7 and 8 for all the map-servers that you want to add.
 - Step 10** Click **Save**
-

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 **Fabric** tab.
 - Step 3** Click the **Add Fabric Domain or Transit** tab.
 - Step 4** Select **Add Fabric** from the pop-up.
 - Step 5** Enter a **Fabric Name**.
 - Step 6** Select one Fabric site.
 - Step 7** 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 8** 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**. Before you add a device to the fabric, you must perform the pre-verification check by clicking on the **Pre-Verification** tab. The pre-verification check can be done only for the devices that have been assigned roles. The pre-verification procedure performs a check on the **Hardware Version** and **Software Version** of the device. The result is displayed mentioning whether the device passed the test, failed the test or, is not supported.

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:

Field	Description
	<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.
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.
Enable Guests	<p>In the pop-up window that is displayed, enter the following options:</p> <ul style="list-style-type: none"> • Set as control plane—Select the check box if you want the device to act as a control plane. • Set as a border node—Select the check box if you want the device to act as a border node. • Select a guest virtual network—All the guest virtual networks created are listed. Select the check box of the guest virtual network, and click Enable. <p>Note Ensure that you have created a guest virtual network in the Policy application. See Create a Virtual Network, on page 207.</p>
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. After selecting the authentication template, click **Save**.
- Associate IP address pools to guest virtual networks and default virtual networks, and click **Update**. The IP address pools displayed will be site specific pools only.
- Specify wireless SSIDs within the network that the hosts can access. You can select the guest or enterprise SSIDs and assign address pools, and click **Save**.
- Check the **Enable Wireless Multicast** check box to transfer data to multiple destinations simultaneously on the wireless network. The information is delivered to each link only once and the copies are created when the links to the destinations split, thus creating an optimal distribution path. Multicasting reduces unnecessary packet duplication.
- 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. The available authentication templates are:

- **Closed Authentication-**
- **Easy Connect-**
- **No Authentication**
- **Open Authentication-**This provides open authentication.

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.

Multicast Overview

Multicast traffic is forwarded in different ways:

- Via shared trees by using Rendezvous Point. PIM SM is used in this case.
- Via shortest path trees (SPT). PIM SSM (Source specific multicast) uses SPT only. PIM SM switches to SPT after source is known on edge router that receiver is connected to.

More information is available on Cisco, [IP Multicast Technology Overview](#).

Configure Multicast Settings

After devices have been added to the fabric domain, you can create multicast IP address pools and rendezvous points. Applicable multicast configurations will be automated on all of the fabric devices operating in that fabric domain.



Note Multicast is defined only for user-defined virtual networks and not for global networks. 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.

Create a Multicast IP Address Pool

To create a multicast IP address pool:

Before you begin

Multicast IP Address Pool is used for internal PIM communication within the fabric domain. There is an option to define multiple multicast pools and each can be associated with a separate Virtual Network. There is a requirement that each Virtual Network needs to have a separate Multicast IP Address Pool created and associated with it.

Procedure

- Step 1** From the DNA Center **Home** page, choose **Design -> Network Settings -> IP Address Pools**.
- Step 2** It will display all IP address pools that have been created.
- Step 3** Click the **Add** button. You can now specify the multicast addresses that should form a pool. Complete the required fields.

Field	Description
IP Pool Name	Multicast IP Address Pool name

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

Step 4 Click Save.

Step 5 In case there is a need to enable multicast in multiple Virtual Networks, create a separate IP multicast pools for each Virtual Network (repeat steps 3-4).

Add a Device as Rendezvous Point

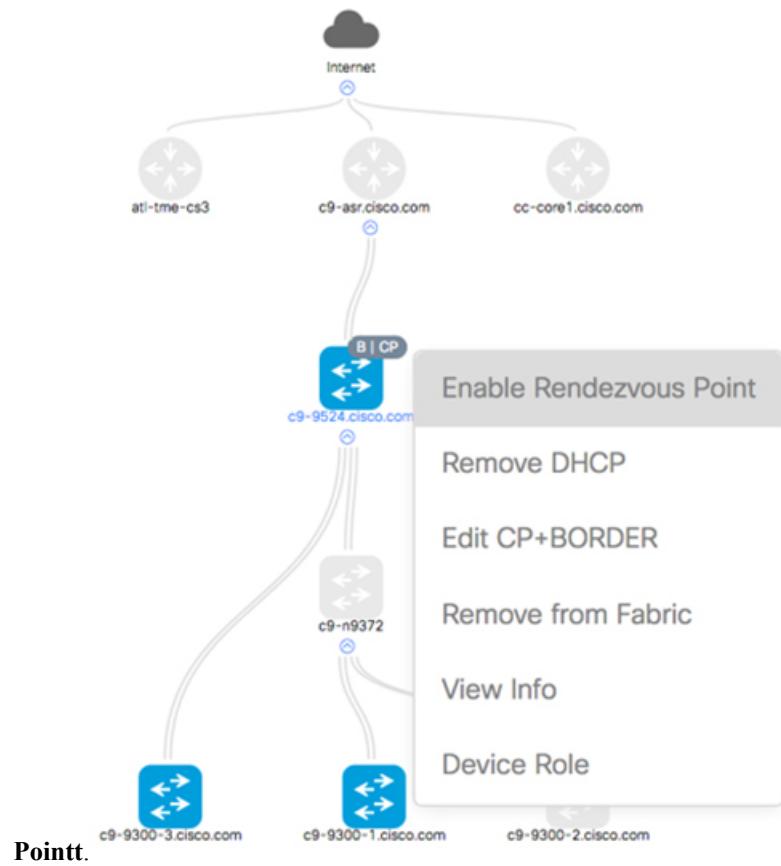
To add a Device as rendezvous point:

Procedure

- Step 1** From the DNA Center **Home** page, click on the **Provision** tab. The screen displays the Devices page (default).
- Step 2** From the **Provision - Devices** page, click on the **Fabric** tab. The screen displays the list of fabric domains.
- Step 3** From the **Provision - Fabric** page, select a fabric. The screen displays the **Fabric - Devices** page, with all of the devices in the network. Any device that is added to the fabric is highlighted in blue color.

Add a Device as Rendezvous Point

Step 4 Click on a fabric device that you want to add as a rendezvous point, and select **Enable Rendezvous**



Pointt.

Step 5 DNA Center will display the list of Virtual Networks in the pop-up window. Expand the **Virtual Networks**, and select an **IP multicast pool** by clicking on the **Plus** button. Select

Associate Multicast Pools to VNs

Associate Virtual Networks

- ▼ DEFAULT VN
- ▼ Guest
- ^ Campus9

Campus-Multicast |
 XXXXX(XX)XX/24

Next

- Step 6** **Note** Only a single IP address pool for each VN for multicast is currently supported.
In order to enable multicast in multiple Virtual Networks, it is required to create multiple Multicast IP Address pools.
- Step 7** Associate Virtual Network and click **Enable**.
Click **Save** on the main screen. **Apply** the changes.

Verification**Procedure**

- Step 1** From the DNA Center **Home** page, click on the **Provision** tab. The screen displays the Devices page (default).
- Step 2** From the **Provision - Devices** page, click on the **Fabric** tab. The screen displays the list of fabric domains.
- Step 3** From the **Provision - Fabric** page, select a fabric. The screen displays the **Fabric - Devices** page, with all of the devices in the network.
- Step 4** Any Virtual Network enabled for IP multicast will be marked with an "M" icon.

**Add a Device as Redundant Rendezvous Point****Note**

Dual RP is only supported for EXTERNAL or INTERNAL BORDERNODE.

When a redundant Rendezvous Point is added to the network, the MSDP session is enabled. Each fabric device that's hosts the RP creates 2 Loopbacks per VRF - one for RP and another loopback to establish MSDP session.

To add a Device as a redundant rendezvous point:

Procedure

- Step 1** From the DNA Center **Home** page, click on the **Provision** tab. The screen displays the Devices page (default).
- Step 2** From the **Provision - Devices** page, click on the **Fabric** tab. The screen displays the list of fabric domains.
- Step 3** From the **Provision - Fabric** page, select a fabric. The screen displays the **Fabric - Devices** page, with all of the devices in the network. Any device that is added to the fabric is highlighted in blue color.

Add a Device as Redundant Rendezvous Point

- Step 4** Click on a device that you want to add as a redundant rendezvous point, and select **Enable Rendezvous Point**.
 - Step 5** DNA Center will display the list of Virtual Networks in the pop-up window. Expand the **Virtual Networks** for which you would like to redundant RP, and a Multicast IP address pool should be pre-populated. Select **Next**.
 - Step 6** Associate Virtual Network and click **Enable**.
 - Step 7** Click **Save** on the main screen. **Apply** the changes.
-



CHAPTER 13

DNA Center Assurance Overview

- [About DNA Center Assurance, on page 233](#)
- [About DNA Center Assurance and Analytics, on page 233](#)

About DNA Center Assurance

DNA Center Assurance provides a comprehensive solution to assure better and consistent service levels to meet growing business demands. DNA Center Assurance addresses not just reactive network monitoring and troubleshooting, but also the proactive and predictive aspects of running the network, ensuring client, application, and service performance.

DNA Center Assurance provides the following benefits:

- Provides actionable insights into network, client, and application related issues. These issues consist of basic and advanced correlation of multiple pieces of information, thus eliminating white noise and false positives.
- Provides both system-guided as well as self-guided troubleshooting. For a large number of issues, DNA Center Assurance provides a system-guided approach, where multiple Key Performance Indicators (KPIs) are correlated, and the results from tests and sensors are used to determine the root cause of the problem, and then possible actions are provided to resolve the problem. The focus is on highlighting the issue rather than monitoring data. Quite frequently, DNA Center Assurance performs the work of a Level 3 support engineer.
- Provides in-depth health scores for the network and its devices, clients, applications, and services. Client experience is assured both for access (onboarding) and connectivity.

About DNA Center Assurance and Analytics

Companies deal with an abundance of network data. Tackling the volume, variety, speed, and accuracy of network data is crucial for IT organizations. DNA Center Assurance is designed to handle this network data problem.

DNA Center Assurance is a multipurpose, real-time, network data collection and analytics engine used to significantly increase the business potential of network data.

DNA Center Assurance simplifies and abstracts the collection and analysis layers and offers a rich set of APIs along with a web interface. By using a single set of network data, DNA Center Assurance powers a broad set

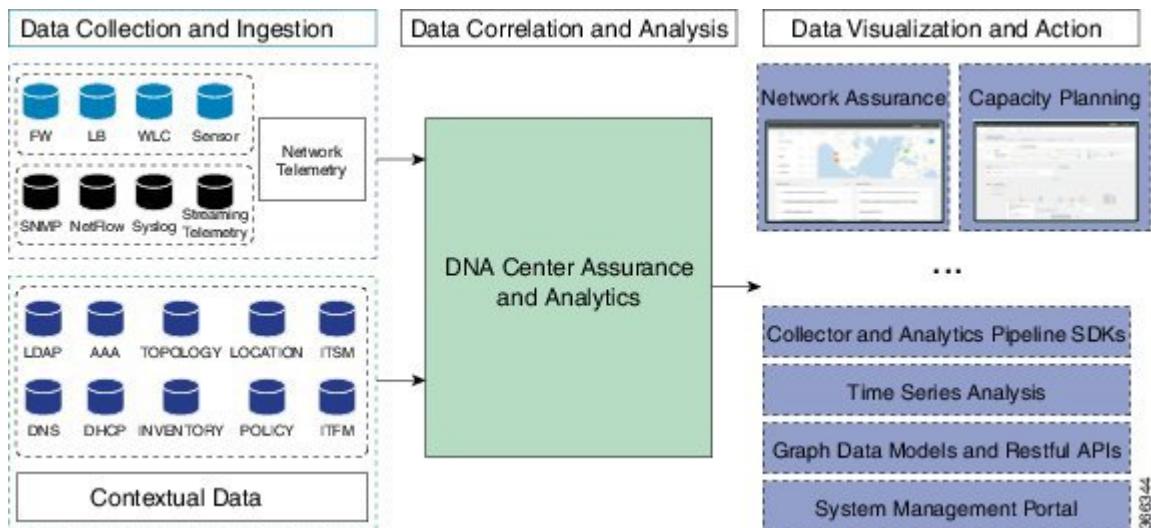
About DNA Center Assurance and Analytics

of use cases. These efficiencies streamline the operational and network management overhead of collecting and analyzing network data, thereby allowing companies to effectively focus on their business goals.

Given its flexible architecture, DNA Center Assurance addresses many common use cases, including monitoring and troubleshooting, cost management, and policy discovery, while supporting the broader Cisco DNA strategy.

The following figure and the information that follows describes the DNA Center Assurance and Analytics architecture:

Figure 7: DNA Center Assurance and Analytics Architecture



- Data Collection and Ingestion—DNA Center Assurance leverages streaming technologies to collect a variety of network telemetry and contextual data in real time.
- Data Correlation and Analysis—As data is ingested, DNA Center Assurance correlates and analysis the data.
- Data Visualization and Action—Data is stored in databases and exposed through APIs to DNA Center Assurance as well as other applications, such as Capacity Planning. DNA Center Assurance is an open system that provides the following:
 - Collector and analytics pipeline SDKs
 - Time series analysis
 - Graph data models and restful APIs
 - System management portal



CHAPTER 14

Configure DNA Center Assurance

- Basic Workflow for Configuring DNA Center Assurance, on page 235
- DNA Center Assurance and Cisco ISE Integration, on page 236
- Assurance Application , on page 240

Basic Workflow for Configuring DNA Center Assurance

Before you begin using the DNA Center Assurance application, you must configure DNA Center Assurance. This procedure provides the basic workflow.

Procedure

Step 1 Discover devices (routers, switches, Cisco WLCs, and access points).

See [Discover Your Network Using an IP Address Range, on page 16](#), [Discover Your Network Using CDP, on page 11](#), or [Discover Your Network Using LLDP, on page 21](#).

Note Cisco WLCs must be discovered using the Management IP address instead of the Service Port IP address. If not, the related WLC 360 and AP 360 pages will not display any data.

Step 2 Make sure that the devices appear in the device Inventory.

See [Display Information About Your Inventory, on page 56](#).

Note You must wait for all the devices to get into a Managed state.

Step 3 Design your network hierarchy. Configure the location of the device, such as area, site, building, and floor.

See [Create Sites in the Network Hierarchy, on page 92](#), [Add Buildings, on page 95](#), and [Add Floors to Buildings, on page 96](#).

Step 4 Provision your network. Add devices to the sites.

See [Add Devices to Sites, on page 211](#).

Step 5 If you are adding APs, we recommend that you assign and position them on a floor map.

See [Add, Position, and Delete APs, on page 100](#).

Step 6 Configure and apply Telemetry profile to network devices.

See [Configure a Telemetry Profile, on page 153](#) and [Apply a Telemetry Profile to the Devices, on page 154](#).

- Step 7** If your network uses Cisco ISE for user authentication, you can configure DNA Center Assurance for Cisco ISE integration. This will allow you to see more information about wired clients, such as the username and operating system, in DNA Center Assurance.

See [DNA Center Assurance and Cisco ISE Integration, on page 236](#).

- Step 8** Enable Device Controllability. Device Controllability is enabled by default. Device Controllability automatically configures discovered devices with SNMP trap servers, NetFlow, Syslog, and NETCONF.

For information about Device Controllability, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

- Step 9** Start using the Assurance application.

See [Assurance Application , on page 240](#).

DNA Center Assurance and Cisco ISE Integration

If your network uses Cisco ISE for user authentication, you can configure DNA Center Assurance for Cisco ISE integration. This will allow you to see more information about wired clients, such as the username and operating system, in DNA Center Assurance. Do the following:

1. Generate Keystore file. See [Generate Keystore File, on page 236](#).
2. Generate Truststore file. See [Generate Truststore File, on page 238](#).
3. Configure DNA Center Assurance for ISE integration. See [Configure DNA Center Assurance for Cisco ISE Integration, on page 240](#).

Generate Keystore File

Use this procedure to generate the Keystore file. The keystore.jks file that is generated contains certificates, which DNA Center uses to communicate with ISE.

Before you begin



- Note** You must have Java Keytool installed to complete this procedure.

Procedure

- Step 1** Log into Cisco ISE.

- Step 2** From the Cisco ISE home page, choose **Administration > pxGrid Services > Certificates**.

The Generate pxGrid Certificates page opens.

- Step 3** Do the following:
- From the **I want to** drop-down list, choose **Generate cert (without certificate signing request)**.
 - In the **Common Name (CN)** field, enter the name of the DNA Center server including domain name. For example, dnac.yourdomain.com.
 - From the **Subject Alternative Name (SAN)** drop-down list, choose **IP address**, and then enter the DNA Center IP address in the field provided.
 - From the **Certificate Download Format** drop-down list, choose **PKCS format (including certificate chain; one file for both the certificate name and key)**.
 - In the **Certificate Password** field, enter a unique password.
 - In the **Confirm Password** field, enter the password again.

Save this password. You will need to use this password when you configure DNA Center Assurance for ISE integration.

- Click **Create**.
A Zip file is generated.
- Extract the files from the Zip file.

- Step 4** From a terminal prompt, do the following:

- Go to the directory where you extracted the files.

Example

```
$ cd /home/user/certificate
```

- Enter the following command:

```
keytool -v -list -storetype pkcs12 -keystore filename -storepass certificate-password | grep -i alias
```

Example

```
$ keytool -v -list -storetype pkcs12 -keystore DNAC.cisco.com_192.168.0.1.p12 -storepass Cisco123 | grep -i alias
Alias name: dnac.cisco.com_192.168.0.1
```

An Alias Name is generated.

- Copy the Alias Name.
- Enter the following command:

```
keytool -importkeystore -srckeystore filename -srcstoretype pkcs12 -srcalias alias name -destkeystore keystore.jks -deststoretype jks -deststorepass certificate-password -destalias Keystore
```

Example

```
$ keytool -importkeystore -srckeystore DNAC.cisco.com_192.168.0.1.p12 -srcstoretype pkcs12 -srcalias dnac.cisco.com_192.168.0.1 -destkeystore keystore.jks -deststoretype jks -deststorepass Cisco123 -destalias Keystore
```

- At the **Enter the source keystore password:** prompt, enter the Certificate Password that you entered in **Step 3 e**.

The keystore.jks file is created in the same folder where you extracted the files. The keystore.jks file that is generated contains certificates, which DNA Center uses to communicate with ISE.

What to do next

Do the following:

- Generate the Truststore file. See [Generate Truststore File, on page 238](#).
- Configure DNA Center Assurance for Cisco ISE integration. See [Configure DNA Center Assurance for Cisco ISE Integration, on page 240](#).

Generate Truststore File

Use this procedure to generate the Truststore file. The truststore.jks keystore file that is generated contains ISE certificates, which allow DNA Center to validate the ISE server in all communications.

Before you begin

Make sure you have generated the Keystore file. See [Generate Keystore File, on page 236](#).



Note

You must have Java Keytool installed to complete this procedure.

Procedure

Step 1 Log into Cisco ISE.

Step 2 From the Cisco ISE home page, choose **Administration > pxGrid Services > Certificates**.

The Generate pxGrid Certificates page opens.

Step 3 Do the following:

- From the **I want to** drop-down list, choose **Download Root Certificate Chain**.
- In the **Host Name** field, enter a host name.
- From the **Certificate Download Format** drop-down list, choose **Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKSCB format (including certificate chain)**.
- Click **Create**.
A Zip file is generated.
- Extract the four files from the Zip file.

Step 4 From a terminal prompt, do the following:

- Go to the directory where you extracted the files.

Example

```
$ cd /home/user/certificate
```

- Enter the following command:

```
keytool -importcert -file filename -keystore truststore.jks -alias filename-without-extension
```

- At the **Enter the keystore password:** prompt, enter the Certificate Password that you created when you generated the Keystore file. See [Generate Keystore File, on page 236](#).
- At the **Re-enter the new password:** prompt, enter the password to confirm it.

- e) At the **Trust this certificate? [no]:**prompt, enter yes.

The certificate is added to Keystore. The truststore.jks keystore file that is generated contains ISE certificates, which allow DNA Center to validate the ISE server in all communications.

- f) Repeat **Step 4** for each of the extracted files.

The truststore.jks file is created in the same folder where you extracted the files. The ISE server certificate chain is added to the truststore.jks file.

Example

```
$ keytool -importcert -file CertificateServicesEndpointSubCA-dnac-ise-01_.cer -keystore
truststore.jks -alias CertificateServicesEndpointSubCA-dnac-ise-01_
Enter keystore password:
Re-enter new password:
Owner: CN=Certificate Services Endpoint Sub CA - dnac-ise-01
Issuer: CN=Certificate Services Node CA - dnac-ise-01
Serial number: 9a91659bf1546c19e8ccd43fb4b6b62
Valid from: Sat Sep 16 11:59:43 PDT 2017 until: Fri Sep 17 11:59:40 PDT 2027
Certificate fingerprints:
      SHA1: 6D:F5:B6:8F:E2:21:D5:91:44:23:28:7B:59:71:34:23:03:8F:F2:99
      SHA256:
1A:8D:54:73:48:E6:2B:40:8A:64:AB:04:98:40:C9:C0:EB:07:28:54:C4:0C:4F:DD:7D:66:FA:5B:EB:C6:54:ED
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 4096-bit RSA k
Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 5A 8A 8D 1B 32 3B 41 31    93 BF 12 E6 53 44 9E 52  Z...2;A1....SD.R
0010: 07 0E F1 E2                ....
]
[CN=Certificate Services Root CA - dnac-ise-01]
SerialNumber: [      332cc5aa 641e4b8a a6b0cf67 a0ac24bd]
]
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]
#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
]
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 72 3C 5F 26 5F D4 7A AF    17 85 2B 72 C9 C3 82 16  r<_&_.z...+r....
0010: 0D 46 FE 48                .F.H
]
Trust this certificate? [no]: yes
Certificate was added to keystore
```

What to do next

Configure DNA Center Assurance for Cisco ISE integration. See [Configure DNA Center Assurance for Cisco ISE Integration, on page 240](#).

Configure DNA Center Assurance for Cisco ISE Integration

Before you begin

- Make sure you have generated the Keystore file. See [Generate Keystore File, on page 236](#).
- Make sure you have generated the Truststore file. See [Generate Truststore File, on page 238](#).

Procedure

Step 1 From the DNA Center **Home** page, choose  > **System Settings** > **Data Platform** > **Collectors**.

The Collectors page appears.

Step 2 Click **Collector-ISE**.

The Collector-ISE page appears.

Step 3 Click **+ Add**.

The ISE Collector Configuration page appears.

Step 4 Do the following:

- In the **ISE Service IP Address** field, enter the IP address of the ISE server.
- In the **Username** field, enter the ISE username.
- In the **Password** field, enter the ISE password.
- From the **Truststore File** area, click **Browse**, and then upload the Truststore file.
- In the **Truststore Passphrase** field, enter the Certificate Password.
- From the **Keystore File** area, click **Browse**, and then upload the Keystore file.
- In the **Keystore Passphrase** field, enter the Certificate Password.

You created the Certificate Password when you generated the Keystore file. See [Generate Keystore File, on page 236](#).

- (Optional) Check the **Anonymize** check box if you want to hide the user name. In the **Salt** field, enter the Salt string for the user name.
 - In the **Subscriber Name** field, enter the name of the pxGrid subscriber. For example: dnac-assurance
 - In the **Configuration Name** field, enter a unique name for the ISE configuration.
 - Click **Save Configuration**.
-

Assurance Application

To access the Assurance application, log into DNA Center, then from the DNA Center home page, click the **Assurance** tab.

**Note**

Before you begin using the Assurance application, you must configure DNA Center Assurance. See [Basic Workflow for Configuring DNA Center Assurance](#), on page 235.

From the Assurance application, you can do the following:

Table 53: Assurance Tab

Task	Navigation	Reference
Get a global view of your entire enterprise, which includes network and clients.	Assurance landing page	See Monitor and Troubleshoot the Overall Health of Your Enterprise , on page 243.
Get a global view of your entire network, which includes routers, switches, access points, and Cisco WLCs.	Assurance > Health > Network	See Monitor and Troubleshoot the Health of Your Network , on page 246.
Get an individual 360° view of a specific network element (router, switch, access point, or Cisco WLC).	Assurance > Health > Network . In the Network Devices table, Device column, click the device name to display the Device 360 page.	See Monitor and Troubleshoot the Health of a Device , on page 252.
Get a global view of all wired and wireless clients.	Assurance > Health > Client	See Monitor and Troubleshoot the Health of All Client Devices , on page 261.
Get a 360° view of a specific client.	Assurance > Health > Client . In the Client Devices table, click the MAC address to display the Client 360 page.	See Monitor and Troubleshoot the Health of a Client Device , on page 270.
Get a global view of all the applications running on a client device and their qualitative and quantitative metrics.	Assurance > Health > Application	See Monitor the Health of All Applications , on page 279.
Get a 360° view of a specific application.	Assurance > Health > Application . In the Applications table, click the name of an application to display the Application 360 page.	See Monitor the Health of an Application , on page 281.
Manage sensor-driven tests.	Assurance > Sensor Management	See Manage Sensors and Sensor-Driven Tests , on page 283.

Task	Navigation	Reference
Manage and create custom dashboards.	Assurance > Dashboards > Dashboard Library	See Manage Dashboards, on page 293 .
Display and troubleshoot issues.	Global Issues— Assurance > Issues Overall Health Issues— Assurance landing page Client Issues— Assurance > Health > Client . In the Client Devices table, click the MAC address to display the Client 360 page. Device Issues— Assurance > Health > Network . In the Network Devices table, Device column, click the device name to display the Device 360 page. Issue Catalog— Assurance > Issues > View Issue Catalog .	See Issues Detected by DNA Center Assurance, on page 299 .



CHAPTER 15

Assure the Health of Your Enterprise

- [About Enterprise, on page 243](#)
- [Monitor and Troubleshoot the Overall Health of Your Enterprise, on page 243](#)
- [Monitor and Troubleshoot the Health of Your Network, on page 246](#)
- [Monitor and Troubleshoot the Health of a Device, on page 252](#)

About Enterprise

You can use DNA Center Assurance to monitor and troubleshoot your enterprise. An enterprise consists of network devices and clients.

A network consists of one or more devices, which include routers, switches, wireless controllers, and access points.

A client is an end device (computer, phone, and so on) that is connected to a network device (access point or switch). DNA Center supports both wired and wireless clients.

Monitor and Troubleshoot the Overall Health of Your Enterprise

Use this procedure to get a global view of the health of your enterprise, which includes network devices and clients, and to determine if there are potential issues that must be addressed.

Before you begin

Configure DNA Center Assurance. See [Basic Workflow for Configuring DNA Center Assurance, on page 235](#).

Procedure

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

The **Overall Health** page appears with three dashlets as described in the table below.

The colors in the page represent the health of the devices:

- Red—Critical issues. Health score range is 1 to 3.

- Orange—Warnings. Health score range is 4 to 7.
- Green—No errors or warning. Health score range is 8 to 10.
- Grey—No data available. Health score is 0.

Table 54: Overall Health Page

Item	Description
Last 24 Hours, All Domains, Actions drop-down lists	<ul style="list-style-type: none"> • Last 24 Hours—Displays information on the page based on the time you select from the drop-down list. Options are: last 3 hours, last 24 hours, and last 7 days. Default is last 24 hours. • All Domains—Displays information for all domains or fabric domains. Default is all domains. • Actions—Allows you to make changes to the dashboard display when you choose Edit Dashboards from the drop-down list. See Change the Position of a Dashlet, on page 297 and Create a Custom Dashboard, on page 293.
Overall Health Map or Hierarchical Site/Building View dashlet	<p>The Hide or Show button, allows you to hide or display this dashlet. By default, the Overall Health Map dashlet displays.</p> <p>This dashlet contains two buttons that allow you to display the health of all the components in the enterprise in a map view or site/building view.</p> <ul style="list-style-type: none"> • Overall Health Map—Click the map button to display health of all the sites in your enterprise on a geographic location-oriented health map. By default, the sites that are represented are color-coded according to the severity of the problem. • Hierarchical Site/Building View—Click the site button, and then choose the hierarchical site view or building view from the drop-down list. Based on what you choose, the table provides the relevant information.

Item	Description
Overall Health Summary dashlet	<p>Contains the following:</p> <ul style="list-style-type: none"> • Client area—Provides the following: <ul style="list-style-type: none"> • Client Score—Percentage of healthy (good) wired and wireless client devices in your overall enterprise. See, Client Health Summary Score, on page 268. • Wired and Wireless Score—Provides the score distribution between wired and wireless clients. <p>Click View Client Health to open the Client Health page.</p> <ul style="list-style-type: none"> • Network area—Provides the following: <ul style="list-style-type: none"> • Network Score—Percentage of healthy (good) devices (routers, switches, wireless controllers, and access points) in your overall enterprise. See, Global Network Health Summary Score or Site Health Summary Score , on page 251. • Device Category Health Score—Provides the score distribution between device categories: Core Switch, Access Switch, Distribution Switch, Router, and Wireless. The device category score is the percentage of healthy (good) devices in a particular device category. <p>Note When a fabric domain is selected, this area provides the score distribution between the following categories: Fabric Edge, Fabric Border, and Fabric Control Plane.</p> <p>Click View Network Health to open the Network Health page.</p>
Issues dashlet	<p>Issues, if any, that must be addressed. Issues are listed based on the time stamp, the most recent issue is listed first.</p> <p>Click an issue to display details, such as the summary of the issue, impact, and suggested actions. To resolve an issue, from the Status field, choose Resolve.</p> <p>Click View All Issues to open the Issues page.</p> <p>For information about the types of issues, see Issues Detected by DNA Center Assurance, on page 299.</p>

Step 2 Do the following as required:

- To view details about an issue, from the **Issues** dashlet, click an issue.
- If the network health score is red or orange, from the **Overall Health Summary** dashlet, click [View Network Health](#).
- If the client health score is red or orange, from the **Overall Health Summary** dashlet, click [View Client Health](#).
- To display a 360° view of a device, in the **Search field** (located on the top-right corner), enter the following information:

- For client devices—Host name, user ID (authenticated through Cisco ISE), IP address, or MAC address.
 - For switches, routers, access points, and Cisco WLC—Device name, IP address, or MAC address.
-

Monitor and Troubleshoot the Health of Your Network

A network consists of one or more devices, which include routers, switches, wireless controllers, and access points. The client is not a part of the network health score.

Use this procedure to get a global view of your network and to determine if there are potential issues that must be addressed.

Before you begin

Configure DNA Center Assurance. See [Basic Workflow for Configuring DNA Center Assurance, on page 235](#).

**Note**

Network health score exists only in the context of a location. If the location of a device is not available, it is not counted in the network health score.

Procedure

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

The **Overall Health** page appears.

Step 2 Click **Health > Network**.

The **Network Health** page appears with four dashlets as described in the table below.

The colors in the charts represent the health of the network devices:

- Red—Critical issues. Health score range is 1 to 3.
- Orange—Warnings. Health score range is 4 to 7.
- Green—No errors or warning. Health score range is 8 to 10.
- Grey—No data available. Health score is 0.

Table 55: Network Health Page

Item	Description
All Domains and Actions drop-down list	<ul style="list-style-type: none"> • All Domains—Displays information for all domains or fabric domain. Default is All Domains. To view information about the fabric domain, click the drop-down list, and then choose the appropriate option. • Actions—Allows you to make changes to the dashboard display when you choose Edit Dashboards from the drop-down list. See Change the Position of a Dashlet , on page 297 and Create a Custom Dashboard, on page 293.
24 Hours drop-down list and Timeline Slider	<ul style="list-style-type: none"> • 24 Hours—Displays information on the page based on the time range you select. Do the following: <ol style="list-style-type: none"> 1. From the 24 Hours drop-down list, choose a time range: 3 hours, 24 hours, or 7 days. 2. Specify the Start date and time; and the End date and time. 3. Click Apply. This sets the time boundaries on the timeline slider. • Timeline Slider—Allows you to specify a more granular time range. Move the timeline slider to the desired time range, and then click Apply.

Item	Description
Network Health Map, Network Topology, or Hierarchical Site/Building View dashlet	<p>The Hide or Show button, allows you to hide or display this dashlet. By default, the Network Health Map dashlet displays.</p> <p>This dashlet contains three buttons that allow you to display the health of the network in a map view, topology view, or site/building view.</p> <ul style="list-style-type: none"> • Network Health Map—Click the map button to display health of all the network sites on a geographic location-oriented network health map. By default, the network sites that are represented are color-coded according to the severity of the problem. The color of the health score represents its severity. The health is measured on a scale of 1 to 10, with 10 being the best score, and a score of 0 where data could not be obtained. • Network Topology—Click the topology button to display a topology view of how the components in the network are connected. Hover your cursor over a device to display device information such as the device role, IP address, and software version. To obtain a 360° view of the device, click View Details 360. • Hierarchical Site/Building View—Click the site button, and then choose the hierarchical site view or building view from the drop-down list. Based on what you choose, the table provides the relevant information. To view information about a specific site, building, or floor, click Apply in the appropriate row, the information on the page refreshes based on your selection.
Network Health Summary or Site Health Summary dashlet	<p>The Network Health Summary score or Site Health Summary score is the percentage of healthy (good) devices in your overall network or selected site. See, Global Network Health Summary Score or Site Health Summary Score , on page 251.</p> <p>This dashlet includes the following charts:</p> <ul style="list-style-type: none"> • 15 Minutes—Color-coded percentage chart that shows the performance of each device category (access, core, distribution, router, wireless, and other) over the last 15 minutes. Hover your cursor over a color to display the health score. • 24 Hours—Color-coded trend chart that shows the performance of devices over the last 24 hours. Hover your cursor over the chart to display the number of devices that are doing well or poorly over time. <p>Click View Details to open a side bar with additional details. From the side bar, click a color in the chart, the timeline slider moves to that instance, and the data in the table below refreshes with that time stamp.</p>

Item	Description
Network Health By Device Role/Type dashlet	<p>Provides a breakdown of the device health, per device role (category), along with a 24 hour health history. Contains device health category tabs (Access, Core, Distribution, Router, Wireless, and Other) and corresponding analytic charts.</p> <ul style="list-style-type: none"> • Device Health Category Tabs—Each tab contains a device health category score and a trend chart. The device health category score is the percentage of healthy (good) devices in that category. The trend chart shows the performance of the devices over time. See Device Category Health Score, on page 251 • Analytic Charts—Click a device category tab to display analytic charts (donut chart) for that device type. The following analytic charts are provided: <p>Note For the Wireless category, instead of the donut charts, bar charts are provided: one bar for APs and the other bar for Cisco WLCs.</p> <p>Depending on the device category you click, the metrics that display in the analytic charts vary.</p> <ul style="list-style-type: none"> • System Health—Provides system monitoring metrics, such as CPU utilization, memory utilization, and temperature. • Data Plane Connectivity—Provides metrics, such as uplink availability and link errors. • Control Plane Connectivity—Provides information about connectivity to the MAP servers. This analytic chart is available for fabric devices only. <p>Click View Details to open a side bar with additional details. From the side bar, you can drill-down to display the following:</p> <ul style="list-style-type: none"> • Click a color in the chart to populate or refresh the data in the table below. • Click a color in the chart, and then expand the Device Distribution drop-down list. The Device Type, Device Model, and Device OS tabs display. Click a tab to display donut charts corresponding to the tab you selected. <p>Note For fabric devices, the following category tabs are provided: Fabric Edge, Fabric Border, and Fabric Control Plane. To view information about fabric domain, from the All Domains drop-down list, choose the appropriate option.</p> <p>Note For information about how the individual device health score is computed, see Individual Device Health Score, on page 251.</p>

Item	Description
AP Analytics dashlet	<p>Contains two dashlets:</p> <ul style="list-style-type: none"> • Total APs Up and Down—Color-coded chart that provides the AP status information: number of APs that are connected to the network and the number of APs that are not connected to the network. • Top N APs by Client Count—Chart that provides information about the APs that have the highest number of clients. <p>Click View Details to open a side bar with additional details. From the side bar, click a color in the chart to refresh the data in the table below.</p>
Network Devices Table dashlet	<p>Allows you to filter, view, and export network device information:</p> <ul style="list-style-type: none"> • Filter the table based on device, type, overall health, or add custom filters: <ul style="list-style-type: none"> • Device—Monitored and Unmonitored. • Type—All, Access, Core, Distribution, Router, Wireless, and Other. • Overall Health—Poor, Fair, and Good. <ul style="list-style-type: none"> • Poor—Devices with a health score range from 1 to 3. • Fair—Devices with a health score range from 4 to 7. • Good—Devices with a health score range from 8 to 10. • View device information for all the devices in the network or for a selected site. • Note The Overall Health Score is the minimum sub-score of the following KPI metric health scores: System Health, Data Plane Connectivity, and Control Plane Connectivity. • Display a 360° view of a device by clicking the device name from the Device column. • Export the device information to a CSV file.

Step 3 To display a 360° view of the device, do one of the following:

- In the **Network Devices** dashlet, click the device name from the **Device** column.
- In the **Search field** (located on the top-right corner), enter one of the following: device name, IP address, or MAC address.

Global Network Health Summary Score or Site Health Summary Score

The Global Network Health Summary score or Site Health Summary score is a percentage of the number of healthy network devices (a health score from 8 to 10) divided by the total number of network devices. The score is calculated every 5 minutes.

For example: 90% health score = 90 network devices with health score from 8 to 10 / 100 network devices.

Device Category Health Score

The Device Category Health score (Access, Core, Distribution, Router, Wireless) is the percentage of the number of healthy network devices (a health score from 8 to 10) in a target category, divided by the total number of network devices in that category. The score is calculated every 5 minutes.

For example: 90% health score = 90 network devices in a target category with health score from 8 to 10 / 100 network devices in that category.

Individual Device Health Score

The Individual Device Health score is the minimum score of following KPI metric health scores: System Health, Data Plane Connectivity, and Control Plane Connectivity. The KPI metric score is based on the threshold that is defined per KPI.

Device Health Score = MIN (System Health, Data Plane Connectivity, Control Plane Connectivity)

Depending on the type of device, the metrics vary.

System Health

Switch (Access and Distribution)—Includes system-monitoring metrics, such as CPU utilization and memory utilization.

Wireless—Includes the following system-monitoring metrics:

- For Cisco WLC, it includes memory utilization, free timers, and free Mbufs.
- For AP, it includes CPU utilization and memory utilization.

Router—Includes system-monitoring metrics, such as CPU utilization and memory utilization.

Fabric—Includes system-monitoring metrics, such as CPU utilization and memory utilization.

Data Plane Connectivity

Switch (Access and Distribution)—Includes metrics, such as link errors and link status.

Wireless—Includes the following metrics:

- For Cisco WLC, it includes metrics, such as WQE pool, packet pools, and link errors.
- For AP, it includes RF metrics, such as interface, noise, air quality, and radio utilization.

Router—Includes metrics, such as link errors.

Control Plane Connectivity—Available for Fabric Devices Only

Wireless—Includes the following KPIs:

- For Cisco WLC, it includes connectivity to MAP servers.
- For fabric devices, it includes metrics, such as connectivity to MSMR.

Monitor and Troubleshoot the Health of a Device

Use this procedure to view details about a specific device and to determine if there are potential issues that must be addressed.

Procedure

- Step 1** From the DNA Center home page, click the **Assurance** tab.
The **Overall Health** page appears.
- Step 2** Click **Network**.
The **Network Health** page appears.
- Step 3** Do one of the following:
 - From the **Network Devices** dashlet, click the device name from the **Device** column.
 - In the **Search** field (located on the top-right corner), enter the device name, IP address, or MAC address.A 360° view of the device appears with the following information:

Table 56: Device 360 Page

Item	Description
Device Health Score	<p>Health score of a device:</p> <ul style="list-style-type: none"> • Switch—The Switch Health score is the minimum subscore of the following parameters: memory utilization, CPU utilization, link errors, and link status. In addition, for fabric devices, it includes connectivity to MAP servers. For more information, see Switch Health Score, on page 257. • Router—The Router Health score is the minimum subscore of the following parameters: memory utilization, CPU utilization and link errors. For more information, see Router Health Score, on page 257. • AP—The AP Health score is the minimum subscore of the following parameters: memory utilization, CPU utilization, link errors, radio utilization, interference, noise, and air quality. For more information, see AP Health Score, on page 258. • WLC—The Cisco WLC Health score is the minimum subscore of the following parameters: memory utilization, free timers, free memory buffers, wqe pools, packet pools, link errors, and for fabric WLCs only, it includes connection to MAP servers. For more information, see Cisco WLC Health Score, on page 259. <p>The color of the health score represents its severity. The health is measured on a scale of 1 to 10, with 10 being the best score, and a score of 0 where data could not be obtained.</p> <ul style="list-style-type: none"> • Red—Critical issues. Health score range is 1 to 3. • Orange—Warnings. Health score range is 4 to 7. • Green—No errors or warning. Health score range is 8 to 10. • Grey—No data available. Health score is 0.
Device Information bar	Information about a device, such as the building and floor where the device is located. The Cisco IOS software version installed on the device, the IP address or MAC address, and the uptime.
Historical Health Graph area	<p>Health information about the selected network device over a period of time.</p> <p>To get the health score at a particular time, hover your cursor over the time instance on the graph, for example, you can hover your cursor at 7:00, 7:05, 7:20, and so on.</p> <p>When you click a time, for example, 7:05, the entire page is refreshed providing updates for that point of time. Note that the timestamp next to each category (Issues, Connectivity, and so on) is also refreshed.</p>

- Step 4** View information about issues, physical neighbor topology, path trace, application experience, and detail information under the appropriate category.

Table 57: Categories in the Device 360 Page

Category	Description
Issues category	Issues, if any, that must be addressed. Issues are listed based on the time stamp, the most recent issue is listed first. Click an issue to display details, such as the summary of the issue, impact, and suggested actions. To resolve an issue, from the Status field, choose Resolve . Click View All Issues to open the Issues page. For information about the types of issues, see Issues Detected by DNA Center Assurance, on page 299 .
Physical Neighbor Topology category	Displays a topology view of a specific device and shows how that device is connected to neighboring devices.
Path Trace category	Click Run New Path Trace to display a network topology between a specified source device and a destination device. The topology includes the path's direction and the devices along the path (including their IP addresses). The display also shows the protocol of the devices along the path, Switched , STP , ECMP , Routed , Trace Route , or other source type. See Perform a Path Trace, on page 274 .
Detail Information category	Historical KPIs performing over a period of time displayed in appropriate charts.
Connectivity category	Health of the device's connection with the network.

- Step 5** To view additional attributes of a device, such as general information, network information, and rack location, click the **View Details** tab located on the top-right corner.

Enable SNMP Collector Metrics for Fabric Devices

For the health score to populate correctly for fabric devices, you must enable the SNMP Collector metrics.

Procedure

- Step 1** From the DNA Center home page, click the gear icon , and then choose **System Settings > Data Platform**.
- Step 2** Click **Collectors**.
A list of collectors are displayed.
- Step 3** Click **Collector-SNMP**.

The **Collector-SNMP** window appears.

Step 4 Click **+ Add**.

The **SNMP Configuration** side bar opens.

Step 5 Select the check boxes adjacent to all the metrics except QOS.

Figure 8: SNMP Configuration

- Step 6** In the **Configuration Name** field, enter a unique name for the SNMP configuration.
- Step 7** Click **Save Configuration**.

Switch Health Score

The Switch Health score is the minimum subscore of the following parameters:

- **CPU Utilization:**
 - If CPU utilization is 95 percent or less, the score is 10.
 - If CPU utilization is more than 95 percent, the score is 1.
- **Memory Utilization:**
 - If memory utilization is 95 percent or less, the score is 10.
 - If memory utilization is more than 95 percent, the score is 1.
- **Link Errors (Rx and Tx):**
 - If link errors are 1 percent or less, the score is 10.
 - If link errors are more than 1 percent, the score is 1.
- **Link Status:**
 - If link status is LINK UP, the score is 10.
 - If link status is LINK DOWN, the score is 1.
- **Connection to Control Plane Node—Fabric Devices Only (Edge and Border):**
 - If the Control Plane node is reachable, the score is 10.
 - If the Control Plane node is unreachable, the score is 1.



Note If there is more than 1 Control Plane node in a fabric domain, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1.



Note For the health score to populate correctly for fabric devices, enable SNMP Collector metrics. See [Enable SNMP Collector Metrics for Fabric Devices, on page 254](#).

Router Health Score

The Router Health the score is the minimum subscore of the following parameters:

- **CPU Utilization:**
 - If CPU utilization is 95 percent or less, the score is 10.
 - If CPU utilization is more than 95 percent, the score is 1.
- **Memory Utilization:**
 - If memory utilization is 95 percent or less, the score is 10.
 - If memory utilization is more than 95 percent, the score is 1.
- **Link Errors:**
 - If interface errors are 1 percent or less, the score is 10.
 - If interface errors are more than 1 percent, the score is 1.

AP Health Score

The AP Health the score is the minimum subscore of the following parameters:

- **CPU Utilization:**
 - If CPU utilization is 90 percent or less, the score is 10.
 - If CPU utilization is more than 90 percent, the score is 1.
- **Memory Utilization:**
 - If memory utilization is less than 90 percent, the score is 10.
 - If available memory is 90 percent or more, the score is 1.
- **Radio Utilization Score** (calculated individually for each radio, and then the average radio the score is determined):
 - If radio utilization is less than 60 percent, the score is 10.
 - If radio utilization is 60 percent or more, the score is 0.
- **Interference Score** (calculated individually for each radio, and then the average radio the score is determined):
 - If interference is less than or equal to 30 percent for 5 GHz radio and less than or equal to 50 percent for 2.4 GHz radio, the score is 10.
 - If interference is more than 30 percent for 5 GHz radio and more than 50 percent for 2.4 GHz radio, the score is 0.
- **RF Noise Score** (calculated individually for each radio, and then the average radio the score is determined):
 - If RF noise is less than -70dBm, the score is 10.
 - If RF noise is -70dBm or more, the score is 0.

- **Air Quality Score** (calculated individually for each radio, and then the average radio the score is determined):
 - If air quality is 40 percent or more, the score is 10.
 - If air quality is less than 40 percent, the score is 0.

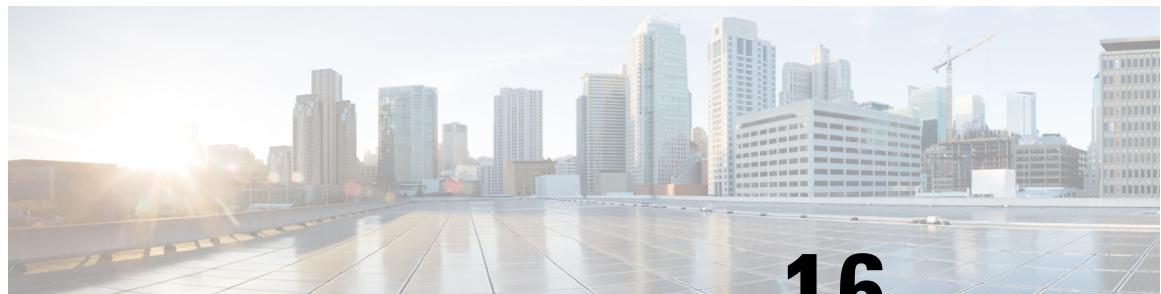
Cisco WLC Health Score

The Cisco WLC Health score is the minimum subscore of the following parameters:

- **Memory Utilization:**
 - If memory utilization is less than 90 percent, the score is 10.
 - If the available memory is 90 percent or more, the score is 1.
- **Free Timer Score:**
 - If the number of free timers is 20 percent or more, the score is 10.
 - If the number of free timers is 20 percent or less, the score is 1.
- **Free Memory Buffers (MBufs):**
 - If the number of free memory buffer is 20 percent or more, the score is 10.
 - If the number of free memory buffer is less than 20 percent, the score is 1.
- **Work Queue Element (wqe) Pool Score:**
 - If the wqe pool is greater than wqe pool threshold, the score is 10.
 - If the wqe pool is at the same level as or lower than the wqe pool threshold, the score is 1.
- **Packet Pools:**
 - If the packet pool is greater than the packet pool threshold, the score is 10.
 - If the packet pool is at the same level as or lower than the packet pool threshold, the score is 1.
- **Link Errors:**
 - If link errors are less than 1 percent, the score is 10.
 - If link errors are 1 percent or more, the score is 1.
- **Connection to Control Plane Node—Fabric WLC Only:**
 - If the Control Plane node is reachable, the score is good.
 - If the Control Plane node is unreachable, the score is poor.

**Note**

If there is more than 1 Control Plane node in a fabric domain, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1.



CHAPTER 16

Assure Client Health

- [About Clients, on page 261](#)
- [Monitor and Troubleshoot the Health of All Client Devices, on page 261](#)
- [Monitor and Troubleshoot the Health of a Client Device , on page 270](#)
- [Trace the Path of a Device, on page 273](#)

About Clients

A client is an end device (computer, phone, and so on) that is connected to a network device (access point or switch). DNA Center supports both wired and wireless clients.

Monitor and Troubleshoot the Health of All Client Devices

A client is an end device (computer, phone, and so on) that is connected to a network device (access point or switch). DNA Center supports both wired and wireless clients.

Use this procedure to get a global view of the health of all the wired and wireless client devices and to determine if there are potential issues that must be addressed.

Before you begin

Configure DNA Center Assurance. See [Basic Workflow for Configuring DNA Center Assurance, on page 235](#).

Procedure

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

The **Overall Health** page appears.

Step 2 Click **Health > Clients**.

The **Client Health** page appears with the following information.

The colors in the charts represent the health of the client devices.

- Red—Poor client devices. Health score range is 1 to 3.

Monitor and Troubleshoot the Health of All Client Devices

- Orange—Fair client devices. Health score range is 4 to 7.
- Green—Good client devices. Health score range is 8 to 10.
- Grey—Inactive client devices. Health score is 0.

Table 58: Client Health Page

Item	Description
All SSIDs, All Bands, and Actions drop-down list	<ul style="list-style-type: none"> • All SSIDs—Displays information for the SSID you choose from the drop-down list. Default is All SSIDs. • All Bands—Displays information for the band frequency you choose from the drop-down list. Options are: 2.4 GHz, 5 GHz, or All Bands. • Actions—Allows you to make changes to the dashboard display when you choose Edit Dashboards from the drop-down list. See Change the Position of a Dashlet, on page 297 and Create a Custom Dashboard, on page 293.
24 Hours drop-down list and Timeline Slider	<ul style="list-style-type: none"> • 24 Hours—Displays information on the page based on the time range you select. Do the following: <ol style="list-style-type: none"> 1. From the 24 Hours drop-down list, choose a time range: 3 hours, 24 hours, or 7 days. 2. Specify the Start date and time; and the End date and time. 3. Click Apply. This sets the time boundaries on the timeline slider. • Timeline Slider—Allows you to specify a more granular time range. Move the timeline slider to the desired time range, and then click Apply.

Item	Description
Client Health Map or Hierarchical Site/Building View dashlet	<p>The Hide or Show button, allows you to hide or display this dashlet. By default, the Client Health Map dashlet displays.</p> <p>This dashlet contains two buttons that allow you to display the health of the client devices in a map view or site/building view.</p> <ul style="list-style-type: none">• Client Health Map—Click the map button to display health of all the client sites on a geographic location-oriented client health map. By default, the client sites that are represented are color-coded according to the severity of the problem.• Hierarchical Site/Building View—Click the site button, and then choose the hierarchical site view or building view from the drop-down list. Based on what you choose, the table provides the relevant information. To view information about a specific site, building, or floor, click Apply in the appropriate row, the information on the page refreshes based on your selection.

Monitor and Troubleshoot the Health of All Client Devices

Item	Description
Client Health dashlet	<p>This dashlet includes the following information:</p> <ul style="list-style-type: none"> • Client Health Summary area—Contains a Client Health Summary score and a client count distribution trend chart. The Client Health Summary score is the percentage of healthy (good) wired and wireless client devices in your overall network or selected site. The client count distribution trend chart (located below the health score) shows the count of all clients over time, shown as a stacked area chart based on their health scores. See Client Health Summary Score, on page 268. • Wireless and Wired areas—Contains the following: <ul style="list-style-type: none"> • Score—The client category (Wired and Wireless) health score is the percentage of healthy (good) client devices in a target category. See Client Category Health Score, on page 268. • Trend Chart—Health of clients displayed in a trend chart (located on the right of the health score). • Donut Chart—Provides a count of poor, fair, good, and inactive client devices. The client devices are color-coded and broken down according to the severity of the scores. Hover your cursor over a specific color on the donut chart to display the number of clients associated with that color. <ul style="list-style-type: none"> • Red—Poor client devices. Health score range is 1 to 3. • Orange—Fair client devices. Health score range is 4 to 7. • Green—Good client devices. Health score range is 8 to 10. • Grey—Inactive client devices. Health score is 0. <p>Click View Details to open a side bar with additional details. From the side bar, click a color in the chart to populate or refresh the data in the table below.</p>

Item	Description
Client Onboarding Times, Connectivity RSSI, Connectivity SNR, Client Count Per SSID, Client Count Per Band, DNS, and Connectivity Physical Link dashlets	<p>Analyzes the health of the client devices every 30 minutes and updates the charts in the dashlets listed below. Click a dashlet to open a side bar with additional drill-down capabilities.</p> <ul style="list-style-type: none"> • Client Onboarding Times—Distribution of all client's attempts to onboard, in all sites or a selected site, over time. • Connectivity RSSI—Received Signal Strength Indication (RSSI) distribution for all clients, in all sites or a selected site. • Connectivity SNR—Signal-to-Noise ratio (SNR) distribution for all clients, in all sites or a selected site. • Client Count Per SSID—Distribution of the number of clients per SSID, in all sites or a selected site, over time. • Client Count Per Band—Distribution of the number of clients per band frequency (2.4 GHz and 5 GHz), in all sites or a selected site, over time. • DNS—Distribution of the DNS requests and response counters, in all sites or a selected site, over time. • Connectivity Physical Link—Distribution of wired client device link state: the number of devices that had their physical links up, down, and had errors. <p>Click View Details to open a side bar with additional details. From the side bar, click a color in the chart to populate or refresh the data in the table below.</p>

Monitor and Troubleshoot the Health of All Client Devices

Item	Description
Client Devices Table dashlet	

Item	Description
	<p>Allows you filter, view, and export client device information:</p> <ul style="list-style-type: none"> • Filter the table based on client type, client health, and data. • Client Type—Options are wired and wireless clients. • Client Health—Options are: <ul style="list-style-type: none"> • Poor—Client devices with a health score range from 1 to 3. • Fair—Client devices with a health score range from 4 to 7. • Good—Client devices with a health score range from 8 to 10. • Inactive—Client devices with a health score of 0. • Data—Options are Onboarding Time > Threshold, Association Time > Threshold, DHCP > Threshold, AAA > Threshold, and RSSI > Threshold. <p>To determine the threshold values for onboarding, association time, DHCP, and AAA, from the Client Attempts on Onboarding Time dashlet, click View Details. From the side bar that opens, click the appropriate option, and then view the value in the Threshold legend.</p> <p>To determine the threshold value for RSSI, see the Threshold legend in the Connectivity RSSI dashlet.</p> <ul style="list-style-type: none"> • View client device information in a table format. The client device table lists information about client devices, such as user ID, hostname, MAC address, IP address, device type, last heard, location, VLAN ID, SSID, and the following information: <ul style="list-style-type: none"> • Overall Health Score—This score is the sum of the onboarding and connected scores. • Onboarding Score—Indicates the experience of a client device <i>while</i> connecting to the network; whether the client connected (onboarded) to the network successfully or not. For more information, see Client Onboarding Score, on page 268. • Connected Score—Indicates the experience of a client device <i>after</i> the device is connected to the network. For more information, see Client Connectivity Score, on page 269. • Connected To—Provides the following information: <ul style="list-style-type: none"> • Wireless Clients—Provides the name of the AP or Cisco WLC to which the client device is connected. • Wired Client—Provides the name of the switch to which the client device is connected.

Client Health Summary Score

Item	Description
	<ul style="list-style-type: none"> • Display a 360° view of a client by clicking the MAC address of a client device.

Step 3 To display a 360° view of the client, do one of the following:

- In the **Client Devices** table, click the MAC address of the device.
 - In the **Search field** (located on the top-right corner), enter one of the following: host name, user ID (authenticated through Cisco ISE), IP address, or MAC address.
-

Client Health Summary Score

The Client Health Summary score is the percentage of the number of healthy client devices (a health score from 8 to 10) divided by the total number of client devices. The score is calculated every 5 minutes.

For example: 90% health score = 90 client devices with health score from 8 to 10 / 100 client devices.

Client Category Health Score

The Client Category Health score (Wireless or Wired) is the percentage of the number of healthy client devices (a health score from 8 to 10) in a target category, divided by the total number of client devices in that category. The score is calculated every 5 minutes.

For example: 90% health score = 90 client devices in a target category with health score from 8 to 10 / 100 client devices in that category.

The Individual Client Health score is the sum of the Client Onboarding score and the Client Connectivity score. The client health score ranges from 1 to 10, with a score of 0 for inactive clients. It is calculated as follows:

- **Wired Client**—Link to first switch is up, authentication and authorization is successful, IP address is received. Client score is 10.
- **Wireless Client**—Client joined the network and has good connection in terms of the RSSI and SNR KPIs.

Client Onboarding Score

The Client Onboarding score indicates the experience of a client device *while* connecting to the network.

- If a client connects to the network successfully, the score is 4.
- If a client is unable to connect to the network, the score is 1.

The Client Onboarding score is calculated as follows:

- **Wired Client**—Link to the first switch is up, authentication and authorization is successful, and IP address is received.

- **Wireless Client**—Client Onboarding score range is from 1 to 4. When the client connects to the network successfully, the score is 4. If the client is unable to connect to the network, the score is 1.

Client Connectivity Score

The Client Connectivity score indicates the experience of the client device *after* the device is connected to the network.

The Client Connectivity score is calculated as follows:

- **Wired Client**—Connectivity score can be 0, 2, or 6. Connectivity to the DNS server or link errors determines the Connectivity score and the resulting Overall Health score as shown below:
 - If a client onboards successfully, but is unable to connect to the DNS server, the Connectivity score is 0.
 - If a client onboards successfully and is able to connect to a DNS server, but has link errors, the Connectivity score is 2 and the Overall Health score is 6.
 - If the client onboards successfully and there are no link errors between the client and the first hop switch, the Connectivity score is 6 and the Overall Health score is 10.
- **Wireless Client**—Connectivity score range is 0 - 6. The RSSI and SNR range determines the Connectivity score and the resulting Overall Health score is calculated as the weighted average of the RSSI-driven Connectivity score and the SNR-driven Connectivity score.

RSSI-Driven Connectivity Score

- If RSSI is less than -72 dBm, the RSSI-Driven Connectivity score is 0.
- If RSSI is equal to -71 dBm, the RSSI-Driven Connectivity score is 1.
- If RSSI is equal to -70 dBm, the RSSI-Driven Connectivity score is 2.
- If RSSI is equal to -69 dBm, the RSSI-Driven Connectivity score is 3.
- If RSSI is equal to or greater than -68 dBm and less than -55 dBm, the RSSI-Driven Connectivity score is 4.
- If RSSI is equal to or greater than -55 dBm and less than -45 dBm, the RSSI-Driven Connectivity score is 5.
- If RSSI is equal to or greater than -45 dBm, the RSSI-Driven Connectivity score is 6.

SNR-Driven Connectivity Score

- If SNR is from 0 to 9, the SNR-Driven Connectivity score is 0.
- If SNR is equal to 10, the SNR-Driven Connectivity score is 1.
- If SNR is 11 or 12, the SNR-Driven Connectivity score is 2.
- If SNR is 13 or 14, the SNR-Driven Connectivity score is 3.
- If SNR is 15, 16, 17, 18, or 19, the SNR-Driven Connectivity score is 4.
- If SNR is from 20 to 39, the SNR-Driven Connectivity score is 5.

- If SNR is equal to or greater than 40, the SNR-Driven Connectivity score is 6.

Monitor and Troubleshoot the Health of a Client Device

Use this procedure to view details about a specific client device and to determine if there are potential issues that must be addressed.

Procedure

- Step 1** From the DNA Center home page, click the **Assurance** tab.
The **Overall Health** page appears.
- Step 2** Click **Clients**.
The **Client Health** page appears.
- Step 3** Do one of the following:
 - In the **Client Devices** table, click the MAC address of the device.
 - In the **Search field** (located on the top-right corner), enter one of the following: host name, user ID (authenticated through Cisco ISE), IP address, or MAC address.

A 360° view of the client device appears with the following information.

Table 59: Client 360 Page

Item	Description
Individual Client Health Score	<p>If you search by the host name or user ID, the Individual Client Health score that is displayed is the minimum score of all the monitored client devices associated with that user. For more information, see Individual Client Health Score, on page 273.</p> <p>If you search by MAC address or IP address, the Individual Client Health score is the health score for that client device.</p> <p>The color of the health score represents its severity. The health is measured on a scale of 1 to 10, with 10 being the best score, and a score of 0 where data could not be obtained.</p> <ul style="list-style-type: none"> • Red—Poor client devices. Health score range is 1 to 3. • Orange—Fair client devices. Health score range is 4 to 7. • Green—Good client devices. Health score range is 8 to 10. • Grey—Inactive client devices. Health score is 0. <p>Note For clients that are disconnected from the network, the score is represented as a --.</p>

Item	Description
Client Device tabs	<p>Details about each of the client's devices is represented in a separate tab, for example, <i>username-macbook</i> or <i>username-iphone</i>.</p> <p>Hover your cursor over a tab to view details about a device, such as device type, OS version, MAC address, and IP address.</p>
Historical Health, Events, and Band Frequency Graph	<p>Health, events, and band frequency information about the selected client device over a period of time displayed in a graph.</p> <ul style="list-style-type: none"> • Health—To obtain the health score at a particular time, hover your cursor over the time instance on the graph, for example, you can hover your cursor at 7:00, 7:05, 7:20, and so on. When you click a time, for example, 7:05, the entire page is refreshed, providing updates for that point of time. Note that the timestamp next to each category (Issues, Onboarding, Event Viewer, Connectivity, and so on) is also refreshed. • Events—Event data is displayed by color-coded vertical bars on the graph. Green vertical bars indicate successful event(s) and the red vertical bars indicate event(s) that failed. Each vertical bar represents 5-minutes of time. Multiple significant events can be generated during each 5-minute window. Hover your cursor over the vertical bar to get more information about the event(s). • Band—Band frequency data is color-coded and displayed as a horizontal line at the bottom of the graph. Light blue color represents 2.4 GHz band frequency and purple color represents 5 GHz band frequency. A gap in the horizontal line indicates that either the client device is not connected to the network or that the client device is not sending data. <p>If you do not want to view the event or band frequency data in the graph, uncheck the Events or Band check box in the Displayed Data area.</p>

- Step 4** View information about issues, onboarding, event viewer, path trace, application experience, and detail information under the appropriate category.

Table 60: Categories in the Client 360 Page

Category	Description
Issues category	<p>Issues, if any, that must be addressed. Issues are listed based on the time stamp, the most recent issue is listed first.</p> <p>Click an issue to display details, such as the summary of the issue, impact, and suggested actions. To resolve an issue, from the Status field, choose Resolve.</p> <p>Click View All Issues to open the Issues page.</p> <p>For information about the types of issues, see Issues Detected by DNA Center Assurance, on page 299.</p>
Onboarding category	<p>Topology of how a client got on the network, including information about the following services: AAA, DHCP, and DNS.</p> <p>Example of wired client topology: Client > Switch > Router</p> <p>Example of wireless client topology: Client > SSID > Access Point > WLC</p>
Event Viewer category	<p>Lists scenarios and the sequence of sub-events that led to each scenario. This allows you to pin-point during which sub-event an issue occurred. The following scenarios are provided:</p> <ul style="list-style-type: none"> • Re-Authentication • Broadcast Rekey—Process of changing the session key—the encryption key of an ongoing communication—in order to limit the amount of data encrypted with the same key. • Onboarding • Delete • INTRA-Roaming <p>When an issue occurs, that event is marked red, otherwise it is green. The second column provides additional information about the issue, such as the error message, and the AP and Cisco WLC to which the client device is connected. The third column provides the time stamp when the event occurred.</p> <p>Click an event, to view details about that event in the right pane.</p>
Path Trace category	<p>Click Run New Path Trace to display a network topology between a specified source device and a destination device. The topology includes the path's direction and the devices along the path (including their IP addresses). The display also shows the protocol of the devices along the path, Switched, STP, ECMP, Routed, Trace Route, or other source type.</p> <p>See Perform a Path Trace, on page 274.</p>

Category	Description
Application Experience category	<p>Applications running on a client device with their qualitative and quantitative metrics.</p> <p>To view the metrics in a chart format, select the radio button next to an application in the table. A side bar opens with the relevant information.</p> <p>See About Application Experience, on page 277 and View the Application Experience of a Client Device, on page 278.</p>
Detail Information category	<p>Contains the following tabs: Device Info, RF, and Connectivity. Click each tab to get the appropriate information.</p> <p>Note For Apple devices, the iOS Analytics tab is also provided.</p>

Individual Client Health Score

The Individual Client Health score is the sum of the Client Onboarding score and the Client Connectivity score. The client health score ranges from 1 to 10, with a score of 0 for inactive clients. It is calculated as follows:

- **Wired Client**—Link to first switch is up, authentication and authorization is successful, IP address is received. Client score is 10.
- **Wireless Client**—Client joined the network and has good connection in terms of RSSI and SNR KPIs.

See the following topics:

- [Client Onboarding Score, on page 268](#)
- [Client Connectivity Score, on page 269](#)

Trace the Path of a Device

About Path Trace

You can perform a path trace between two nodes in your network—a specified source device and a specified destination device. The two nodes can be a combination of wired or wireless hosts and/or Layer 3 interfaces. In addition, you can specify the protocol the DNA-Center controller should use to establish the path trace connection, either TCP or UDP.

When you initiate a path trace, the DNA-Center controller reviews and collects network topology and routing data from the discovered devices. It then uses this data to calculate a path between the two hosts or Layer 3 interfaces, and displays the path in a path trace topology. The topology includes the path direction and the devices along the path (including their IP addresses). The display also shows the protocol of the devices along the path: **Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**, or other source type.

Perform a Path Trace

The path trace feature works in a similar manner in all the devices. You can perform a path trace from the **Client 360** or **Device 360** page.

Before you begin

Make sure that the devices (routers, switches, Cisco WLCs, and access points) are discovered. See [Discover Your Network Using an IP Address Range, on page 16](#) or [Discover Your Network Using CDP, on page 11](#).

Procedure

Step 1 From the **Client 360** or **Device 360** page, in the **Path Trace** category, click **Run New Path Trace**.

The **Set Up Path Trace** dialog box appears.

Step 2 Do one of the following:

- Enter the source and destination information:

Client Device—In the **Source** field, enter the IP address, host name, username, or application name from which you want the trace to start. In the **Destination** field, enter the IP address, host name, username, or application name at which you want the trace to end.

Switch or Router—In the **Source** field, enter the IP address of the host from which you want the trace to start. In the **Destination** field, enter the IP address of the host at which you want the trace to end.

- Enter the following 5-tuple values (source IP address and port number; destination IP address and port number; and the protocol in use):

1. In the **Source** field, enter the IP address of the host from which you want the trace to start.

Note The IP address in the **Source** field is prepopulated; however, you can change this.

In the **Port (optional)** field, under **Source**, enter the port number of the host from which you want the trace to start.

2. In the **Destination** field, enter the IP address of the host or the Layer 3 forwarding interface at which you want the trace to end.

In the **Port (optional)** field, under **Destination**, enter the port number of the host at which you want the trace to end.

3. Click **Show Options**.

4. From the **Protocol** drop-down list, choose either **tcp** or **udp**.

Step 3 Click **Show Options**, and then do the following, as required:

- a) (Optional) To configure the path trace topology to refresh every 30 seconds, click **Refresh Every 30secs** such that its status is **On**.
- b) (Optional) To display whether the devices have Access Control List (ACL) trace enabled, click **ACL Trace** such that its status is **On**.

Note By default, **ACL Trace** is **On**; however, you can change it to **Off**, if required.

- c) (Optional) To configure the path trace to collect additional statistics, click **Include Stats** such that its status is **On**. The following options are displayed. Check any of the check boxes, as needed:

- **Interface**—Collects and displays information about the interfaces on the devices along the path.
- **Device**—Collects and displays information, such as the device CPU and memory usage.

Step 4 Click **Start Path Trace**. The path trace topology appears.

This includes the path direction and the intermediate devices along the path, and their IP addresses. The display also shows the protocol of the devices along the path, **Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**, or other source type.

In addition, you can also view the following information from the path trace topology:

- **ACL Enabled Devices**—If **ACL Trace** is set to **On**, for the devices that have ACL enabled in them, the path trace topology displays a green check mark on top of the device; otherwise, the check mark is black.
- **Device Statistics**—If **Include Stats** is set to **On**, click the devices in the path trace topology to display the appropriate device statistics.
- **Last Updated Time Stamp**—The time stamp indicating when the path trace was last updated is displayed to the left of the topology.
- **Clients Per Device**—The number of clients per device is displayed below each device in the path trace topology.

■ Perform a Path Trace



CHAPTER 17

Monitor Application Health

- [About Application Experience, on page 277](#)
- [Enable Cisco NetFlow Collection , on page 277](#)
- [View the Application Experience of a Client Device, on page 278](#)
- [Monitor the Health of All Applications, on page 279](#)
- [Monitor the Health of an Application , on page 281](#)

About Application Experience

Application Experience (AppX) allows you to monitor the health of an application. Application health is measured using a score value, which is calculated based on the application's qualitative metrics—packet loss and network latency.

Only application client-server statistics and ART (TCP) metrics can be monitored. Application Experience is based on the Cisco NetFlow records exported by the routers.

Based on the relevancy of an application, it is classified as Business Relevant, Business Irrelevant, or Default. This classification is done based on the NBAR standard.

To enable AppX, you must enable Cisco NetFlow collection on the device. See [Enable Cisco NetFlow Collection , on page 277](#).

Enable Cisco NetFlow Collection

To view the applications running on a client device with their qualitative and quantitative metrics, you must enable Cisco NetFlow collection on the device. Do the following:

1. Add description on device interface(s) containing keyword "lan." This can be either configured on the device interface manually or by using the Template Editor tool in DNAC.
2. Resynchronize the network device to read this interface description. The Telemetry Provisioning module looks for interfaces having "lan" in the description and applies the NetFlow configuration to only those interfaces.
3. Configure and apply NetFlow Telemetry profile to network devices. See [Configure a Telemetry Profile, on page 153](#) and [Apply a Telemetry Profile to the Devices, on page 154](#).



Note NetFlow telemetry is applied only to interfaces that have description “lan” on them.

View the Application Experience of a Client Device

Use this procedure to view the applications running on a client device with their qualitative and quantitative metrics.

Before you begin

- Make sure that the devices (routers, switches, Cisco WLCs, and access points) are discovered. See [Discover Your Network Using an IP Address Range, on page 16](#) or [Discover Your Network Using CDP, on page 11](#).
- Enable Cisco NetFlow collection on the device. See [Enable Cisco NetFlow Collection , on page 277](#).

Procedure

Step 1 From the **Client 360** page, scroll down to the **Application Experience** category.

The Application Experience table displays with three tabs: Business Relevant, Business Irrelevant, or Default.

Note The information displayed in the table is based on the time you selected from the drop-down list in the Client 360 page. Options are: last 3 hours, last 24 hours, and last 7 days. Default is last 24 hours.

The following application attributes are provided in the table:

- **Name**—The application name.
- **Domain Name**—HTTP hostname used by the client to access the application.
- **Health**—The health score is calculated on the basis of a combination of metrics of packet loss and latency. For each application, you can hover your cursor over **View** to view the variations in application health score.
- **Usage**—The number of bytes transferred by the client for this application.
- **Average Throughput**—The rate of the application traffic (in Mbps) flowing between the client and server.
- **Traffic Class**—The categorization of the application based on the NBAR standard.
- **Packet Loss**—The percentage (maximum and average) of packet loss.
- **Latency**—The network latency time (maximum and average) in milliseconds.
- **Application Delay**—The application delay time (maximum and average) in milliseconds.

Note For client devices that are connected only through a Cisco WLC (without a router), the **Domain Name**, **Health**, **Packet Loss**, **Latency**, and **Application Delay** attributes in the table will be empty.

- Step 2** To view the application experience metrics in chart format in a side bar, select the radio button next to an application in the table.

Monitor the Health of All Applications

Use this procedure to get a global view of the health of all the applications.

Before you begin

- Make sure that the devices (routers, switches, Cisco WLCs, and access points) are discovered. See [Discover Your Network Using an IP Address Range, on page 16](#) or [Discover Your Network Using CDP, on page 11](#).
- Enable Cisco NetFlow collection on the device. See [Enable Cisco NetFlow Collection , on page 277](#).

Procedure

- Step 1** From the DNA Center home page, click the **Assurance** tab.

The **Overall Health** page appears.

- Step 2** Click **Health > Application**.

The **Application Health** page appears with the following information.

The colors in the chart represent the health of the business relevant applications.

- Red—Critical issues. Health score range is 1 to 3.
- Orange—Warnings. Health score range is 4 to 7.
- Green—No errors or warning. Health score range is 8 to 10.
- Grey—Unknown. Health score is unknown.

Table 61: Application Health Page

Item	Description
Application Health Summary dashlet	Contains an Application Health Summary score and an application count distribution trend chart. The Application Health Summary score is the percentage of healthy (good) business relevant applications in your overall network or selected site. The application count distribution trend chart (located next to the health score) shows the count of all business relevant applications over time, shown as a stacked area chart based on their health scores. See Application Health Score, on page 280 .

Item	Description
Last 24 Hours drop-down list and Actions drop-down list	<ul style="list-style-type: none"> • Last 24 Hours—Displays information on the page based on the time you select from the drop-down list. Options are: Last 3 hours, Last 24 hours, or Last 7 days. • Actions—Allows you to make changes to the dashboard display when you choose Edit Dashboards from the drop-down list. See Create a Custom Dashboard, on page 293.
Application dashlet	<p>Allows you to filter, view, and export application health information:</p> <ul style="list-style-type: none"> • Filter the table based on application type and health. <ul style="list-style-type: none"> • Application Type—Options are All, Business-relevant, Business-irrelevant, and Default applications. • Application Health—Options are: <ul style="list-style-type: none"> • Poor—Applications with a health score range from 1 to 3. • Fair—Applications with a health score range from 4 to 7. • Good—Applications with a health score range from 8 to 10. • All—All applications. • View application information in a table format. The application table lists information about the application, such as name, health, business class, traffic class, usage, average throughput, packet loss, latency, and application delay. • Display a 360° view of an application by clicking the name of the application.

Step 3 To display a 360° view of the application, in the **Application** table, click the name of an application.

Application Health Score

The Application Health score is the percentage of the number of healthy business relevant applications (a health score from 8 to 10), divided by the total number of business relevant applications. The score is calculated every 5 minutes.

For example: 90% health score = 90 business relevant applications with a health score from 8 to 10 / 100 business relevant applications.

Monitor the Health of an Application

Use this procedure to view details about a specific application.

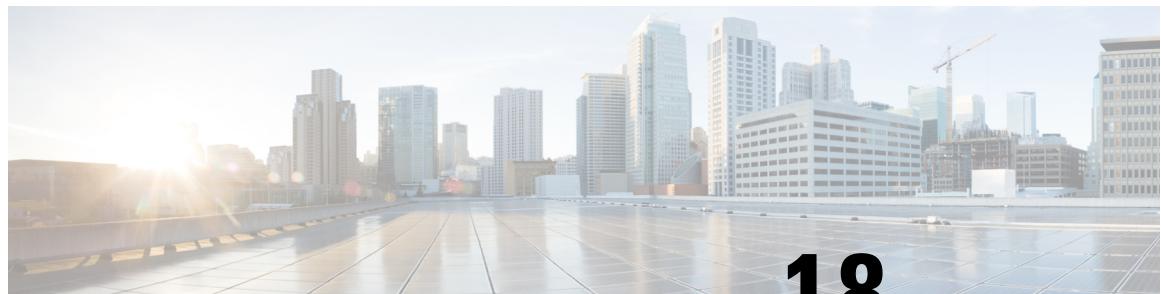
Procedure

- Step 1** From the DNA Center home page, click the **Assurance** tab.
The **Overall Health** page appears.
- Step 2** Click **Health > Application**.
The **Application Health** page appears.
- Step 3** In the **Application** table, click the name of an application.
A 360° view of the application appears with the following information.

Table 62: Application 360 Page

Item	Description
Historical Health Graph area	Health information about the selected application over a period of time. To get the application health score at a particular time, hover your cursor over the time instance on the graph, for example, you can hover your cursor at 7:00, 7:05, 7:20, and so on. Click View Details to open a side bar with additional details about the application.

Item	Description
Application Experience area	<p>View application information in a table format and chart format. The application table lists information about the application, such as average throughput, average bandwidth utilization, packet loss, latency, application delay, and the following information:</p> <ul style="list-style-type: none"> • Source Location—The client site that's accessing the particular application. <p>Click the radio button on a row to open a side bar with additional details, such as a chart for each metric and also the clients that are accessing the application. Details about each of the client's devices is shown such as the client health score, MAC address, IP address, and usage.</p> <ul style="list-style-type: none"> • Health—The health score is calculated on the basis of a combination of metrics of packet loss and latency. For each application, you can hover your cursor over View to view the variations in application health score. • Usage—The number of bytes transferred by the client for the particular application. • DSCP—Marking of the application traffic for an application and if it is preserved or not.



CHAPTER 18

Manage Sensors and Sensor-Driven Tests

- [About Sensors and Sensor-Driven Tests, on page 283](#)
- [View Sensor-Driven Tests, on page 284](#)
- [Add a Sensor-Driven Test, on page 285](#)
- [Monitor and Troubleshoot the Health of Wireless Sensors, on page 287](#)
- [Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 289](#)
- [Enable Cisco Provisioning SSID on the Cisco WLC, on page 290](#)
- [Edit, Delete, or Run a Sensor-Driven Test, on page 290](#)

About Sensors and Sensor-Driven Tests

Sensors use sensor-driven tests to test the health of wireless networks. A wireless network includes AP radios, WLAN configurations, and wireless network services.



Note Sensor functionality requires the following minimum software versions of Cisco WLC and Cisco Aironet 1800s Active Sensor images:

- Cisco WLC (35xx, 55xx, 85xx)—software release 8.5.115.0
- Cisco Aironet 1800s Active Sensor—software release 8.5.257.0

The following modes of sensors are available:

- **Dedicated Sensor**—An AP is converted into a sensor, and it stays in sensor mode (does not serve clients) unless it is manually converted back into AP mode.



Note For APs with XOR radios, for example, AP 2800, you can convert the XOR radio as a dedicated sensor.



Note **Sensor Device**—A dedicated Cisco Aironet 1800s Active Sensor. This sensor gets bootstrapped using PnP. After this sensor obtains Assurance server-reachability details, it directly communicates with the Assurance server.

- **On-Demand Sensor**—An AP is temporarily converted into a sensor to run tests. After the tests are complete, the sensor goes back to AP mode.



- Note**
- After the AP switches to sensor mode (dedicated or on-demand), it cannot serve as an AP and cannot serve clients.
 - After the AP runs as a sensor, it cannot participate in radio resource management (RRM).

View Sensor-Driven Tests

Use this procedure to view all the sensor-driven tests that are configured in the system, and to determine the tests that have passed or failed.

Before you begin

Make sure that APs are discovered. See [Discover Your Network Using an IP Address Range, on page 16](#) or [Discover Your Network Using CDP, on page 11](#).

Procedure

Step 1 From the DNA Center home page, click the **Assurance** tab, and then choose **Manage > Sensor-Driven Tests**.

The Sensor-Driven Tests page is displayed listing all the sensor-driven tests configured in the system. It provides information such as the test name, location, schedule, SSIDs, types of tests that were run, latest results, results in the last 24 hours, and the time the last test was run.

Note In the test results, the colors indicate the following:

- **Green**—Pass
- **Red**—Fail
- **Yellow**—Slow. Test passed but the test completion time was above the threshold.

Note For Onboarding and IP addressing, the threshold is 5 seconds.

For all other sensor-driven tests, the threshold is 2 seconds.

Step 2 From the **Details** column, click **View**.

A side bar opens providing details, such as the sensor and AP combination used for the sensor-driven tests.

- Step 3** If a test fails, the **Latest** column displays a red box. Click **Fail** to display information about the failed test.
- Step 4** If a test is slow, the **Latest** column displays a yellow box. Click **Show** to display information about the slow test.

Add a Sensor-Driven Test

Use the **Add Test** wizard to add and schedule a new sensor-driven test, select the tests to run, and then select APs to run as sensors. After you select an AP to run as a sensor, that sensor acts as a client and tests the health of the wireless clients, such as AP radios, WLAN configurations, and network services.

Before you begin

- Make sure that APs are discovered. See [Discover Your Network Using an IP Address Range, on page 16](#) or [Discover Your Network Using CDP, on page 11](#).
- If you are using the Cisco Aironet 1800s Active Sensor to run sensor-driven tests, make sure that the sensors are provisioned using PnP, so that they show up in the Inventory. See [Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 289](#)

Procedure

- Step 1** From the DNA Center home page, click the **Assurance tab**, and then choose **Manage > Sensor-Driven Tests**. The **Sensor-Driven Tests** page appears listing all the sensor-driven tests configured in the system.
- Step 2** To add a new sensor, click **+ Add Test** at the top-right corner. The Add Test window opens and the first step, **Schedule Tests**, is displayed. Do the following:
- a) In the **Test Name** field, enter the name of the sensor-driven test. Use letters, numbers, underscores, hyphens, and periods.
 - b) From the **Location** drop-down list, choose the location of the sensor. A table displays with all the SSIDs, radios to test, security, and credentials.
 - c) In the **Radios to Test** column, check the check box adjacent to the radios that you want to add to the test.
 - d) In the **Credentials** column, enter the username and password if required.
 - e) From the **EAP** drop-down list, choose the Extensible Authentication Protocol (EAP) method. The three methods supported are EAP-FAST, PEAP-MSCHAPv2, and EAP-TLS. If you select the EAP-TLS method, you can select and upload a certificate (PKCS bundle) that is needed for the EAP-TLS. Then enter the password associated with the certificate. Using this certificate and password, the test is created, which is used to connect to the SSIDs.
 - f) Applicable for WebAuth Enabled SSIDs—For Layer 3 security if WebAuth is enabled on the SSID, provide the following:
 - For WebAuth with user authentication, provide the necessary credentials.
 - For WebAuth with Passthrough, you can choose to provide an email address.

- Note**
- Only **Internal Authentication** is supported for sensor testing.
 - WebAuth is supported on Cisco WLC and Cisco Aironet 1800s Active Sensors, with software release 8.7.

g) From the **Interval Hours** drop-down list, choose the day and time to run the test. Default is every hour.

Step 3 Click **Next**. The second step, **Select Tests**, is displayed.

Step 4 From the **Select Tests** widow, select the tests to run. Do the following:

a) Check the check boxes for the **Network Tests** that you want to run, and then enter the required information for those tests.

Options are IP addressing, DNS, host reachability, and RADIUS tests:

- **IP Addressing Tests (DHCPv4)**—Connects to the SSID with credentials and gets the IP address through DHCP. It then verifies the gateway and DNS server received through DHCP.
- **DNS Tests**—Resolves IP address for the domain name.
- **Host Reachability Tests**—Verifies reachability using the Internet Control Message Protocol (ICMP) echo request.
- **Radius Tests**—The sensor acts as a Dot1x supplicant and authenticates through wireless. Dot1x supplicant supports protocols such as Protected Extensible Authentication Protocol (PEAP) with Password Authentication Protocol (PAP) or the Microsoft version of the Challenge-Handshake Authentication Protocol (MS-CHAP).

b) Check the check boxes for the **Application Tests** that you want to run, and then enter the required information for those tests.

Options are email, file transfer, and web tests:

- **Email Tests**—Includes the following:
 - **Internet Message Access Protocol (IMAP)**—Connects to IMAP server TCP port (143).
 - **Post Office Protocol3 (POP3)**—Connects to POP3 server TCP port (110).
 - **Outlook Web Server (OWS)**—Logs into the OWS and verifies access.
- **File Transfer Tests**—Tests for upload and download file operation.
- **Web Tests**—Tests for access to the provided URL and verifies the response data.

Step 5 Click **Next**. The third step, **Select Sensors**, is displayed.

- To set the RSSI threshold, click **Set Threshold**, and then slide the threshold slider to the desired value. From the **Number of Target APs** drop-down list, choose the number of APs you want the sensor to test against, and then click **Apply**.
- The APs that we recommend for providing the best network coverage are selected by default. A graphical view of the sensors and APs is provided in the left pane. If you approve what we recommend, click **Save**. Otherwise, select other APs to run as sensors, and then click **Save**.

Note When you select a new AP, the graphical view on the left pane changes, providing the sensor coverage percentages.

The new test is added and appears on the **Sensor-Driven Tests** page.

Monitor and Troubleshoot the Health of Wireless Sensors

Use this procedure to get a global view of the health of wireless sensors and to determine if there are potential issues that must be addressed.

Before you begin

- Make sure that APs are discovered. See [Discover Your Network Using an IP Address Range](#), on page 16 or [Discover Your Network Using CDP](#), on page 11.
- Make sure you have added and scheduled sensor-driven tests. See [Add a Sensor-Driven Test](#), on page 285.

Procedure

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

Step 2 Choose **Dashboards > Sensor**.

The **Wireless Sensor** page appears with the following information:

Table 63: Wireless Sensor Page

Item	Description
All SSIDs, All Bands, and Actions drop-down lists	<ul style="list-style-type: none">• All SSIDs—Displays information for the SSID you choose from the drop-down list. Default is All SSIDs.• All Bands—Displays information for the band frequency you choose from the drop-down list. Options are: 2.4 GHz, 5 GHz, or All Bands.• Actions—Allows you to make changes to the dashboard display when you choose Edit Dashboards from the drop-down list. See Change the Position of a Dashlet, on page 297 and Create a Custom Dashboard, on page 293.

Item	Description
24 Hours drop-down list and Timeline Slider	<ul style="list-style-type: none"> • 24 Hours—Displays information on the page based on the time range you select. Do the following: <ol style="list-style-type: none"> 1. From the 24 Hours drop-down list, choose a time range: 3 hours, 24 hours, or 7 days. 2. Specify the Start date and time; and the End date and time. 3. Click Apply. This sets the time boundaries on the timeline slider. • Timeline Slider—Allows you to specify a more granular time range. Move the timeline slider to the desired time range, and then click Apply.
Hierarchical Site/Building View dashlet	<p>The Hide or Show button, allows you to hide or display this dashlet. Click the site button, and then choose the hierarchical site view or building view from the drop-down list. Based on what you choose, the table provides the relevant information. To view information about a specific site, building, or floor, click Apply in the appropriate row, the information on the page refreshes based on your selection.</p>
Sensor Health dashlets	<p>Includes the following dashlets:</p> <ul style="list-style-type: none"> • Test Summary—Donut chart that provides a count of failed, slow, and passed sensor-driven tests. The test results are color-coded and broken down according to the severity of the scores. Hover your cursor over a specific color on the donut chart to display the number of sensor-driven tests associated with that color. • Failed Test Types—Donut chart that provides a break-down of the types of sensor-driven tests that failed. It also provides information about the number of issues that were triggered by the sensor-driven tests. <p>Click Global Issues to view sensor-driven test issues.</p> <ul style="list-style-type: none"> • Top Locations by Failure—Lists the top sites where the sensor-driven tests failed and provides the number of tests that failed per site.

Item	Description
Test Results table	<p>Lists all the sensor-driven tests configured for the site. It provides information, such as the test name, location, SSIDs, types of tests that were run, and the test results. Click View to open a side bar with additional details, such as the sensor and AP combination used for the sensor-driven tests.</p> <p>Note In the test results, the colors indicate the following:</p> <ul style="list-style-type: none"> • Green—Pass • Red—Fail • Yellow—Slow. Test passed but the test completion time was above the threshold. <p>Note For Onboarding and IP addressing tests, the threshold is 5 seconds. For all other sensor-driven tests, the threshold is 2 seconds.</p>
<i>Sensor-Driven Test</i> dashlets	<p>Provides timeline charts for the sensor-driven tests. The charts show how much time it took for the sensor to run the test. Hover your cursor over the chart to get test results at a specific time.</p> <p>Click Global Issues to view sensor-driven test issues.</p>
Sensor Devices Table dashlet	<p>Allows you to do the following:</p> <ul style="list-style-type: none"> • View information about the sensor devices in a table format. • Filter the table based on name, type, total failed, issue count, neighbor AP count, device model, and location. • Export the table in a csv format.

Provision the Wireless Cisco Aironet 1800s Active Sensor

Procedure

-
- Step 1** If you are using the Cisco Aironet AP 1800S Sensor without an Ethernet module, you must enable Cisco Provisioning SSID on the WLC. See [Enable Cisco Provisioning SSID on the Cisco WLC](#), on page 290.
- Step 2** Create a sensor profile for the Cisco Aironet 1800s Active Sensor. See [Create a Wireless Sensor Device Profile](#), on page 122.
- Step 3** Provision the Cisco Aironet 1800s Active Sensor. See [Provision a Sensor Device](#), on page 218.

- Step 4** (Optional) After the sensor device is available in the device inventory, you can choose to upgrade the software image.
-

Enable Cisco Provisioning SSID on the Cisco WLC

If you are using the Cisco Aironet AP 1800S Sensor without an Ethernet module, you must enable Cisco Provisioning SSID on the Cisco WLC.

Procedure

- Step 1** Log into Cisco WLC.

The **Network Summary** page appears.

- Step 2** Click the **Advanced** tab from the top right corner.

The **Summary** page appears.

- Step 3** Click the **Management** tab located in the top menu bar.

- Step 4** From the left-navigation pane, click **Cloud Services > Sensor**.

The **Backhaul Configuration** page appears.

- Step 5** In the SSID field, enter **TFTP**.

- Step 6** From the Auth-type drop-down list, choose **Open**.

- Step 7** From the Provisioning drop-down list, choose **Enable**.

- Step 8** Make sure that the DHCP Interface drop-down list is set to **Management**.

- Step 9** Click **Apply**.

After Provisioning is enabled, a hidden WLAN is created, called **CiscoSensorProvisioning**, and the sensor joins using an EAP-TLS client certificate. This enables the sensor to find the DNA Center IP address, which is done using DHCP Option 43 or through DNS.

What to do next

Create a wireless sensor device profile. See [Create a Wireless Sensor Device Profile, on page 122](#).

Edit, Delete, or Run a Sensor-Driven Test

Procedure

- Step 1** From the DNA Center home page, click the **Assurance tab**, and then choose **Manage > Sensor-Driven Tests**.

The **Sensor-Driven Tests** page appears listing all the sensor-driven tests configured in the system.

Step 2 To edit sensor-driven test information, check the check box next to the corresponding test, and then from the **Actions** column, click the  icon, and choose **Edit**.

The wizard similar to the Add Test wizard opens where you can update the information.

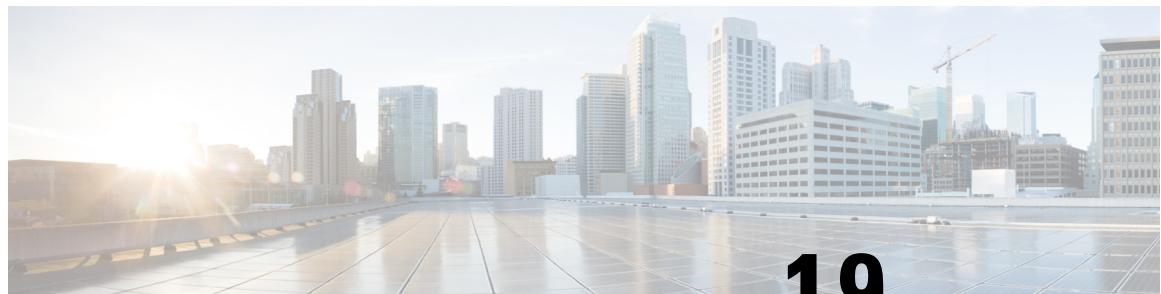
Step 3 To delete a test, check the check box next to the corresponding test, and then from the **Actions** column, click the  icon, and choose **Delete**. Click **OK** in the confirmation dialog box.

Step 4 To initiate a sensor-driven on-demand test, check the check box next to the corresponding test, and then from

the **Actions** column, click the  icon, and choose **Run Test Now**. Click **OK** in the confirmation dialog box.

Note You can schedule the sensor-driven test to run at a particular day and time from the **Add Test** wizard. See [Add a Sensor-Driven Test, on page 285](#). You can schedule to run the test on a particular day and time only once.

Edit, Delete, or Run a Sensor-Driven Test



CHAPTER 19

Manage Dashboards

- [About Dashboards, on page 293](#)
- [Create a Custom Dashboard, on page 293](#)
- [Create a Dashboard From a Template, on page 294](#)
- [View a Dashboard, on page 295](#)
- [Edit or Delete a Dashboard, on page 296](#)
- [Duplicate a Dashboard, on page 296](#)
- [Mark a Dashboard as a Favorite, on page 297](#)
- [Change the Position of a Dashlet , on page 297](#)

About Dashboards

You can create custom dashboards for monitoring your network. Dashboards contain one or more dashlets, which include charts, tables, geographic maps, and other types of information.

See the following topics for more information:

- [Create a Custom Dashboard, on page 293](#)
- [Create a Dashboard From a Template, on page 294](#)
- [View a Dashboard, on page 295](#)
- [Edit or Delete a Dashboard, on page 296](#)
- [Duplicate a Dashboard, on page 296](#)
- [Mark a Dashboard as a Favorite, on page 297](#)

Create a Custom Dashboard

Procedure

- Step 1** From the DNA Center home page, choose **Assurance > Dashboards > Dashboard Library**.
The Dashboard Library page appears, listing all the defined dashboards.

- Step 2** Click **Create a Dashboard** located in the top right corner.
- Step 3** In the **Create a Dashboard** dialog box, enter a title for the dashboard.
- Step 4** Click **Save**.
- Step 5** Click **Add a Dashlet** to add content to this dashboard.
- Step 6** Choose a category from the drop-down list or use the search box at the right to find a dashlet by name or tag.
- Step 7** Click on a dashlet description to see it in the preview pane.
- Step 8** Check the check box next to each dashlet that you want to add to the dashboard.
- Step 9** Click **Add** to display the dashboard.
- Step 10** Drag and drop the dashlets to change their arrangement on the dashboard.
- Step 11** Click the trash can icon to delete a dashlet.
- Step 12** Click **Add Dashlet** to add another dashlet.
- Step 13** Click **Save** to save the dashboard.
- A confirmation dialog is displayed.
- Step 14** Click **OK**.

Create a Dashboard From a Template

Creating a dashboard from a template allows you to use scope to filter the dashboard data. Scope filters devices by location, device type, and other options.

Procedure

- Step 1** From the DNA Center home page, choose **Assurance > Dashboards > Dashboard Library**.
The Dashboard Library page appears, listing all defined dashboards and the templates (at the bottom).
- Step 2** Click on a dashboard template.
- Step 3** In the **Create a Dashboard** dialog box, enter a title for the dashboard.
- Step 4** Click **Save**.
- Step 5** If you want to use an existing scope, select an existing scope and click **Select Scope**.
Skip to Step 15 if you selected an existing scope, or continue with the next step if you want to create a new scope.
- Step 6** To create a new scope, click **Create New Scope**.
- Step 7** Enter a scope name and click **Next**.
- Step 8** Choose one or more locations to include in the scope by checking or unchecking the check boxes next to them. Type in the search field to filter locations.
- Step 9** Click **Next**.
- Step 10** If you are using the Client Health template, you can use the following filters:
- **Client Type**—Choose Wired or Wireless to include these types of devices in the scope by checking or unchecking the boxes next to them.

- **SSIDs**—Choose SSIDs to include in the scope by checking or unchecking the boxes next to them. Type in the search field to filter SSIDs. This filter applies only to wireless devices.
- **Host Name**—Enter the host names to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **Device Type**—Enter the device OS types (for example, IOS or Android) to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **MAC Address**—Enter the MAC addresses to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **IP Address**—Enter the IP addresses to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.

Step 11 If you are using the Network Health template, you can use the following filters:

- **Network Device Type**—Choose one or more device types to include in the scope by checking or unchecking the check boxes next to them. Type in the search field to filter devices.
- **Network OS**—Choose network OS versions to include in the scope by checking or unchecking the check boxes next to them. Type in the search field to filter versions.
- **IP Address**—Enter the IP addresses to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **Host Name**—Enter the host names to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.

Step 12 Click **Save** to save the scope.

A confirmation dialog is displayed.

Step 13 Click **OK**.

Step 14 Drag and drop the dashlets to change their arrangement on the dashboard, which is open in editing mode.

Step 15 Click **Save** to save the dashboard.

A confirmation dialog is displayed.

Step 16 Click **OK**.

If this is a new scope, it can take up to 15 minutes to display data in the dashboard.

View a Dashboard

Procedure

Step 1 From the DNA Center home page, choose **Assurance > Dashboards > Dashboard Library**.

The **Dashboard Library** page appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by typing its name in the **Find** field.

Step 2 To see dashboards marked as favorites, choose **Favorite Dashboards**.

Step 3 Click on the dashboard that you want to view.

Step 4 In the dashboard controls, click **Show** or **Hide** to show or hide the map, if applicable.

- Step 5** (Optional) Filter dashboard data by time period, sites, or domains by choosing the appropriate values from the filters.

Edit or Delete a Dashboard

Procedure

- Step 1** From the DNA Center home page, choose **Assurance > Dashboards > Dashboard Library**.
The **Dashboard Library** page appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by typing its name in the **Find** field.
- Step 2** Click on the dashboard that you want to edit or delete.
- Step 3** Do one of the following:
- To make changes, choose **Edit Dashboard** from the **Actions** menu. You can add or delete dashlets and drag dashlets to different positions in the dashboard. Click **Save** when you are done.
 - To delete the dashboard, choose **Delete Dashboard** from the **Actions** menu. Click **Delete** in the confirmation dialog.

Duplicate a Dashboard

Procedure

- Step 1** From the DNA Center home page, choose **Assurance > Dashboards > Dashboard Library**.
The **Dashboard Library** page appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by typing its name in the **Find** field.
- Step 2** Click on the duplicate icon for a dashboard (next to the star icon).
- Step 3** In the **Duplicate Dashboard** dialog box, enter a title for the dashboard copy.
- Step 4** Click **Save**.
- Step 5** You can change this copied dashboard by adding, deleting, or rearranging dashlets.
- Step 6** Click **Save** to save the dashboard.
A confirmation dialog is displayed.
- Step 7** Click **OK**.

Mark a Dashboard as a Favorite

Procedure

-
- Step 1** From the DNA Center home page, choose **Assurance > Dashboards > Dashboard Library**.

The **Dashboard Library** page appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by typing its name in the **Find** field.

- Step 2** Click the star icon.

You can access favorite dashboards by clicking the **Favorite Dashboards** tab.

Change the Position of a Dashlet

You can change the position of the dashlets in the Overall Health page, Network Health page, and the Client Health page.

Procedure

-
- Step 1** Do one of the following as appropriate:

- From the DNA Center, home page, choose **Assurance > Health > Overall Health**. The Overall Health page appears.
- From the DNA Center, home page, choose **Assurance > Health > Network**. The Network Health page appears.
- From the DNA Center, home page, choose **Assurance > Health > Client**. The Client Health page appears.

- Step 2** From the **Actions** menu (located on the top right corner), choose **Edit Dashboard**.

The page refreshes and becomes editable.

- Step 3** Click the dashlet that you want to move, and drag it to a different position in the dashboard.

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

Change the Position of a Dashlet



CHAPTER 20

Issues Detected by DNA Center Assurance

- [About Issues, on page 299](#)
- [View Global Issues, on page 300](#)
- [View Issue Catalog, on page 300](#)
- [Client Issues, on page 301](#)
- [Switch and Fabric Issues, on page 310](#)
- [Router Issues, on page 314](#)
- [AP and WLC Issues, on page 314](#)
- [Sensor Issues, on page 315](#)

About Issues

DNA Center Assurance provides both system-guided as well as self-guided troubleshooting. For a large number of issues, DNA Center Assurance provides a system-guided approach, where multiple Key Performance Indicators (KPIs) are correlated, and the results from tests and sensors are used to determine the root cause of the problem, and then possible actions are provided to resolve the problem. The focus is on highlighting an issue rather than monitoring data. Quite frequently, DNA Center Assurance performs the work of a Level 3 support engineer.

You can view issues from the following pages:

- **Overall Health** page—Assurance landing page.
- **Global Issues** page—Assurance > Issues tab.
- **Client 360** page—Assurance > Health > Client. From the Client Devices table, click the MAC address to display the **Client 360** page.
- **Device 360** page—Assurance > Health > Network. From the Network Devices table, **Device** column, click the device name to display the **Device 360** page.

Click an issue to display details, such as the summary of the issue, impact, and suggested actions. Some client and AP issues also show an additional floor map to aid troubleshooting. To resolve an issue, from the **Status** field, choose **Resolve**.

View Global Issues

Use this procedure to view all the issues detected by Assurance.

Procedure

-
- Step 1** From the DNA Center home page, click the **Assurance** tab, and then choose **Issues**.
The Issues page is displayed listing all the issues.
- Step 2** Click an issue to display details, such as the summary of the issue, impact, and suggested actions. Some client and AP issues also show an additional floor map to aid troubleshooting.
- Step 3** To resolve an issue, from the **Status** field, choose **Resolve**.
- Step 4** To view all the issues that are resolved, click the **Resolved** tab.
- Step 5** To view all the issues that Assurance is capable of monitoring in a customer environment, click **View Issue Catalog** (located in the top right corner). See [View Issue Catalog, on page 300](#).
-

View Issue Catalog

Use this procedure to view all the issues that Assurance is capable of monitoring in a customer environment. The page shows the types of issues that are open in a customer environment and the root cause of the issues.

Procedure

-
- Step 1** From the DNA Center home page, click the **Assurance** tab, and then choose **Issues**.
The Issues page is displayed listing all the issues.
- Step 2** Click **View Issue Catalog** (located in the top right corner).
All the issues that Assurance is capable of monitoring in a customer environment are displayed. The issues are grouped and categorized as follows:
- **Onboarding**—Displays the wireless and wired client onboarding issues.
 - **Connectivity**—Displays network connectivity issues such as OSPF, BGP tunnels, and so on.
 - **Connected**—Displays client issues.
 - **Device**—Displays device-related issues such as CPU, memory, fan, and so on.
 - **Availability**—Displays device availability issues for APs, Cisco WLCs, and so on.
 - **Utilization**—Displays utilization issues of APs, Cisco WLCs, radios, and so on.
 - **Application**—Displays Application Experience issues.
 - **Sensor Test**—Displays sensor global issues.

- Step 3** Click an issue to display its root cause.

Client Issues

Connectivity Issues

The following table provides a list of connectivity issues detected by DNA Center Assurance:

Issue	Description
Client Unable to Connect—Invalid Credentials	This client failed to authenticate due to an invalid username or password.
Client Unable to Connect—4-Way Handshake Issue Misconfigured PSK	This client failed to authenticate and complete the 4-way handshake due to a misconfigured WPA or WPA2 preshared key.
Client Unable to Connect to SSID on AP—Client Side Timeout	This client failed to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz) due to client timeout during the authentication process. Note This issue is applicable for both single clients and global clients.
<i>Value</i> Clients Unable to Connect to SSID—Credentials Rejected	<i>Value</i> clients failed to connect to <i>SSID</i> because the client credentials are getting rejected during the authentication process.
Client Unable to Connect to SSID—AAA Failure	This client failed to connect to <i>SSID</i> because of a AAA failure during the authentication phase. Note This issue is applicable for both single clients and global clients.
<i>Value</i> Clients Unable to Connect to SSID—Authentication Parameters Rejected	<i>Value</i> clients failed to connect to <i>SSID</i> because the client authentication parameters are getting rejected during the authentication process.
Client Unable to Connect to SSID on AP and WLC—AAA Server Side Timeout	This client failed to authenticate and complete the 4-way handshake <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz) and <i>WLC Name</i> because the WLC did not receive a response from the AAA server <i>IP Address</i> . Note This issue is applicable for both single clients and global clients.
Client Unable to Connect to SSID on WLC—Security Parameter Mismatch	This client failed to authenticate and complete the authentication because the security parameters have a mismatch issue. Note This issue is applicable for both single clients and global clients.

Issue	Description
Value Clients Unable to Connect to SSID on WLC—WLC Operational Errors	<i>Value</i> clients failed to connect because of operational errors on <i>WLC Name</i> during the authentication process.
Client Unable to Connect to SSID on WLC—WLC Configuration Issue	This client failed to authenticate and complete the authentication because of issues in the <i>WLC Name</i> configuration.
Value Clients Unable to Connect to SSID on WLC—WLC Operational Errors	Clients experienced WLC operational errors. <i>Value</i> clients failed to connect because of configuration issues in the <i>WLC Name</i> during the authentication process.
Client Unable to Connect to SSID through AP and WLC—Client PMK Not Found	This client failed to connect to <i>SSID</i> through the <i>AP Name</i> (2.4 GHz 5 GHz) and <i>WLC Name</i> because the client Pairwise Master Key (PMK) was not found on the AP and the WLC. Client was roaming from <i>WLC Name</i> and <i>AP Name</i> [2.4 5] GHz radio. Note This issue is applicable for both single clients and global clients.
Network Latency for Application is Above the Threshold Value.	The client <i>client-name</i> is experiencing high network latency for application <i>app-name</i> located at site <i>site-name</i> .
Dual Band Capable Client Prefers 2.4 GHz over 5 GHz Radio	This dual band capable client is consistently connecting to 2.4 GHz radio although 5 GHz radio that provides a better experience, is available. This client is on <i>SSID</i> and <i>AP Name</i> , which is connected to <i>WLC Name</i> .
Wireless Client Exhibiting Sticky Behavior	This client is maintaining an association with <i>AP Name</i> at <i>rssiThreshold</i> dBm RSSI, which is a weaker signal. The client should roam to an available AP that has a stronger signal. This client was connected to <i>SSID</i> on <i>frequency</i> GHz radio on <i>AP Name</i> in location <i>siteHierarchy</i> . The AP is connected to <i>WLC Name</i> .
802.11r FT Client Roaming Slowly	This client supports Fast Transition and is roaming slowly. This client has performed one or more full 802.1X authentications while roaming between APs when it could roam faster with 802.11r/FT.

RF Condition Issues

The following table provides a list of RF condition issues detected by DNA Center Assurance:



-
- Note** Some issues provide a floor map with AP positioning.
If Cisco Connected Mobile Experiences (CMX) is being managed, the location of the client is also provided.
-

Issue	Description
Client Associated with AP Experiencing Poor RF Condition on SSID	This client's RSSI has been below <i>Value</i> dBm for more than <i>Value</i> minutes. This client is experiencing poor RF condition because the client is unable to roam to the available neighboring APs that have better coverage.
Client Associated with AP Experiencing Poor RF Condition on AP	This AP has <i>Value</i> clients that have RSSI Values below <i>Value</i> dBm for more than <i>Value</i> minutes. These clients are considered to be in poor RF condition as their signal is weak and they are not roaming to other APs.
Client Roaming Between Two APs	This client is roaming excessively between <i>AP-Name</i> and <i>AP-Name</i> . This client is probably located in a coverage area where the signal from SSIDs is unstable, or where the signal of several SSIDs and the roaming threshold are similar.
Client Alternating Between SSID and SSID	This client is alternating excessively between <i>SSID</i> and <i>SSID</i> . This client is probably located in a coverage area where the signal from SSIDs is unstable, or where the signal of several SSIDs and the roaming threshold are similar.
Client Roaming Between Radios	This client is roaming excessively between the 2.4 GHz and 5G Hz radios on <i>AP-Name</i> .

DHCP Issues

The following table provides a list of DHCP issues detected by DNA Center Assurance:

Issue	Description
<i>Value</i> Clients Experiencing DHCP Failure on DHCP Server	<i>Value</i> clients have not been assigned an IP Address from the DHCP server <i>Server IP</i> .
<i>Value</i> Clients in AP Group Experiencing DHCP Failure	<i>Value</i> clients assigned to <i>AP Group Name</i> have not been assigned an IP address from the DHCP server <i>Server IP</i> .
Wireless Client Failed to Connect to SSID on AP (2.4 GHz 5 GHz) Because DHCP IP Addressing Timed Out	This client failed to connect to <i>SSID</i> on <i>AP Name</i> and <i>WLC Name</i> because the DHCP IP addressing from the DHCP server <i>Server IP</i> timed out. Note This issue is applicable for both single clients and global clients.
<i>Value</i> Clients Failing DHCP Attempts in AP Group Because DHCP IP Addressing Timed Out	<ul style="list-style-type: none"> DHCP Server: <i>Value</i> clients timed out and have not been assigned an IP Address from the DHCP server <i>Server IP</i>. AP Group: <i>Value</i> clients assigned to <i>AP Group Name</i> timed out and have not been assigned an IP address from the DHCP server <i>Server IP</i>.

Issue	Description
Client on SSID and Associated with AP (2.4 GHz 5 GHz) Failed to Obtain IPv4 Address from DHCP Server	<p>This client has not been assigned an IPv4 address by DHCP server <i>Server IP</i> on <i>SSID</i> over VLAN <i>VLAN-ID</i>. This DHCP server has not responded to DHCP discover requests. This client is currently associated with <i>AP Name</i> (2.4 GHz 5 GHz).</p> <p>Note This issue is applicable for both single clients and global clients.</p>
<i>Value</i> Wireless Clients Failed to Connect to SSID—No Response from DHCP Server	<p><i>Value</i> clients assigned to VLAN <i>VLAN-ID</i> in <i>Location</i> have not been assigned an IP address. The DHCP server <i>Server IP</i> is not responding to DHCP requests.</p>
Client on SSID and Associated with AP (2.4 GHz 5 GHz) Failed to Obtain IPv4 Address—Client Side Root Cause	<p>Client failed to complete the DHCP transaction with DHCP server <i>Server IP</i>. Client is associated to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz) radio.</p> <p>Note This issue is applicable for both single clients and global clients.</p>
<i>Value</i> Wireless Clients Failed to Connect to SSID—Client Side Root Cause	<p><i>Value</i> assigned to VLAN <i>VLAN-ID</i> in <i>Location</i> failed to complete the DHCP transaction with DHCP server <i>Server IP</i>.</p>
Client Failed to Obtain IPv4 Address from DHCP Server	<p>This client with <i>MAC Address</i> was has not been assigned an IPv4 address from the DHCP server <i>Server IP</i>. This DHCP server is not responding to DHCP discover requests.</p>

Apple iOS Client Issues

The following table provides a list of Apple iOS client issues detected by DNA Center Assurance:

Issue	Description
Apple iOS Client Disconnected from SSID on AP—Client Internal Event	<p>This Apple iOS client, running Apple iOS <i>iOS version</i>, got disconnected from the network because of reasons that are internal to the client, such as software or operating system actions. This client was connected to <i>SSID</i> on <i>AP Name</i> in <i>Location</i>.</p> <p>Note This issue is applicable for both single clients and global clients.</p>
Apple iOS Client Disconnected from SSID on AP—Decryption Failure	<p>This Apple iOS client failed to decrypt multiple frames from the AP, and consequently disconnected from the <i>SSID</i> on <i>AP Name</i> radio <i>radio-index</i>.</p> <p>Note This issue is applicable for both single clients and global clients.</p>
Apple iOS Client Disconnected from SSID on AP—Captive Portal Verification Failure	<p>This Apple iOS client disconnected from <i>SSID</i> on <i>AP Name</i> because the captive-portal internet verification process failed.</p> <p>Note This issue is applicable for both single clients and global clients.</p>

Client Excessive Onboarding Issues

The following table provides a list of client excessive onboarding issues detected by DNA Center Assurance:


Note

Some issues provide a floor map with AP positioning.

If Cisco Connected Mobile Experiences (CMX) is being managed, the location of the client is also provided.

Issue	Description
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Excessive Time on Authentication and Key Exchange from the Network/Server Side	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Authentication and Key Exchange took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). <p>Note This issue is applicable for both single clients and global clients.</p>
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Excessive Time on Authentication and Key Exchange Because of RF Issue on the Client Side	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Authentication and Key Exchange took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). <p>Note This issue is applicable for both single clients and global clients.</p>
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Excessive Time on IP Addressing	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Authentication and Key Exchange took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds).

Issue	Description
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Excessive Time on Onboarding	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Association took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Authentication and Key Exchange took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). IP Addressing took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). <p>Note This issue is applicable for both single clients and global clients.</p>
Wireless Clients Taking a Long Time to Connect to SSID—Excessive Time on Authentication and Key Exchange Time from the Network/Server Side	<p><i>Value</i> clients taking longer than expected time to connect to <i>SSID</i> in <i>Location</i>. The server is taking longer than usual time to respond:</p> <ul style="list-style-type: none"> These clients took <i>Value</i>% longer than association time baseline of <i>Value Time-Unit</i>. These clients took <i>Value</i>% longer than authentication and 4-way handshake time baseline of <i>Value Time-Unit</i>.
Clients Experiencing Excessive Onboarding Time—Excessive IP Addressing on DHCP Server	<p><i>Value</i> clients are taking longer than expected time to connect through DHCP Server <i>Server IP</i>:</p> <ul style="list-style-type: none"> Onboarding took an average of <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). IP Addressing took an average of <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds).
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Excessive Time on Authentication and Key Exchange Because of WLC Issues	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Authentication and Key Exchange took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). The WLC was identified as the slow component in the process. <p>Note This issue is applicable for both single clients and global clients.</p>

Issue	Description
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Excessive Time on Authentication and Key Exchange Because of Issues from the Client Side	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Authentication and Key Exchange took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). The client was slow to respond to network messages. <p>Note This issue is applicable for both single clients and global clients.</p>
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Excessive Time on Authentication and Key Exchange Because of Slow Network	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Authentication and Key Exchange took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). The network was slow to carry the authentication messages. <p>Note This issue is applicable for both single clients and global clients.</p>
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Excessive Time on Authentication and Key Exchange Because of Server Issues	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Authentication and Key Exchange took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). The network was slow to carry the authentication messages. <p>Note This issue is applicable for both single clients and global clients.</p>
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Excessive IP Addressing Time Because of DHCP Failures	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). IP addressing took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). <p>Note This issue is applicable for both single clients and global clients.</p>

Issue	Description
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz) - Excessive Association Time	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Association took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). <p>Note This issue is applicable for both single clients and global clients.</p>
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz 5 GHz)—Association Failures	<p>This client is taking longer than expected time to connect to <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz):</p> <ul style="list-style-type: none"> Onboarding took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). Association took <i>Value</i> seconds (expected time should be less than <i>Value</i> seconds). <p>Note This issue is applicable for both single clients and global clients.</p>
Client Device Authentication Failed—Dot1.x Failure	The client device <i>Device Name</i> could not be authenticated because <i>Failure Reason</i> .
Client Device Authentication Failed—MAB Failure	The client device <i>Device Name</i> could not be authenticated because <i>failure reason</i> .
Client Failed to Obtain a Response from DNS Server	The client <i>MAC Address</i> failed to obtain a response from the DNS Server <i>DNS Server IP</i> because the server might be unreachable or is no longer responding to queries.

Client Exclusion Issues

The following table provides a list of client exclusion issues that are detected by DNA Center Assurance:

Issue	Description
Client Excluded by WLC—Too Many Web Authentication Failures	This client has been excluded by <i>WLC Name</i> due to <i>Value</i> or more failed AAA authentication attempts within <i>Value</i> seconds. This client is probably failing authentication because of invalid username or password.
Wireless Client Unable to Roam to AP—Too Many Web Authentication Failures	This client is unable to roam <i>AP Name</i> (2.4 GHz 5 GHz) on <i>SSID</i> . This client has been excluded by <i>WLC Name</i> on Web authentication server (LWA/redirect Value/CWA Value) due to <i>Value</i> or more failed Web authentication attempts within <i>Value</i> seconds.
Wireless Client Unable to Roam to AP—IDS Shunned List	This client is unable to roam to <i>AP Name</i> (2.4 GHz 5 GHz) on <i>SSID</i> . This client was identified by Intrusion Detection System (IDS) as a threat and was shunned.

Issue	Description
<i>Value</i> Wireless Clients Failed to Roam on <i>SSID</i> as Clients were Excluded Before Roaming—Too Many Web Authentication Failures	<i>Value</i> clients connected to <i>SSID</i> in <i>Location</i> have been excluded due to <i>Value</i> or more failed Web authentication attempts on Web authentication server (LWA/redirect Value/CWA Value) within <i>Value</i> seconds. As these clients were excluded, they could not roam.
<i>Value</i> Wireless Clients Failed to Roam on <i>SSID</i> as Clients were Excluded Before Roaming—Too Many Failed Authentication	<i>Value</i> clients connected to <i>SSID</i> in <i>Location</i> have been excluded due to <i>Value</i> or more failed AAA authentication attempts within <i>Value</i> seconds. As these clients were excluded, they could not roam.
<i>Client Excluded on SSID on AP (2.4 GHz 5GHz)—Too Many Authentication Failures</i>	This client has been excluded by <i>WLC Name</i> due to <i>Value</i> or more failed AAA authentication attempts within <i>Value</i> seconds. This client is probably failing authentication because of invalid username or password.
<i>Value</i> Clients Excluded by WLC—Authentication Failures	<i>Value</i> clients have been excluded by <i>WLC Name</i> due to <i>Value</i> or more failed AAA authentication attempts within <i>Value</i> seconds. These clients are probably failing authentication on AAA server <i>Server IP</i> because of invalid usernames or passwords.
<i>Client Excluded on SSID on AP (2.4 GHz 5 GHz)—Too Many Web Authentication Failures</i>	This client has been excluded by <i>WLC Name</i> on Web authentication server (LWA/redirect Value/CWA Value) due to <i>Value</i> or more failed Web authentication attempts within <i>Value</i> seconds. This client is probably failing authentication because of an invalid username or password. Note This issue is applicable for both single clients and global clients.
<i>Client Excluded on SSID and WLC—IP Theft Issue</i>	This client was excluded on <i>SSID</i> and <i>WLC Name</i> . The client was rejected for reusing the IP address of another active client. Note This issue is applicable for both single clients and global clients.
<i>Client Excluded on SSID and WLC—IDS Shunned List</i>	This client was excluded on <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz) and <i>WLC Name</i> . This client was identified by Intrusion Detection System (IDS) as a threat and was shunned. Note This issue is applicable for both single clients and global clients.
<i>Client Excluded on SSID and WLC—Too Many Association Failures</i>	This client was excluded on <i>SSID</i> on <i>AP Name</i> (2.4 GHz 5 GHz) and <i>WLC Name</i> because this client failed 802.11 association too many times. Note This issue is applicable for both single clients and global clients.

Mobility Failure Issues

The following table provides a list of mobility failure issues detected by DNA Center Assurance:

Switch and Fabric Issues

Issue	Description
Client Unable to Roam on SSID—AAA Server Rejected Client	This client failed to authenticate and complete the 4-way handshake while roaming from <i>AP Name</i> to <i>AP Name</i> because the AAA server <i>IP Address</i> rejected the client.
Client Unable to Roam on SSID on WLC—Security Parameter Mismatch.	This client failed to authenticate and complete the authentication while roaming from <i>AP Name</i> and <i>WLC Name</i> to <i>AP Name</i> and <i>WLC Name</i> because the security parameters had a mismatch issue.
Client Unable to Roam on SSID Through AP (2.4 GHz 5 GHz) and WLC—Client PMK Not Found	This client failed to connect to <i>SSID</i> through the <i>AP Name</i> (2.4 GHz 5 GHz) and <i>WLC Name</i> because the client Pairwise Master Key (PMK) was not found on the AP and WLC. Client was roaming from <i>WLC Name</i> and <i>AP Name</i> [2.4 5] GHz radio.
Client Unable to Roam on SSID and WLC—WLC Configuration Issue	This client failed to authenticate and complete the authentication while roaming because of issues in the <i>WLC Name</i> configuration. Client was roaming from <i>AP Name</i> on <i>WLC Name</i> .
Client Unable to Roam on SSID to AP (2.4 GHz 5 GHz) and WLC—AAA Server Side Timeout	This client failed to authenticate and complete the 4-way handshake <i>SSID</i> while roaming to <i>AP Name</i> (2.4 GHz 5 GHz) and <i>WLC Name</i> because the WLC did not receive a response from the AAA server <i>IP Address</i> .
Client Unable to Roam on SSID on AP (2.4 GHz 5GHz)—Client Side Timeout	This client failed to connect to <i>SSID</i> while roaming to <i>AP Name</i> (2.4 GHz 5 GHz) due to client timeout during the authentication process.
Client Failed Authentication and Key Exchange—WLC Internal Failure	This client failed to connect to <i>SSID</i> while roaming on <i>WLC Name</i> because of internal failures in the WLC, such as insufficient buffer or insufficient memory.

Switch and Fabric Issues

The following table provides a list of switch and fabric issues detected by DNA Center Assurance:

Issue	Description
Device Experiencing High CPU Utilization	CPU utilization on <i>Device Name</i> has exceeded <i>threshold%</i> in the last 30 minutes.
Device Experiencing High Memory Utilization	Memory utilization on <i>Device Name</i> has exceeded <i>threshold%</i> in the last 30 minutes.
Device Experiencing High Temperature	The temperature on <i>Device Name</i> has exceeded <i>threshold%</i> degree Celsius in the last 30 minutes.
Network Device Unreachable from Controller	This network <i>Network Device Name</i> is unreachable from controller. The device role is <i>Fabric or Device Role</i> .
Fan Failure on Device	The fan(s) in <i>Device Name</i> have failed critically.
Power Supply Failure on Device	The power supply(ies) in <i>Device Name</i> have failed critically.

Issue	Description
Switch Rebooting	This <i>Switch Name</i> is rebooting because of a power outage or system crash.
<i>Interface Name</i> Flapping in the Network	The switch port <i>Interface Name</i> has flapped <i>Value</i> times within the past <i>Value</i> minutes.
Applications Experiencing Slow Response Time—High Input Utilization on Interface	Applications are experiencing slow response time because of <i>Input Utilization%</i> input utilization on <i>Interface Name</i> .
Applications Experiencing Slow Response Time—High Output Utilization on Interface	Applications are experiencing slow response time because of <i>Output Utilization%</i> output utilization on <i>Interface Name</i> .
Applications Experiencing Slow Response Time—Input Errors on Interface	Applications are experiencing slow response time because of <i>Input Errors%</i> input errors on interface <i>Interface Name</i> .
Applications Experiencing Slow Response Time—High Output Utilization on Interface	Applications are experiencing slow response time because of <i>Output Utilization%</i> output utilization on <i>Interface Name</i> .
Applications Experiencing Slow Response Time—Input Errors on Interface	Applications are experiencing slow response time because of <i>Input Errors%</i> input errors on <i>Interface Name</i> .
Status Down on <i>Role</i> Node Fabric-Facing Interface	The status of the <i>Role</i> node fabric-facing <i>Interface Name</i> is down, which is impacting many fabric services from functioning properly.
Reachability Issue Between Fabric Edge and Fabric Border in Overlay <i>vrf</i>	In overlay <i>vrf</i> , the Fabric Edge device <i>Source Device IP</i> failed to reach the Fabric Border device <i>Destination Device IP</i> , which is impacting many fabric services from functioning properly.
Reachability Issue Between Fabric Edge Device and Fabric Border Device in Underlay	There is a connectivity failure between the Fabric Edge device <i>Source Device IP</i> and the Fabric Border device <i>Destination Device IP</i> in underlay, which is impacting many fabric services from functioning properly.
Reachability Issue Between Fabric Edge Device and Fabric Control Plane in Underlay	There is a connectivity failure between the Fabric Edge device <i>Source Device IP</i> and the Fabric Control Plane device <i>Destination Device IP</i> in underlay, which is impacting many fabric services from functioning properly.
Reachability Issue Between Fabric Border Device and Fabric Control Plane in Underlay	There is a connectivity failure between the Fabric Border device <i>Source Device IP</i> and the Fabric Control Plane device <i>Destination Device IP</i> in underlay, which is impacting many fabric services from functioning properly.
Reachability Issue Between Fabric Edge Device and ISE/AAA Server	There is a connectivity failure between the Fabric Edge device <i>Source Device IP</i> and the ISE/AAA server <i>Destination Device IP</i> , which is impacting many fabric services from functioning properly.

Switch and Fabric Issues

Issue	Description
Network Device Lost Connectivity to the DHCP Server in Underlay	The network device <i>Device IP</i> cannot reach the DHCP server <i>DHCP Server IP</i> in underlay.
Network Device Lost Connectivity with External Services	The network device <i>Device IP</i> cannot reach the <i>Destination IP</i> . The device has lost connectivity to external services.
Network Device Lost Connectivity to the DHCP Server in Overlay <i>vrf</i>	The network device <i>Device IP</i> cannot reach the DHCP server <i>DHCP Server IP</i> in overlay <i>vrf</i> .
Border Network Device Lost Connectivity to External URL	The border network device <i>Device IP</i> cannot reach user-provisioned external URL <i>Destination IP</i> .
Reachability Issue Between Network Device and LISP Control Plane "	There is a connectivity failure between the network device <i>Device IP</i> and LISP Control Plane <i>Map Server</i> , which is impacting many fabric services from functioning properly.
Map Cache Entries Exceeded Limit	The SNMP map cache Limit <i>Map Cache Size</i> has exceeded the threshold <i>Map Cache Limit</i> in the last 5 minutes.
High CPU Utilization on Network Device	Network device <i>Device Name</i> is experiencing <i>Value%</i> CPU utilization.
High Memory Utilization on Network Device	Network device <i>Device Name</i> is experiencing <i>Value%</i> memory utilization.
High Temperature on Network Device	Network device <i>Device Name</i> is experiencing <i>Value</i> degree Celsius temperature.
Controller Unable to Reach Network Device	This network device <i>Device Name</i> with <i>Device Role</i> is unreachable from the controller.
Fan Failure on Network Device	The fans in the network device <i>Device Name</i> have failed.
Power Supply Failure on Network Device	The power supplies in the network device <i>Device Name</i> have failed.
Switch Rebooting	This switch <i>Switch Name</i> is rebooting.
<i>Interface Name</i> Flapping in the Network	The switch port <i>Interface Name</i> is flapping.
High Input/Output Utilization on Interface	Interface <i>Interface Name</i> is experiencing high input/output utilization: Rx <i>Rx Input Utilization%</i> Tx <i>Tx Output Utilization%</i>
High Input/Output Errors on Interface	Interface <i>Interface Name</i> is experiencing high input/output errors: Rx <i>Rx Error Percent%</i> Tx <i>Tx Error Percent%</i>
Stackmember Running an Incompatible Image	Stackmember is running an incompatible image.

Issue	Description
Stackmember Removed from Stack	Stackmember has been removed from the stack.
PoE Power Controller: <i>Error Message</i>	PoE power controller error <i>Error Message</i> detected on the switch.
Interface Power Overdrawn	The power on the <i>Interface Name</i> is overdrawn.
Switch Experiencing TCAM Exhaustion	The switch <i>Switch Name</i> has a TCAM area that exceeds a threshold of 95%.

Interface Issues

The following table provides a list of interface issues detected by DNA Center Assurance:

Issue	Description
<i>Interface Name</i> Flapping in the Network	The switch port <i>Interface Name</i> has flapped <i>Value</i> times within the past <i>Value</i> minutes.
Applications Experiencing Slow Response Time—High Input Utilization on Interface	Applications are experiencing slow response time because of <i>Input Utilization%</i> input utilization on <i>Interface Name</i> .
Applications Experiencing Slow Response Time—High Output Utilization on Interface	Applications are experiencing slow response time because of <i>Output Utilization%</i> output utilization on <i>Interface Name</i> .
Applications Experiencing Slow Response Time—Input Errors on Interface	Applications are experiencing slow response time because of <i>Input Errors%</i> input errors on <i>Interface Name</i> .

Fabric Issues

The following table provides a list of fabric issues detected by DNA Center Assurance:

Issue	Description
Status Down on <i>Role</i> Node Fabric-Facing Interface	The status of the <i>Role</i> node fabric-facing <i>Interface Name</i> is down, which is impacting many fabric services from functioning properly.
Reachability Issue Between Fabric Edge Device and Fabric Border Device in Underlay	There is a connectivity failure between the Fabric Edge device <i>Source Device IP</i> and the Fabric Border device <i>Destination Device IP</i> in underlay, which is impacting many fabric services from functioning properly.
Routing Protocol Adjacency Failure from Network Device (OSPF/ISIS)	Routing adjacency between peers fails. The fabric needs underlay configured with ISIS/OSPF routing to communicate between Edge, Border, and Control Plane nodes.
Reachability Issue Between Fabric Border Device and DHCP Server in Overlay <i>vrf</i>	In overlay <i>vrf</i> , the Fabric Border device <i>Source Device IP</i> failed to reach the DHCP Server <i>Destination Device IP</i> , which is impacting many fabric services from functioning properly.

Router Issues

The following table provides a list of router issues detected by DNA Center Assurance:

Issue	Description
Router Received Error Message From Neighbor Interface "Passive 2/2 (Peer in Wrong AS)"	<i>Router IP Address at Router location</i> —Border Gateway Protocol (BGP) peering with neighbor <i>Interface IP address</i> failed due to Autonomous System (AS) Number mismatch. The configured AS number does not match with peer.
BGP is Flapping on Router Interface Because of Missing BGP Hello Keepalives or Peer Terminating Session	<i>Router IP Address at Router location</i> —BGP is flapping on <i>Interface IP Address</i> because of missing BGP hello keepalives or because of a peer terminating the session.
Process 1, Nbr on Went From FULL to DOWN Status, Neighbor Down	OSPF adjacency failed with <i>IP Address at Device Location on Interface Name</i> : dead timer expired.
SIP0/1 Interface State Changed to Down on Router	<i>Router Name at Router location - Interface Name</i> state changed to Down.
High Input/Output Utilization on Router Interface	High Input/Output utilization Rx <i>Value%</i> Tx <i>Value%</i> on <i>Interface Name</i>
Router Experiencing High Memory Utilization	Memory utilization has exceeded <i>Value%</i> over the last <i>Value</i> minutes on <i>Router Name</i> .
Router Experiencing High CPU Utilization	CPU Utilization has exceeded <i>Value%</i> over the last <i>Value</i> minutes on <i>Router Name</i> .
Router Experiencing High Temperature	The temperature of <i>Router Name</i> has exceeded 42 degree Celsius over the last 30 minutes.

AP and WLC Issues

The following table provides a list of AP and WLC issues detected by DNA Center Assurance:

Issue	Description
AP is Currently Down	This <i>AP Name</i> is no longer connected to a WLC. This AP was previously connected to the switch <i>Switch Name</i> and <i>port ID</i> .
AP Flapping Between WLC(s)	The <i>AP Name</i> has disconnected from <i>Old WLC Name</i> and reconnected to <i>Current WLC Name</i> .
AP Experiencing High CPU Utilization	CPU utilization for the <i>AP Name</i> has exceeded the <i>Threshold %</i> threshold. This issue is potentially impacting <i>Value client(s)</i> .
AP Experiencing High Memory Utilization	Memory utilization for the <i>AP Name</i> has exceeded the <i>Threshold %</i> threshold. This issue is potentially impacting <i>Value client(s)</i> .

Issue	Description
AP Rebooted Due to a Hardware or Software Crash	The <i>AP Name</i> has rebooted due to a hardware or software crash.
The 2.4 GHz Radio on AP Experiencing High Utilization	The 2.4 GHz radio on the <i>AP Name</i> has exceeded the <i>Threshold %</i> threshold and is currently experiencing <i>Utilization %</i> utilization. This issue is impacting <i>Value</i> client(s).
The 5 GHz Radio on AP Experiencing High Utilization	The 5 GHz radio on the <i>AP Name</i> has exceeded the <i>Threshold %</i> threshold and is currently experiencing <i>Utilization %</i> utilization. This issue is impacting <i>Value</i> client(s).
AP Experiencing a Coverage Hole	The <i>AP Name</i> is currently experiencing a coverage hole. <i>Value</i> client(s) have had their RSSI threshold lower than -60 dBm over the last 3 minutes. These clients are considered to be in a coverage hole because they are unable to roam to neighboring AP(s) with improved coverage because the AP(s) are not available.
High Memory Utilization on WLC	Memory utilization in the <i>WLC Name</i> has exceeded the <i>Threshold %</i> threshold in the past 15 minutes. This issue is potentially impacting <i>Value</i> client(s).
WLC Rebooted	The <i>WLC Name</i> has rebooted due to a hardware or software crash.
High AP License Utilization on WLC	The <i>WLC Name</i> is licensed to support <i>Max-Count</i> AP(s) and it currently has <i>In Use Count</i> AP(s). If this trend continues, this WLC will exhaust all of its AP license(s).
Power Supply on WLC Failed	The <i>Power Index</i> power supply has failed on the <i>WLC Name</i> . This WLC is now operating with a single power supply.
WLC Not Exporting Data	The <i>WLC Name</i> is not exporting WSA data. It was previously connected to the switch <i>NW Device Name</i> and port <i>Target Interface Name</i> . The switch port is currently <i>Link Status</i> .
WLC Not Exporting AP Data	The <i>WLC Name</i> is not exporting WSA AP data since the last 15 mintutes.
WLC Not Exporting Client Data	The <i>WLC Name</i> is not exporting Client data since the last 15 mintutes.
WLC AP License Exhaustion	The <i>WLC Name</i> is currently licensed to support <i>Max-Count</i> AP(s) and is now operating at its full licensed capacity. No additional AP can join this WLC.
Excessive time lag between Cisco DNA Center and WLC <i>WLC Name</i>	The time on Cisco DNA Center and WLC <i>WLC Name</i> has drifted too far apart. The drift between the two devices is <i>time</i> . Cisco DNA Center cannot process the wireless client data accurately if the time difference is more than 10 minutes.

Sensor Issues

The following table provides a list of sensor issues detected by DNA Center Assurance:

Issue	Description
<i>Value</i> Sensors Failed to Connect to the Wireless Network	<i>Value</i> sensors from <i>Location</i> failed to connect to <i>SSID</i> . They either failed to associate, or authenticate, or get an IP address.
<i>Value</i> Sensors Failed to Get an IPv4 Address from the DHCP Server	<i>Value</i> sensors from <i>Location</i> have failed to get an IPv4 address from DHCP server <i>IP Address</i> in <i>VLAN ID</i> . The DHCP server is reachable.
<i>Value</i> Sensors Slow to Get an IPv4 Address from the DHCP Server	<i>Value</i> sensors from <i>Location</i> are slow to get an IPv4 address from DHCP server <i>IP Address</i> . The sensors are getting an IPv4 address on an average in <i>Value</i> seconds. Clients should be able to get an IPv4 address in 5 seconds. If this problem is not resolved, users will have a poor onboarding experience.
<i>Value</i> Sensors Unable to Reach the the DNS Server	<i>Value</i> sensors from <i>Location</i> are unable to reach the DNS server <i>IP Address</i> . Pings are failing, which will impact user connectivity.
<i>Value</i> Sensors Failed to Resolve Domain Name with the DNS Server	<i>Value</i> sensors from <i>Location</i> are unable to resolve the given <i>Test Domain Name</i> with the DNS server <i>IP Address</i> . This will impact connectivity. The DNS server is reachable.
<i>Value</i> Sensors Experiencing Slow Response from the DNS Server Host	<i>Value</i> sensors from <i>Location</i> are reporting slow response from the DNS server host <i>IP Address</i> . The ping response time to the host is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
<i>Value</i> Sensors Experiencing Slow Name Resolution from the DNS Server	<i>Value</i> sensors from <i>Location</i> are reporting slow name resolution time from the DNS Server <i>IP Address</i> . The name resolution time is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network or server issue that could lead to slow performance.
<i>Value</i> Sensors Not Able to Reach the Test Host	<i>Value</i> sensors from <i>Location</i> are not able to reach test host <i>IP Address</i> . Pings to the hosts are failing.
<i>Value</i> Sensors Experiencing Slow Response from the Host	<i>Value</i> sensors from <i>Location</i> are reporting slow response from the host <i>IP Address</i> . The ping response time to the host is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
<i>Value</i> Sensors Experiencing Slow Response from the Local Gateway	<i>Value</i> sensors from <i>Location</i> are reporting slow response from their local gateway in VLAN <i>x, y</i> . The ping response time to the gateway is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
<i>Value</i> Sensors Not Receiving a Response from their Local Gateway	<i>Value</i> sensors from <i>Location</i> are reporting no ping responses from their local gateway in VLAN <i>x, y</i> . This might indicate a network issue that could lead to network access problems.
<i>Value</i> Sensors Not Able to Reach the RADIUS Server	<i>Value</i> sensors from <i>Location</i> are not able to reach the RADIUS server host <i>IP Address</i> . Pings are failing.

Issue	Description
<i>Value</i> Sensors Experiencing Slow Response from the RADIUS Server	<i>Value</i> sensors from <i>Location</i> are reporting slow response from the RADIUS server host <i>IP Address</i> . The ping response time to the host is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow onboarding.
<i>Value</i> Sensors Experiencing Slow Authentication Time with the RADIUS Server	<i>Value</i> sensors from <i>Location</i> are reporting slow authentication time with RADIUS server <i>IP Address</i> . The sensors are authenticating on an average in <i>Value</i> seconds. Clients should be able to authenticate in 3 seconds. This slow authentication could lead to poor onboarding experience.
<i>Value</i> Sensors Failed to Authenticate with the RADIUS Server	<i>Value</i> sensors from <i>Location</i> are unable to authenticate with the RADIUS server <i>IP Address</i> .
<i>Value</i> Sensors Unable to Reach the Outlook Web Access Host	<i>Value</i> sensors from <i>Location</i> are not able to reach the Outlook Web Access host <i>IP Address</i> . Pings to the Outlook Web Access hosts are failing.
<i>Value</i> Sensors Experiencing Slow Response from the Outlook Web Access Host	<i>Value</i> sensors from <i>Location</i> are reporting slow response from the Outlook Web Access host <i>IP Address</i> . The ping response time to the host is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow Outlook Web Access performance.
<i>Value</i> Sensors Experiencing Slow Response from the Outlook Web Access' First Hop Gateway	<i>Value</i> sensors from <i>Location</i> are reporting slow response from their Outlook Web Access' first hop gateway in VLAN x, y. The ping response time to the gateway is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
<i>Value</i> Sensors Experiencing Slow Mail Connection Time to Outlook Web Access	<i>Value</i> sensors from <i>Location</i> are reporting slow connection time to the Outlook Web Access <i>IP Address</i> . The sensors are connecting to the Outlook Web Access on an average in <i>Value</i> seconds. Clients should be able to connect to the Outlook Web Access in <i>Value</i> seconds. This might lead to poor mail experience.
<i>Value</i> Sensors Failed to Connect to the Outlook Web Access	<i>Value</i> sensors from <i>Location</i> are unable to connect to the Outlook Web Access. Users might not be able to send mail.
<i>Value</i> Sensors Unable to Reach the Web Server	<i>Value</i> sensors from <i>Location</i> are not able to reach the Web server host <i>IP Address</i> . Pings to the web server hosts are failing.
<i>Value</i> Sensors Experiencing Slow Response from the Web Server	<i>Value</i> sensors from <i>Location</i> are reporting slow response from the Web server host <i>IP Address</i> . The ping response time to the host is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow web performance.

Issue	Description
<i>Value</i> Sensors Experiencing Slow Response from the Web Server First Hop Gateway	<i>Value</i> sensors from <i>Location</i> are reporting slow response from their Web server's first hop gateway in VLAN <i>x,y</i> . The ping response time to the gateway is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
<i>Value</i> Sensors Experiencing Slow Web Response Time from the Web Server	<i>Value</i> sensors from <i>Location</i> are reporting slow web page load time from the Web server <i>IP Address</i> . The sensors are connecting and loading the web page on an average in <i>Value</i> seconds. Clients should be able to load the page in <i>Value</i> seconds. This could lead to poor web experience.
<i>Value</i> Sensors Failed to Load Page from the Web Server	<i>Value</i> sensors from <i>Location</i> are unable to load a page with the Web server <i>IP Address</i> .
<i>Value</i> Sensors Unable to Reach the SSH Server	<i>Value</i> sensors from <i>Location</i> are not able to reach the SSH server host <i>IP Address</i> . Pings are failing.
<i>Value</i> Sensors Experiencing Slow Response from the SSH Server	<i>Value</i> sensors from <i>Location</i> are reporting slow response from the SSH server host <i>IP Address</i> . The ping response time to the host is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow SSH performance.
<i>Value</i> Sensors Experiencing Slow SSH Login Time	<i>Value</i> sensors from <i>Location</i> are reporting slow SSH login time to SSH server <i>IP Address</i> . The sensors are connecting on an average in <i>Value</i> seconds. Clients should be able to connect in <i>Value</i> seconds. This could lead to poor SSH experience.
<i>Value</i> Sensors Unable to Connect with the SSH Server	<i>Value</i> sensors from <i>Location</i> are unable to connect with the SSH server <i>IP Address</i> .
<i>Value</i> Sensors Unable to Reach the Mail Server	<i>Value</i> sensors from <i>Location</i> are not able to reach the Mail server host <i>IP Address</i> . Pings are failing.
<i>Value</i> Sensors Experiencing Slow Response from the Mail Server	<i>Value</i> sensors from <i>Location</i> are reporting slow response from the Mail server host <i>IP Address</i> . The ping response time to the host is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow mail performance.
<i>Value</i> Sensors Experiencing Slow Connection Time to the Mail Server	<i>Value</i> sensors from <i>Location</i> are reporting slow connection time to the Mail server <i>IP Address</i> . The sensors are connecting to the Mail server on an average in <i>Value</i> seconds. Clients should be able to connect in <i>Value</i> seconds. This can lead to poor mail experience.
<i>Value</i> Sensors Unable to Connect to the Mail Server	<i>Value</i> sensors from <i>Location</i> are unable to connect to the Mail server <i>IP Address</i> . Users might not be able to use mail services.
<i>Value</i> Sensors Unable to Reach the FTP Server	<i>Value</i> sensors from <i>Location</i> are not able to reach the FTP server host <i>IP Address</i> . Pings are failing.

Issue	Description
Value Sensors Experiencing Slow Response from the FTP Server	<i>Value</i> sensors from <i>Location</i> are reporting slow responses from the FTP server host <i>IP Address</i> . The ping response time to the host is on an average <i>Value</i> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow FTP performance.
Value Sensors Experiencing Slow FTP Transfer Time with the FTP Server	<i>Value</i> sensors from <i>Location</i> are reporting slow FTP transfer time with the FTP server <i>IP Address</i> . The sensors are transferring a file size <i>Value</i> on an average in <i>Value</i> seconds. Clients should be able to do this in <i>Value</i> seconds. This could lead to poor FTP application experience.
Value Sensors Failed to Transfer File with the FTP Server	<i>Value</i> sensors from <i>Location</i> are unable to transfer file with the FTP server <i>IP Address</i> . Users might not be able to use FTP services on this server.
Value Sensors are Unable to Connect to the FTP Server	<i>Value</i> sensors from <i>Location</i> are unable to connect to FTP server <i>IP Address</i> . Users might not be able to use FTP services on this server.



CHAPTER 21

Troubleshoot DNA Center Using Data Platform

- [About Data Platform, on page 321](#)
- [Troubleshoot DNA Center Using the Analytics Ops Center, on page 322](#)
- [View Collector Status, on page 323](#)
- [Configure Data Retention Settings, on page 324](#)
- [View Pipeline Status, on page 324](#)

About Data Platform

Data Platform provides tools that can help you monitor and troubleshoot DNA Center applications. **Data Platform** displays synthesized data from various inputs to help you identify patterns, trends, and problem areas in your network. For example, if something goes wrong in your network, you can quickly get answers to questions such as whether a pipeline is in an error state and what is the real-time traffic flow in a particular area. The main areas of Data Platform are:

- **Analytics Ops Center**—The Analytics Ops Center provides a graphical representation of how data is streamed through collectors and pipelines and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network. See [Troubleshoot DNA Center Using the Analytics Ops Center, on page 322](#).
- **Collectors**—Collectors collect a variety of network telemetry and contextual data in real time. As data is ingested, DNA Center correlates and analysis the data. You can view the status of collectors and quickly identify any problem areas. See [View Collector Status, on page 323](#).
- **Store Settings**—Allows you to specify how long data is stored for an application. See [Configure Data Retention Settings, on page 324](#).
- **Pipelines**—Pipelines allow DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas. See [View Pipeline Status, on page 324](#).

Troubleshoot DNA Center Using the Analytics Ops Center

The Analytics Ops Center provides a graphical representation of how data is streamed through collectors and pipelines, and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network, such as:

- Missing data in DNA Center Assurance.
- Inaccurate health score.
- Devices appear as monitored under Inventory but unmonitored under DNA Center Assurance.

Procedure

Step 1 From the DNA Center home page, click  and then choose **System Settings**.

The **System 360** page appears.

Step 2 Click the **Data Platform** tab.

Step 3 Click **Analytics Ops Center**.

A list of applications are displayed. For example, Assurance and Pegasus.

Step 4 Click the application name for which you want to view metrics, for example, **Assurance**.

A graphical representation of all the existing collectors and pipelines in the application appear. CPU or throughput values corresponding to each pipeline are also provided.

The current health status of each component is indicated by its color:

- Red—indicates an error.
- Yellow—indicates a warning.
- Grey—indicates normal operation.

Step 5 To view historical data of pipelines, click **Timeline & Events**.

A timeline bar providing data for the time interval appears. You can also:

- Move the timeline slider to view data for a specific time.
- Hover your cursor over an event in the timeline bar to display additional details or a group of events that occurred at the same time.
- Click on an event to display the Analytics Ops Center visualization at that particular time.

Step 6 To view additional details to help you troubleshoot an issue and determine the cause of an error or warning, click a *Collector Name*.

A side bar appears with the following tabs:

- **Metrics**—Provides a selection of available metrics gathered during the last 30 minutes. It displays summary information indicating the component status, start and stop time, and exceptions if errors have occurred. You can also select a different time interval.

- **Grafana**—Displays a dashboard associated with the respective component for deeper debugging.

Step 7

To view whether data is flowing through a specific pipeline, click on a pipeline stream.

A sidebar appears with graphs. The graphs display whether the application is receiving data from the underlying pipelines. The graph information is based on the time interval you select from the drop-down list in the sidebar. Options are **Last 30 Min, Last Hour, Last 2 hours, and Last 6 Hours**. Default is Last 30 Min.

Step 8

If a pipeline is not flowing at normal levels, hover your cursor over the stream to display the lag metrics.

Step 9

To view detail information for a specific pipeline, click a *Pipeline Name*.

The appropriate *Pipeline* page displays with the following tabs:

Note Make sure to click the **Exceptions** tab to determine if any exceptions have occurred in the pipeline. Under normal working conditions, this tab displays **null**.

- **Metrics**—Displays metrics, updated every 30 minutes in a graph.
- **Summary**—Displays summary information such as stats, run-time, and manifest.
- **Exceptions**—Displays any exceptions that have occurred on the pipeline.
- **Stages**—Displays the pipeline stages.

Step 10

To change the metrics you want displayed in the Analytics Ops Center page, click **Key Metrics**, select up to two metrics, and then click **Apply**.

By default, DNA Center displays CPU and Throughput metrics.

Step 11

To view metrics for a particular flow, do the following:

- a) Click **View Flow Details**.
- b) Select three connected components (collector, pipeline, and store) by clicking the tilde (~) located on the component's top left corner.
- c) Click **View Flow**.

DNA Center displays the metrics associated with that specific flow.

View Collector Status

Collectors collect a variety of network telemetry and contextual data in real time. As data is ingested, DNA Center correlates and analyzes the data. You can view the status of collectors and quickly identify any problem areas.

Procedure

- Step 1** From the DNA Center home page, click  and then choose **System Settings > Data Platform**.
- Step 2** Click **Collectors**. The colored dot next to each collector indicates its overall status.
- Step 3** To view additional details, click on a collector name.

Configure Data Retention Settings

By default, DNA Center displays the Current Configurations list.

- Step 4** To view, update, or delete a configuration, click on a specific configuration name.
 - Step 5** To add a new configuration, click **Add**, enter the required information, then click **Save Configuration**.
 - Step 6** To view configured instances, click the **Instances** tab.
 - Step 7** To view summary information and metrics, select an Instance from the list.
-

Configure Data Retention Settings

You can specify how long data is stored for an application.

Procedure

- Step 1** From the DNA Center home page, click  and then choose **System Settings > Data Platform**, then click **Store Settings**.
 - Step 2** To view a list of historical purge jobs that have completed, click **Data Purge Schedule**.
The History table lists the name of the purge job, the result, time, and other data. You can sort, filter, and export data in the table.
 - Step 3** To view or modify the current data retention and purge settings, click **Data Retention & Purge Configuration**.
Click the data for which you want to view or modify data retention and purge configuration settings:
 - Time Series Document Store—Settings for all time-based data.
 - Trigger Store—Storage space dedicated to issues detected by various data analysis algorithms.
 - Time Series Graph Store—Settings for all time-based graphical data.
-

View Pipeline Status

Data pipelines allow DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas.

Procedure

- Step 1** From the DNA Center home page, click  and then choose **System Settings > Data Platform**.
- Step 2** Click **Pipelines**.
- Step 3** To view whether the application is receiving data from the underlying pipelines, click on a pipeline name.
The appropriate *Pipeline* page displays with the following tabs:

Note Make sure to click the **Exceptions** tab to determine if any exceptions have occurred in the pipeline. Under normal working conditions, this tab displays **null**.

- **Metrics**—Displays metrics, updated every 30 minutes in a graph.
 - **Summary**—Displays summary information such as stats, run-time, and manifest.
 - **Exceptions**—Displays any exceptions that have occurred on the pipeline.
 - **Stages**—Displays the pipeline stages.
-

View Pipeline Status