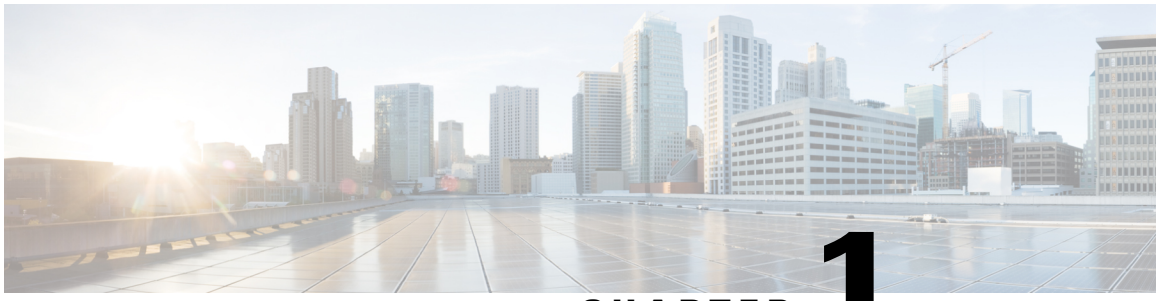
Cisco Digital Network Architecture Center User Guide, Release 1.1

First Published: 2017-11-30

Last Modified: 2018-01-30

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

CONTENTS



CHAPTER 1

Get Started with Cisco DNA Center

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 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 DNA Center Appliance Installation Guide*.

The following are the supported browsers and versions for the DNA Center GUI:

- Google Chrome, version 62.0 or later
- Mozilla Firefox, version 54.0 or later

Note You need to continuously use DNA Center to remain logged in. If you allow too much time of inactivity to elapse, DNA Center automatically logs you out of your session.

Procedure

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

For example, https://192.0.2.1

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

Step 2 Enter the DNA Center GUI username and password, which was configured during the DNA Center installation.

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

Default Home Page

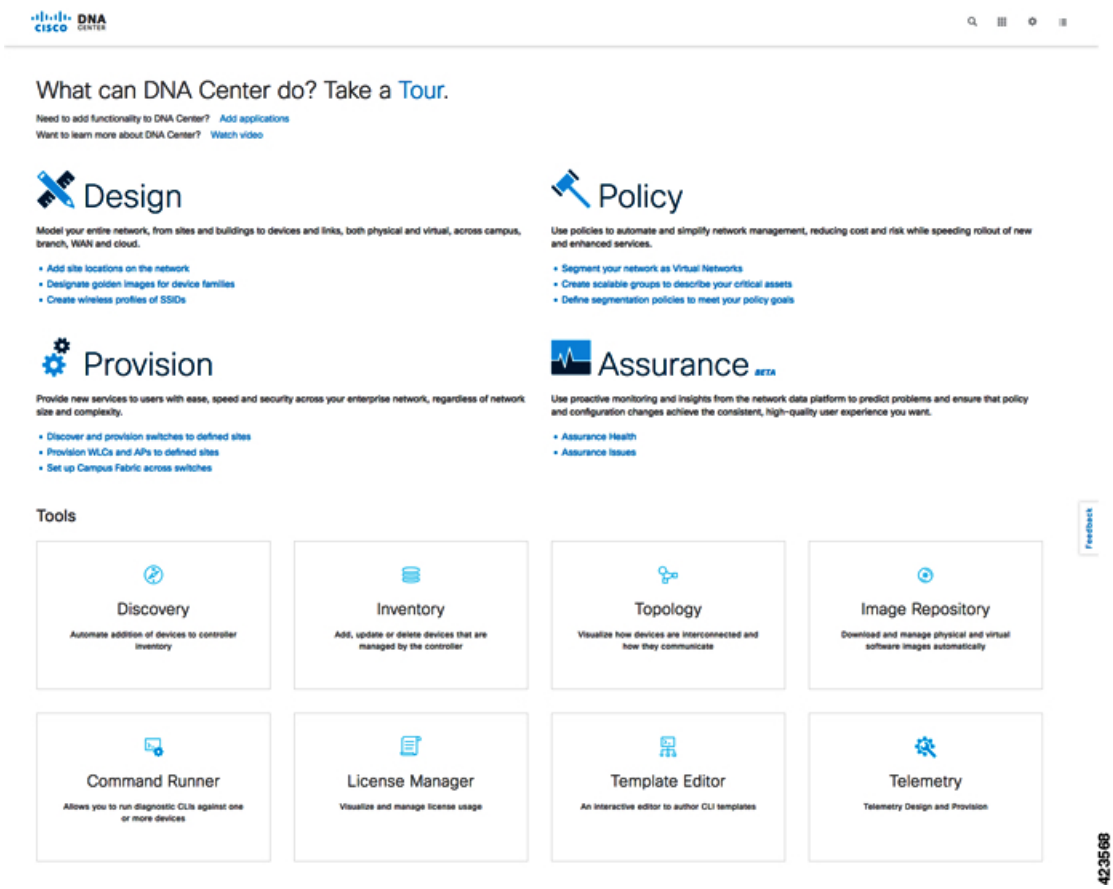
After you log in to DNA Center, you are taken to the DNA Center home page, which is divided into two main areas—**Applications** and **Tools**:

Applications include:

- **Design—**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 to help you configure and manage the network.

Figure 1: DNA Center Home Page



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 Search, on page 4.
- (apps) icon—Lets you return to the home page from any other page in DNA Center (clicking on the "Cisco DNA Center" logo in the upper left corner of the home page does the same thing).
- (settings) icon—Lets you see audit logs, configure system settings, see the DNA Center version you are using, and log out.
- (notifications) icon—Lets you see recently scheduled tasks and other notifications.

If you do not know where to start, see Where to Start, on page 5 for information.

Use Search

Use DNA Center's global Search to search for the following:

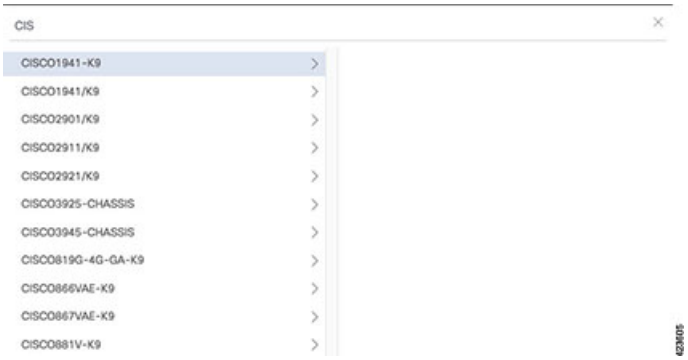
- **Devices**: Search for them by name, IP address, serial number, software version, platform, product family, or MAC address.
- **Hosts**: Search for them by name, IP address, or MAC address.
- **Users**: Search for them by name.
- **IP Pools**: Search for them by name or IP address.
- Other items, 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: Search Icon (at the top right of every page)

DNA Center displays a global search prompt field, where you can begin entering information for the item you are looking for. As you begin entering your search information, DNA Center attempts to autocomplete your entry. It suggests a list of possible search targets matching your input, as shown in the figure below.

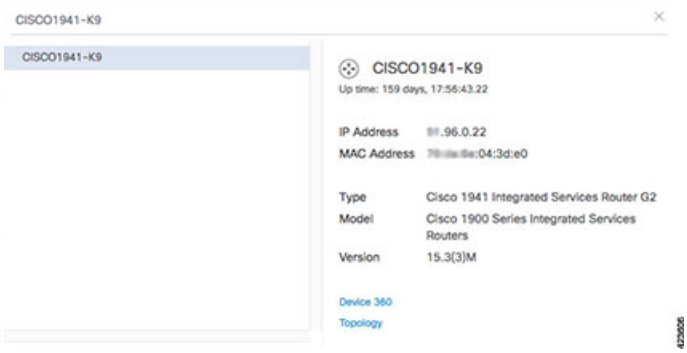
Figure 3: Suggest Search Targets



You can click on any of the suggested targets to see summary information for that item. The summary will include links to additional details appropriate for that item. For example, clicking on the **360 View** and

Topology links in the device detail window shown in the following figure will take you to the pages showing extensive device details and where the device fits in your network topology.

Figure 4: Selected Search Result



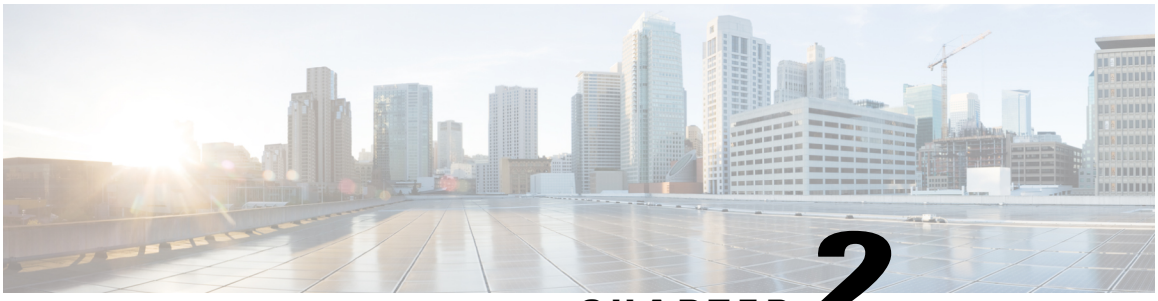
When you are finished, click  to close the search window.

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, also known as a brownfield deployment, start by running a Discovery. After running Discovery, all your devices are displayed on the **Inventory** window. For information, see Discover Your Network, on page 7.
- New or nonexisting infrastructure—If you have no existing infrastructure and are starting from scratch, also known as a green field deployment, you will need to create a network hierarchy. For information about creating a network hierarchy, see Design Network Hierarchy and Settings, on page 59.



CHAPTER 2

Discover Your Network

About Discovery

The Discovery feature scans the devices in your network and sends the list of discovered devices to Device 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 two ways for you to discover devices:

- Using Cisco Discovery Protocol (CDP) and providing a seed IP address.
- Specifying a range of IP addresses (A maximum range of 4096 devices is supported.).

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

- **CDP Level—**If you use CDP as the discovery method, you can set the CDP level. This setting defines the number of hops from the seed device that you want to scan. The default, CDP Level 16, might take a long time on a large network. So, if fewer devices have to be discovered, you can set the CDP 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 or an IP address range, you can specify if 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.

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

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

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 (CLI, SNMPv2c, SNMPv3, and HTTP).

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:

- If you change a device's credential after successfully discovering the device, subsequent polling cycles for that device fail. To correct this situation, use one of the following options:
  - Use the Discovery tool to:
    - Run a new discovery job with job-specific credentials that match the device's new credential.
    - Edit the existing discovery job and re-run the Discovery.
  - Use the Design tool to:
    - Create a new global credential and run a new discovery job using the correct global credential.
    - Edit an existing global credential and re-run the discovery job.
- If an ongoing discovery polling cycle fails due to a device authentication failure, you can correct the situation using one of following options:
  - Use the Discovery tool to:
    - Stop or delete the current discovery job and run a new discovery job with job-specific credentials that match the device's credential.
    - Stop or delete the current discovery job, edit the existing discovery job, and re-run the Discovery.
  - Use the Design tool to:
    - Create a new global credential and run a new discovery job using the correct global credential.
    - Edit an existing global credential and re-run the discovery job.

- Deleting a global credential does not affect previously discovered devices. The status of the previously discovered devices does not indicate an authentication failure. However, the next discovery that tries to use the deleted credential will fail. The discovery will fail **before** it tries to contact any devices. For example, 25 minutes after you delete the credential, discovery jobs that use it will fail.

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 **Device 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.

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.

Perform Discovery

Discover Your Network Using CDP

You can discover devices using Cisco Discovery Protocol (CDP) or an IP address range. This procedure shows you how to discover devices and hosts using CDP. For information about discovering devices using an IP address range, see Discover Your Network Using an IP Address Range, on page 20.

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

a) For **Type**, click **CDP**.
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 **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.
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 CDP neighbor's IP address is reachable from DNA Center.

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

a) Make sure that the global credentials that you want to use are checked. If you do not want to use a credential, remove it by clicking the check mark.
b) To add additional credentials, click **Add Credentials**.
c) 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.
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.

Field	Description
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.

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

Table 2: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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.

Field	Description
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **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: • **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. **Note** • 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: • **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	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. **Note** • 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	You can configure up to five HTTPS read credentials: • **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). **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	You can configure up to five HTTP write credentials: • **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). **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 5 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 checked. If you do not want to use a credential, disable it by clicking the check mark.
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.
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.

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

Table 7: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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: • **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: • **SHA—**Authentication based on HMAC-SHA. • **MD5—**Authentication based on HMAC-MD5.

Field	Description
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. **Note** • 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: • **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	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. **Note** • 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	You can configure up to five HTTPS read credentials: • **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). **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	You can configure up to five HTTP write credentials: • **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). **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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 6 (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 7 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 Cisco Discovery Protocol (CDP) or an IP address range. This procedure shows you how to discover devices and hosts using an IP address range. For information about discovering devices using CDP, see Discover Your Network Using CDP, on page 11.

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

a) For **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.

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 checked. If you do not want to use a credential, disable it by clicking the check mark.

b) To add additional credentials, click **Add Credentials**.

c) To configure CLI credentials, configure the following fields:

Table 11: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.

Field	Description
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.

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

Table 12: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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: • **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: • **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. **Note** • 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: • **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	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. **Note** • 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**.
Read	You can configure up to five HTTPS read credentials: • **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). **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Write	You can configure up to five HTTP write credentials: • **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). **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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:

a) Click the protocols that you want to use. A green check mark indicates that the protocol is selected. Valid protocols are **SSH** (default) and **Telnet**.

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

Step 6 Click **Start**.
The **Discoveries** window displays the results of your scan.

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

Manage Discovery Jobs

Stop and Start a Discovery Job

Procedure

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

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

a) From the **Discoveries** pane, select the corresponding discovery job.

b) Click **Stop**.

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

a) From the **Discoveries** pane, select the corresponding discovery job.

b) Click **Start**.

Clone a Discovery Job

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

Before You Begin

You have run at least one discovery job.

Procedure

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

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

Step 3 Click **Clone**.
DNA Center creates a copy of the discovery job, named Copy of *Discovery_Job*.

Step 4 (Optional) Change the name of the discovery job.

Step 5 Define or update the parameters for the new discovery job.

Delete a Discovery Job

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

Before You Begin

You have run at least one discovery job.

Procedure

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

Step 2 From the **Discoveries** pane, select the discovery job that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK** to confirm.

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:

- **Discovery Details—**Displays the parameters that were used to run the discovery job. Parameters include attributes such as the CDP 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

Manage Your Inventory

About Inventory

The Device Inventory function retrieves and saves the details, such as host IP addresses, MAC addresses, and network attachment points, about the 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*.

Device 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 device 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 Polling Interval, on page 44.) 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.

To access the **Inventory** window, from the DNA Center home page, click the **Inventory** tool. Table 16: Inventory Window Elements, on page 28 describes the main elements in the **Inventory** window.

Table 16: Inventory Window Elements

Window Element	Description
Add Device	Add a device manually to your inventory by providing the device credentials. If authentication of the device fails due to invalid credentials, the **Status** column shows the failure; however the device is still added to inventory. For information, see Add a Device Manually, on page 33.
	Choose one of the following layouts or customize your own layout. For a list of the columns, see Table 17: Inventory Information, on page 29. • **Status—**Layout shows the **Device Name**, **IP Address**, **Reachability Status**, **Up Time**, **Last Updated Time**, **Poller Time**, and **Last Inventory Collection Status**. • **Hardware—**Layout shows the **Device Name**, **IP Address**, **MAC Address**, **IOS/Firmware**, **Platform**, **Serial Number**, **Last Inventory Collection Status**, **Config**, and **Device Family**. • **Tagging—**Layout shows the **Device Name**, **IP Address**, **MAC Address**, **Config**, **Device Role**, **Location**, and **Device Tag**.
Filters	Refine the list of devices that are displayed in the table by device name, IP address, poller time, and last inventory collection status. To remove or change the filters, click **Reset**.

The **Inventory** table displays the following information for each discovered device. All of the columns, except the **Config** column, support sorting. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

Table 17: Inventory Information

Column	Description
Device Name	Name of the device. Click the name to display the **Device Overview** dialog box with the following information: • **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. **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.
IP Address	IP address of the device.

Column	Description
Reachability Status	State of the device. • **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 . 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. • **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. **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.
MAC Address	MAC address of the device.
IOS/Firmware	Cisco IOS software that is currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Up Time	Period of time that the device has been up and running.
Config	Configuration information. Click **View** to display detailed configuration information similar to what is displayed in the output of the **show running-config** command. **Note** This feature is not supported for access points and WLCs. Therefore, configuration data is not returned for these device types.

Column	Description
Device Role	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. **Note** DNA Center updates the device role assignment if it detects a change in a device's placement or role within the network. However, if you manually change the device role, the assignment remains static, and DNA Center will not update the device role if it detects a change. If desired, you can use the drop-down list in this column to change the assigned device role. The following device roles are available: • Unknown • Access • Core • Distribution • Border Router
Location	Denotes a device's geographic location.
Last Updated Time	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.

Column	Description
Last Inventory Collection Status	Status of the last discovery scan for the device: • **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.

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. For information about configuring Cisco ISE setting in DNA Center, see Configure Global Network Servers, on page 102.

  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*.

Add a Device Manually

Procedure

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

Step 2 Click **Add Device**.

Step 3 In the **Add Device** dialog box, enter the device's IP address in the **Device IP** field.

Step 4 In the **Compute Device** field, choose either **TRUE** or **FALSE**, as follows:

- If the device is a Network Functions Virtualization (NFV) or data center device, choose **TRUE** and go to the next step.
- If the device is not an NFV or data center device, choose **FALSE** and go to Step 6.

The default is **FALSE**.

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

Table 18: HTTPS Credentials

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

Table 19: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Write	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 20: 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: • **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: • **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. **Note** • 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	Privacy type. (Enabled if you select **AuthPriv** as a the authentication mode.) Select one of the following privacy types: • **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	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. **Note** • 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 21: SNMP Properties

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

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

Table 22: CLI Credentials

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

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

Step 10 Click **Add**.

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.

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**
- **Poller Time**
- **Last Inventory Collection Status**

Step 3 Enter the appropriate value in the selected filter field, for example, for the **Device Name** filter, enter the name of a device.
DNA Center presents you with auto-complete values as you enter values in the other fields. Choose one of the suggested values or finish entering the desired value.

You can also use a wildcard (asterisk) with these filters, for example, you can enter values with an asterisk at the beginning, end, or in the middle of a string value.

Step 4 Click the plus (+) icon to filter the information.
The data displayed in the **Devices** table is automatically updated according to your filter selection.

Note You can use several filter types and more than one value per filter.

Step 5 (Optional) If needed, add more filters.
To remove a filter, click the **x** icon next to the corresponding filter value.

Change Devices Layout View

Before You Begin

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

Procedure

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

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**.

Add or Remove a Device Tag in Device Inventory

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

Before You Begin

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

Procedure

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

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

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

Step 3 Do one of the following tasks:

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

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

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

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

Step 4 Click  to close the dialog box.

Delete a 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 Click **Delete**.

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 Click **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 23: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 24: 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: • **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: • **SHA—**Authentication based on HMAC-SHA. • **MD5—**Authentication based on HMAC-MD5.

Field	Description
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. **Note** • 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: • **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	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. **Note** • 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 25: SNMP Properties

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

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

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

Table 26: CLI Credentials

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

Step 10 Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field.
NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Step 11 Click **Update**.

Update 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 Click **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**.

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 Click **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**.

Update Device Polling Interval

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

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

Before You Begin

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

Procedure

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

Step 2 Select the devices that you want to update.

Step 3 Click **Update Polling Interval**.

Step 4 From the **Update Resync Interval** dialog box, in the **Status** field, click **Enabled** to turn on polling or click **Disabled** to turn off polling.

Step 5 In the **Polling Time** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24-hours).

Note The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, DNA Center continues to use the device-specific polling time.

Step 6 Click **Update**.

Resynchronize Device Information

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

Procedure

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

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

Step 3 Click **Resync**.

Step 4 Confirm the resynchronization by clicking **OK**.

Use a CSV File to Import and Export Device Configurations

CSV File Import

If you want to use a CSV file to import your device configurations or sites from another source into DNA Center, you can download a sample template by choosing (from the DNA Center home page) **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 manged based on a combination of manually entered credentials and credential profile. For example, if the CSV file contains a credential profile with SNMP and Telnet credentials in addition to manually entered SNMP credentials, then the device is managed based on the manually entered SNMP credentials and the Telnet credentials in the credential profile.

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

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

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

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

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

CSV File Export

DNA Center enables you to create a CSV file that contains all or selected devices in the 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

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

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

Procedure

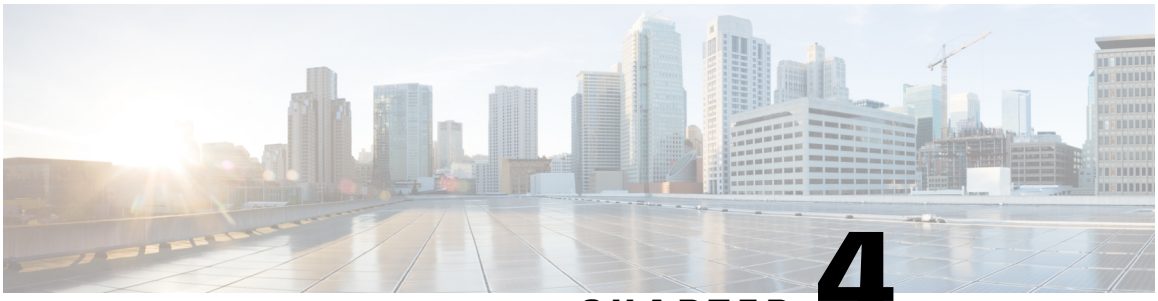
Step 1 From the DNA Center home page, click **Inventory**.

Step 2 Click **Export All** to export all of the devices in the inventory or select the devices that you want to export and click **Export**.

Step 3 In the **Export Device** dialog box, enter a password that will be used to encrypt the exported CSV file. You need to supply this password to open the exported file.

Step 4 Confirm the encryption password and click **Export**.

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



CHAPTER 4

Manage Software Images

About Software Image Management

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

- 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.

Viewing Software Images

After you run Discovery or manually add devices, DNA Center automatically stores all of the software images and SMUs for the devices.

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. By default, the physical software images are displayed.

Step 2 Click **Virtual** to view the virtual software images.

Step 3 In the **Image Name** column, click the downward arrow to view all the software images for the specified device type family. After you select an image type, the **Using Image** field is updated to indicate how many devices are using the image you specified.
The **Using Image** column indicates how many devices are using the specific image you selected in the Image Name field.

Step 4 In the **Version** column, click the **SMU** box to view a list of SMUs versions used.

Step 5 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 51 and Creating Golden Software Images, on page 51.

Using Recommended Software Images

DNA Center can display the Cisco-recommeded 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 51 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 52 for more information.

Import Software Images

You can import a software image 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 stored locally or **Enter image URL** to specify an HTTP or FTP source from which to import the software image.

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.

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 51.

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. After it 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 51 for more information.

Note To provision software images on Cisco WLC and Nexus devices, you must first configure an external SFTP server, which is reachable from DNA Center and the devices. For more information, see the *Cisco Digital Network Architecture Center Administrator Guide*.

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 **Select Devices** drop-down list, choose **Update OS Image**.

Step 4 Click **Update**.

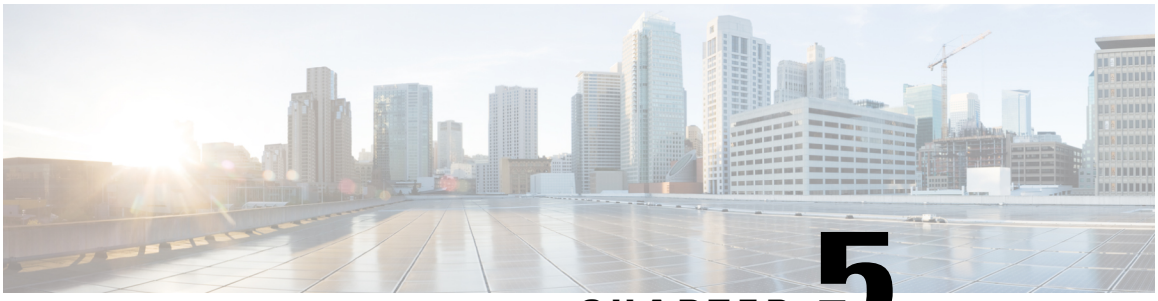
Step 5 Click **OK** to acknowledge that the device will reload after the image is upgraded.

Step 6 (Optional) To view the progress of the image upgrade, you can open a console session to the device.

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 5

Display Your Network Topology

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 a 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 areas, sites, 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 device 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, click 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 Click 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 defult, 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.

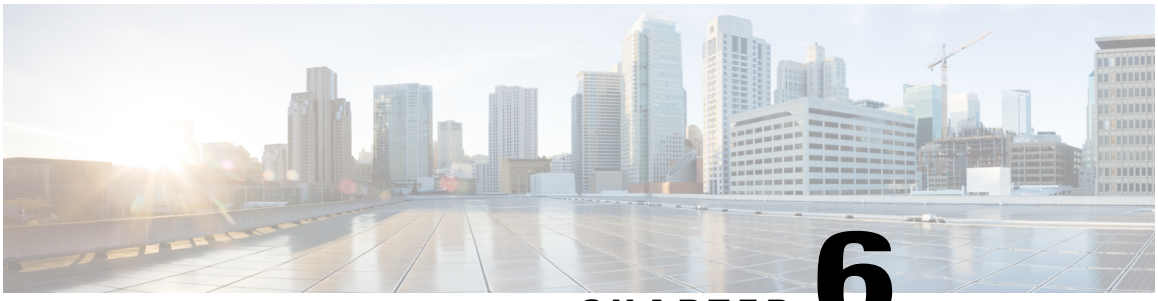
Before You Begin

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  .



CHAPTER 6

Design Network Hierarchy and Settings

Design a New Network Infrastructure

The **Design** area is where you create the structure and framework of your network. This includes 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 61.

Step 2 Define global network settings. See About Global Network Settings, on page 92.

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** don't 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 closed, 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 61.
- Upload an existing network hierarchy from Cisco Prime Infrastructure. See Upload Existing Site Hierarchy, on page 61.

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 **Global** in the left menu and select **Add Site**.

Step 3 You can also upload an existing hierarchy. See Upload Existing Site Hierarchy, on page 61.

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 62 for information about how to export maps from Prime Infrastructure.

Procedure

Step 1 Choose **Design > Network Hierarchy**, then click **Create Site**.

Step 2 At the bottom of the form, click **Upload CSV** to import the Prime Infrastructure Groups CSV file. If you don't have an existing CSV file, click **Download Template** to download a CSV file you can edit and then upload.

Step 3 Navigate to where your CSV file is located, then click **Open**. The site hierarchy is uploaded.

Step 4 To import the Prime Infrastructure maps tar.gz archive file, expand the **Global** site and select **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 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

Step 1 To search the tree hierarchy, place your cursor in the **Search Hierarchy** window and enter the test on which you want to search. The tree is filtered on the information you enter in the search window.

Step 2 To search the map view, place your cursor in the **Search Buildings** window and enter the name of the building for which you want the map view to display.

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 61.

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 27: Map Icons

Icon	Description
Icons	
AP Mode	
L	**Local**
F	**FlexConnect**

Icon	Description
B	**Bridge**
Health Score	
	Good Health
	**Fair Health**
	**Poor Health**
AP Status	
	**Not covered by sensor**
	**Covered by sensor**
	**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	

Icon	Description
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 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**—**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 192. 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 AP1800S Sensor Device, on page 215.

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.
- 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 appears 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:

- Create SSIDs for an Enterprise Wireless Network, on page 82
- Create SSIDs for a Guest Wireless Network, on page 84
- Create a Wireless Interface, on page 88
- Create a Wireless Radio Frequency Profile, on page 88
- Create a Wireless Sensor Device Profile, on page 90

Create SSIDs for an Enterprise Wireless Network

This task shows how to:

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

Procedure

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

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

- 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.
- Check the **Fast Trasition** 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**.
  - **WPA2 Personal—**Provides good security using a passphrase or a preshared key (PSK). Allows anyone with the passkey to access the wireless network. If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.
  - **Open—**Provides no security. Allows any device to access the wireless network without any authentication.
  - Check the **MAC Filtering** check box to enable MAC-based access control on an SSID.

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 specifc 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. See Discover Your Network Using CDP, on page 11 and Discover Your Network Using an IP Address Range, on page 20.
2. Configure policies for your network. See Configure Policies, on page 117.
3. Add Cisco WLC to a site. See Add Devices to Sites, on page 162.
4. Provisioning Cisco WLCs and Cisco APs. See Provision a Cisco WLC, on page 162 and Provision a Cisco AP - Day 1 AP Provisioning, on page 164.
5. Add Cisco WLC to a fabric domain. See Add Devices to a Fabric, on page 168.
6. Configure settings for the various kinds of devices ("hosts") that can access the fabric domain, see Configure Host Onboarding.

Create SSIDs for a Guest Wireless Network

This procedure shows how to:

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

Procedure

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

Step 2 Under **Guest Wireless**, click **+Add** to create new SSIDs.
In the **Create a Guest Wireless Network** window, configure the following parameters:

Step 3 Enter an SSID name in the **Wireless Network Name (SSID)** text box.

Step 4 Under **Level of Security**, select the encryption and authentication type for this guest network. The security options are: **Web AUTH** and **Open**.

- **WEB AUTH—**Provides higher level of layer 3 security.

  Note The WEB AUTH option is disabled if you do not have Cisco ISE configured on the DNA Center server. Cisco ISE acts as a RADIUS server for Web authentication.

- **Open—**Provides no security. Allows devices to connect to the wireless network without any authentication.

Step 5 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 **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 **Non-Fabric** by selecting **Yes** or **No**.
- If you select **No**, check the **Flex Connect** 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.
- 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. See Discover Your Network Using CDP, on page 11 and Discover Your Network Using an IP Address Range, on page 20.
2. Configure policies for your network. See Configure Policies, on page 117.
3. Add Cisco WLC to a site. See Add Devices to Sites, on page 162.
4. Provisioning Cisco WLCs and Cisco APs. See Provision a Cisco WLC, on page 162 and Provision a Cisco AP - Day 1 AP Provisioning, on page 164.
5. Add Cisco WLC to a fabric domain. See Add Devices to a Fabric, on page 168.
6. Configure settings for the various kinds of devices ("hosts") that can access the fabric domain, see Configure Host Onboarding.

Create a Guest Portal Page

You can create the following guest portal pages:

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

Procedure

Step 1 Navigate to the portal page you are creating.

Step 2 Enter the portal name in the **Portal Name** text box.

Step 3 Expand **Page Content** in the left menu to include various variables while creating portal pages.

- List of variables for Login page:
  - Access Code
  - Header Text
  - AUP
  - Text Fields
- List variables for Registration page:
  - First Name
  - Last Name
  - Phone Number

- Company
- Sms Provider
- Person being visited
- Reason for a visit
- Header text
- User Name
- Email Address
- AUP

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

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

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

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

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

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

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

Create a Wireless Interface

Creating wireless interfaces is applicable for nonfabric deployment.

Procedure

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

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

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

Create a Wireless Radio Frequency Profile

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

Procedure

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

Step 2 Under **Wireless Radio Frequency Profile**, click **+Add RF**.
The **Wireless Radio Frequency** window appears.

Step 3 In the **Profile Name** text box, enter the Radio Frequency (RF) profile name.

Step 4 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 the channel assignments:

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

  - **UNNI-1 36-48—**The channels available for UNII-1 band are: **36**, **40**, **44**, and **48**. Check the **UNII-1 36-48** check box to include all channels or check the check box (es) of the channels to select them individually.
  - **UNII-2 52-144—**The channels available for UNII-2 band are: **52**, **56**, **60**, **64**, **100**, **104**, **108**, **112**, **116**, **120**, **124**, **128**, **132**, **136**, **140**, and **144**. Check the **UNII-2 52-144** check box to include all channels or check the check box (es) of the channels to select them individually.

- **UNII-3 149-165—**The channels available for UNII-3 band are: **149**, **153**, **157**, **161**, and **165**. Check the **UNII-3 149-165** check box to include all channels or check the check box (es) of the channels to select them individually.

- 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.
  - **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**.

Create a Wireless Sensor Device Profile

Creating the wireless sensor device profile is applicable for the AP 1800S sensor device.

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 The AP 1800S sensor device with wired connection is supported. To provision the AP 1800S sensor device 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 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 101.
- Select the **Device Family** from the drop down list.
- Enter a unique string in the **Device Tag** to identify the different devices.
- To enable atleast 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 Sevices** window appears. Check the check box next to **WAN Optimizer**or **Firewall** or **+Add Custom** to add a custom service to the profile.

  To configure the router, select **Router Types** and **Profile** from the drop down lists. For more information, see Import Software Images, on page 50. Click **Save**.

  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 61.

What to Do Next

1. Add Cisco WLC to a site. See Add Devices to Sites, on page 162.
2. Provisioning Cisco WLCs and Cisco APs. See Provision a Cisco WLC, on page 162 and Provision a Cisco AP - Day 1 AP Provisioning, on page 164.

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.

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 102.
- Device credentials, such as CLI, SNMP, and HTTP(S)—For more information, see Configure CLI Credentials, on page 95, Configure SNMPv2c Credentials, on page 96, Configure SNMPv3 Credentials, on page 97, and Configure HTTPS Credentials, on page 99.
- IP address pools—For more information, see Configure IP Address Pools, on page 101.
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—For more information, see Configure Global Wireless Settings, on page 82.

Note Certain network settings can be configured on devices automatically using the Device Controllability feature. For more information about Device Controllability, see the *Cisco Digital Network Architecture Center Administrator Guide*.

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 28: SNMPv3 Security Models and Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	User Name	No	Uses a username match for authentication.

Level	Authentication	Encryption	What Happens
AuthNoPriv	Either: • HMAC-MD5 • HMAC-SHA	No	Provides authentication based on the Hashed Message Authentication Code-Secure Hash Algorithm (HMAC-SHA) .
AuthPriv	Either: • HMAC-MD5 • HMAC-SHA	Either: • 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

Configure CLI Credentials

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

Before You Begin

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

Procedure

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

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

Step 3 Enter information in the following fields:

Table 29: 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.

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

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 30: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **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. **Note** 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 SNMPv3 Credentials

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

Before You Begin

- You must have successfully installed DNA Center, and it must be operational. For more information about installing DNA Center, see the *Cisco DNA Center Appliance Installation Guide*.
- 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 31: 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: • **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: • **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. **Note** • 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	Privacy type. (Enabled if you select **AuthPriv** as a the authentication mode.) Select one of the following privacy types: • **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	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. **Note** • 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 32: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to five HTTPS read credentials: • **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). **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	You can configure up to five HTTP write credentials: • **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). **Note** 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 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*.

Procedure

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

Step 2 Click **Add** and complete the required fields.

Step 3 Click **Overlapping** to specify overlapping IP address pool groups to allow different address spaces and concurrently, use the same IP addresses in different address spaces.

Step 4 Click **Save**.

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 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*.

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 (optional) 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 138.

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 DNAC

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

Related Topics

- Prerequisites for Cisco WLC High Availability, on page 104
- Configuring Cisco WLC-HA from Cisco DNA Center, on page 104
- What Happens During or After the High Availability Process is Complete, on page 104
- Commands to Configure and Verify Cisco WLC- High Availability, on page 105

Prerequisites for Cisco WLC High Availability

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

Configuring Cisco WLC-HA from Cisco DNA Center

Procedure

Step 1 Choose **Provision** > **Devices**, and click WLC-1 (configuring this as primary).

Step 2 Click the **High Availability** tab.

Step 3 Select the Select Secondary WLC drop-down list and enter the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses.
Ensure that these IP addresses are the unused IP addresses.

Step 4 Click **Configure HA**.
The HA configuration is initiated at the background using the CLI commands. First, the primary WLC is configured. On success, the secondary WLC is configured. After the configuration is complete, both the WLCs will reboot. This process may take up to 2.5 minutes to complete.

Step 5 After the HA is initiated, the **Redundancy Summary** under **High Availability** tab displays the **Sync Status** as **In Progress**. When DNA Center finds the HA pairing successful, **Sync Status** becomes **Complete**.
This is triggered by the inventory poller or by manual re-sync. By now, the secondary WLC (WLC-2) gets deleted from DNA Center. This flow indicates the successful HA configuration in WLC.

Note There is no real-time data display for Redundancy Summary. During HA pairing, under **Device Inventory**, Cisco WLC shows "Synching" but under **Provision > WLC** shows "Sync Completed".

Note You must perform HA on WLC before adding WLC to connectivity domain. Also ensure that the **Sync status** is **Complete** before adding to connectivity domain.

What Happens During or After the High Availability Process is Complete

1. Cisco WLC-1 and WLC-2 are configured with redundancy management, redundancy units, and SSO. The WLCs reboot in order to negotiate their role as active or stand by. Configuration is synced from active to stand by.
2. On the Show Redundancy Summary page, you can see these configurations:
   - SSO is Enabled
   - WLC1 is Active state

- WLC2 is Hot Stand By state

3 Active WLCs management port will be shared by both the WLCs and will be pointing to active. GUI, Telnet, and SSH on the stand by WLC will not work. You can use the console and service port interface to control the stand by WLC.

Commands to Configure and Verify Cisco WLC- High Availability

The following are the configuration commands sent to primary WLC:

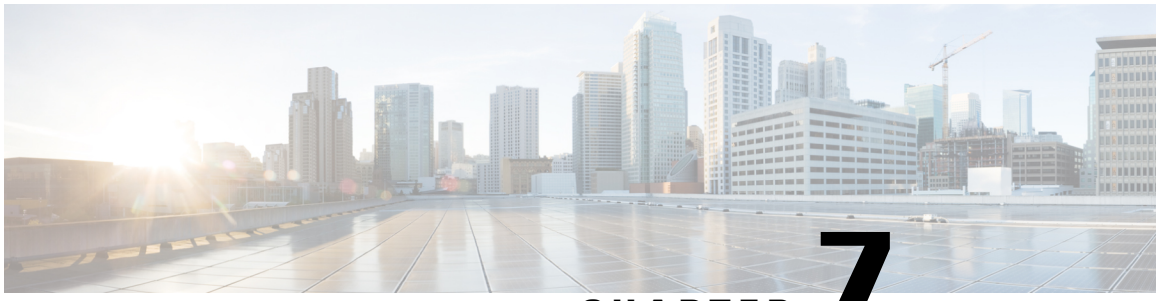
- **config interface address redundancy-management 9.10.45.xx peer-redundancy-management 9.10.45.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

The following are the configuration commands sent to secondary WLC:

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

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

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



CHAPTER 7

About Template Editor

Cisco DNA Center provides an interactive editor to author CLI templates. Template editor is a centralized CLI management tool to help the design and provisioning workflows in the DNA Center. With the template editor you can:

- Create, edit, and delete templates.
- Add interactive commands.
- Validate errors in the template.

Create Projects

Procedure

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

Step 2 To create a project, on the **Template Editor** page, click > **Create Project**.

Step 3 In the **Add New Project** window, enter the following details:

- **Name—**Unique name for the project.
- **Description—**Description for the project.
- **Tags—**Metadata tags, which are used to search projects in the project tree.

Step 4 Click **Save** to save the project.

What to Do Next

1 Create templates. See Create Templates, on page 108.

Create Templates

Procedure

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

Step 2 Select the project in the left menu under which you are creating templates, and click the gear icon > **Add Templates** or click > **Add Templates** located at the top of the tree pane.

Step 3 In the **Add New Template** window, enter the following details:

- **Name—**Unique name for the template within a project.
- **Project Name—**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.
- **Description—**Template description.
- **Tags—**Metadata tags which are used to search projects in the project tree.
- **Device Type—**The drop-down list contains the product family, series, or type. You can select the type of devices to which you want to apply the template.
- **Software Type—**The drop-down list contains the software types. You can select the specific software type such as IOS-XE, ISO-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.
- **Software Version—**Minimum software version to which the template is applicable. During provisioning, the 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.
- Click **Add**. The template is now created and is listed in the left menu.

Step 4 You can edit the template content by selecting the template you created in the left menu.

Step 5 The template editor window opens where you can enter content for the template.

Step 6 You can 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 7 To save the template content, select **Save** from the **Actions** drop-down list. 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, the DNAC checks for any errors in the template. If there are any syntax errors, then the template content is not saved and all the input variables defined in the template is automatically identified during the save process. The local variables (variables used in **for** loops, assigned though a set, and so on) are also ignored.

Step 8 Click the **Form Editor** icon, which is located at the top-right corner of the page to enter additional information to the variables in the template.

Blacklisted Commands

The blacklisted commands are those that are added in the blacklisted category. You can use these commands only through the DNA Center applications. If you use the blacklisted commands in 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
```

Edit Templates

Procedure

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

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

Step 3 The template editor window opens in the right pane.

Step 4 Enter the template content in the template editor, and 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 Select **Save** from the **Actions** drop-down list to save the template content.

Step 6 Click the Form Editor icon, which is located in the top-right corner to enter additional information to the variables in the template.

Template Form Editor

Procedure

Step 1 Select the template in the left menu. The template window opens.

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

- **Required—**Check the 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.
- **Field Name—**Enter the field name. This is the label used for the UI widget of each variable during the provisioning.
- **Tooltip text—**Enter the tooltip text displayed for each variable.
- **Default Value—**Enter the default value. This value appears during provisioning as the default value.
- **Instructional Text—**Enter the instructional text. 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.
- **Data Type—**Select the data type: **String**, **Integer**, **IP Address**, or **Mac Address**.
- **Display Type—**From the drop-down list, select the type of UI widget you want to create at the time of provisioning: **Text Field**, **Single Select**, or **Multi Select**.
- **Maximum Characters—**Enter the number of characters allowed. This is applicable only for string data type.

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

Step 4 After saving the template, you need to 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, select **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

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 Assign Templates to 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 Templates, on page 108.
  - Click **Save**.

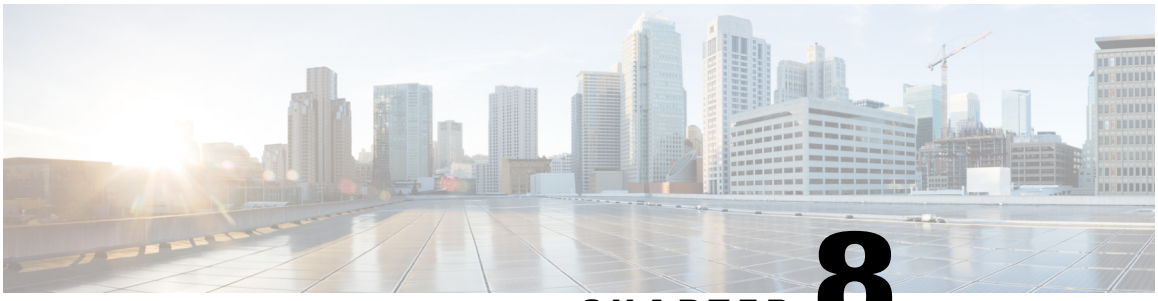
- **Wireless—**Select this to create a wireless profile. Before assigning wireless network profile to a template, ensure that you have created wireless SSIDs. See Configure Global Wireless Settings, on page 82for more information.
  - Enter the **Profile Name**.
  - Click **+ Add SSID**. Those SSIDs 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 **Find Site** field, enter the name of the site to which you want to associate the controller.
- 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**.
- Check the check box of the device and enter the details for the template.
- Click **Next** to deploy.



CHAPTER 8

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, page 115

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 allowed for wireless access points. If in a selected list an access point device is chosen, a warning message is displayed which states that no commands will be executed on the access points.

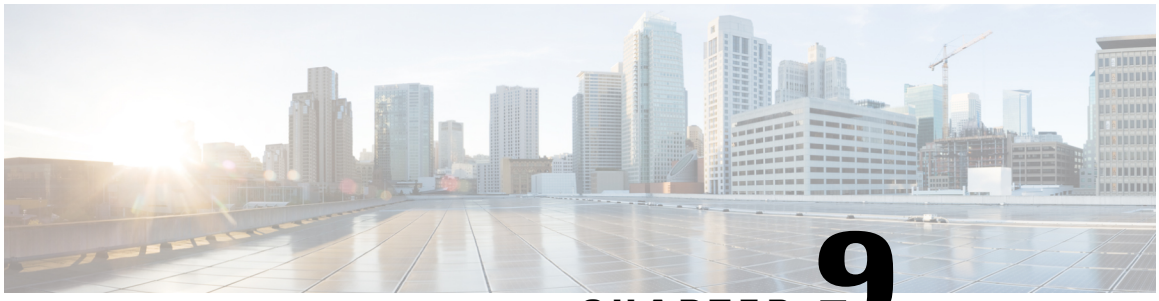
Step 4 In the **Add a Command** field, enter a CLI command and click **Add**.

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 9

Configure Policies

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, 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.

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:

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

Step 3 Click **Save**.

Edit or Delete a Virtual Network

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

Procedure

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

Step 2 Do one of the following tasks:

- Select the virtual network that you want to edit, make the changes, and click **Save**. For field definitions, see Create a Virtual Network, on page 119.
- Delete the virtual network by clicking  and confirming the deletion.

Group-Based Access Control Policies

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

During the initial DNA Center and Cisco ISE integration, scalable groups and policies that are present in Cisco ISE are propagated to DNA Center and placed in the default virtual network. For more information, see the *Cisco DNA Center Appliance 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 > Registry > 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 DNA Center Appliance 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.

Procedure

	Command or Action	Purpose
Step 1	Create virtual networks. Depending on your organization's configuration and its access requirements and restrictions, you can segregate your groups into different virtual networks to provide further segmentation.	(Optional) For more information, see Create a Virtual Network, on page 119.
Step 2	Create scalable groups. After you integrate with Cisco ISE, the scalable groups that exist in ISE are propagated to DNA Center. If a scalable group that you need does not exist, you can create it.	(Optional) For more information, see Create a Scalable Group, on page 121.
Step 3	Create an access control contract. A contract defines a set of rules that dictate the action (allow or deny) that network devices perform based on traffic matching particular protocols or ports.	For more information, see Create an Access Control Contract, on page 122.
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 123

Create a Scalable Group

You can access Cisco ISE through the DNA Center interface to create scalable groups. After you have added the group in Cisco ISE, it is synchronized with the DNA Center database so that you can use it in an access policy. You cannot edit scalable groups in DNA Center; you need to edit them in Cisco ISE.

Procedure

Step 1 From the DNA Center home page, choose **Policy > Registry > Scalable Groups**.
All of the scalable groups that have been created in Cisco ISE appear in the registry.

Step 2 Click **Add**.
DNA Center opens a direct connection to the Cisco ISE server, where you can add the scalable group.

Step 3 In Cisco ISE, create scalable groups (called security groups in Cisco ISE).
For more information, see the *Cisco Identity Services Engine Administrator Guide* .

Step 4 Return to DNA Center.

Create an Access Control Contract

Procedure

Step 1 From the DNA Center home page, choose **Policy > Contracts > Access Contracts**.

Step 2 Click **Add Contract**.

Step 3 In the **Contract Editor** dialog box, enter a name and description for the contract.

Step 4 From the **Implicit Action** drop-down list, choose either **Deny** or **Permit**.

Step 5 From the drop-down list in the **Action** column, choose either **Deny** or **Permit**.

Step 6 From the drop-down list in the **Port/Protocol** column, choose a port or protocol.

Note If DNA Center does not have the port or protocol that you need, you can create your own by clicking **Add Port/Protocol**, configuring the fields, and clicking **Save**.

Step 7 (Optional) To include more rules in your contract, click **Add** and repeat Step 5 and Step 6.

Step 8 Click **Save**.

Edit or Delete an Access Control Contract

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

Procedure

Step 1 From the DNA Center home page, choose **Policy > Contracts > Access Contracts**.

Step 2 Check the check box next to the contract that you want to edit or delete and do one of the following tasks:

- To make changes to the contract, click **Edit**, make the changes, and, click **Save**. .

  Note If you made changes to a contract that is used in a policy, you need to deploy the modifed policy by choosing **Policy Administration > Group-Based Access Control Policies**, checking the check box next to the policy name, and clicking **Deploy**.

- To delete the contract, click **Delete**.

Create a Group-Based Access Control Policy

Procedure

Step 1 From the DNA Center home page, choose **Policy > Policy Administration > Group-Based Access Control Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter the following information:

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

Step 4 To define the source scalable groups, drag and drop the scalable groups from the **Available Security Groups** area to the **Source Scalable Groups** area.

Step 5 To define the destination scalable groups, drag and drop scalable groups from the **Available Security Groups** area to the **Destination Scalable Groups** area.

Step 6 Click **Save**.

Edit or Delete a Group-Based Access Control Policy

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

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

Procedure

Step 1 From the DNA Center home page, choose **Policy > Policy Administration > Group-Based Access Control Policies**.

Step 2 Check the check box next to the policy that you want to edit or delete.

Step 3 Do one of the following tasks:

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

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

- Make sure that you have integrated Cisco ISE with DNA Center if you are creating groups from the **Policy** > **Registry** > **IP Network Groups** page. However, Cisco ISE is not mandatory if you are adding groups within the **Policy** > **Policy AdministrationIP-Based Access Control Policies** page while creating a new IP-based access control policy.

Note Editing an IP network group on the **Policy** > **Registry** page is possible without Cisco ISE. But creation of IP network groups from the **Registry** 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 102.)
  - Device credentials such as CLI, SNMP, HTTP, and HTTPS credentials—(See Configure CLI Credentials, on page 95, Configure SNMPv2c Credentials, on page 96, Configure SNMPv3 Credentials, on page 97, and Configure HTTPS Credentials, on page 99.)
  - IP address pools—(See Configure IP Address Pools, on page 101.)
  - Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—(See Configure Global Wireless Settings, on page 82.)
  - Provision devices—(See Provisioning, on page 161.)

Procedure

	Command or Action	Purpose
Step 1	Create IP network groups.	For more information, see Create an IP Network Group, on page 125.
Step 2	Create an access control contract. An 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.	An access control contract is a common building block that both IP-based and group-based access policies use. For more information, see Create an Access Control Contract, on page 122.
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 126.

Create an IP Network Group

You can create an IP network group from the **Policy** > **Registry** > **IP Network Groups** page or **Policy** > **Policy Administration** > **IP-Based Access control** page.
To create an IP network group from the **Policy Administration** > **IP-Based Access Control**page, follow these steps.

Procedure

Step 1 From the DNA Center home page, choose **Polocy** > **Policy Administration** > **IP-Based Access Control**.

Step 2 Click **Add**.

Step 3 In the **New IP Based Policy** page, click **+Create IP Network Group**.

Step 4 In the **Add IP Network Group** dialog box, enter a name and description for the group.

Step 5 In the **IP Address or IP/CIDR** field, enter an IP address or an IP address with Classless InterDomain Routing (CIDR) notation. (CIDR allows the assignment of Class C IP addresses in multiple contiguous blocks. It also allows you to add a large number of clients that exist in a subnet range by configuring a single client object.)

Step 6 Click **Save**.

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 > Policy Administration > IP-Based Access Control Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter the following information:

- **Policy Name—**Name of the policy.
- **Description—**Word or phrase that identifies the policy.
- **SSID—**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. Otheriwse, it will be configured in a regular way.

  Note If an SSID is part of one policy, that SSID will not be available for another policy.

  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.

- **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 Do one of the following:

- To add another rule, click the plus sign.
- To delete a rule, click +.

Step 5 To reorder the sequence of the rules, drag and drop a rule in the order you want.

Step 6 Click **Deploy**.
A success message saying "IP-Based Access Control Policy has been created and deployed successfully". Depending on the SSID selected, either FlexConnect policy or a normal policy is be created with different level of mapping information and is 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.

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 devices 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 Configure Ports Within the Fabric Domain, on page 172.
- 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 125.

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 130.
Step 2	Create a traffic copy contract. The contract defines the copy destination.	For information, see Create a Traffic Copy Contract, on page 131.
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 131.

Create an IP Network Group

You can create an IP network group from the **Policy** > **Registry** > **IP Network Groups** page or **Policy** > **Policy Administration** > **IP-Based Access control** page.
To create an IP network group from the **Policy Administration** > **IP-Based Access Control**page, follow these steps.

Procedure

Step 1 From the DNA Center home page, choose **Polocy** > **Policy Administration** > **IP-Based Access Control**.

Step 2 Click **Add**.

Step 3 In the **New IP Based Policy** page, click **+Create IP Network Group**.

Step 4 In the **Add IP Network Group** dialog box, enter a name and description for the group.

Step 5 In the **IP Address or IP/CIDR** field, enter an IP address or an IP address with Classless InterDomain Routing (CIDR) notation. (CIDR allows the assignment of Class C IP addresses in multiple contiguous blocks. It also allows you to add a large number of clients that exist in a subnet range by configuring a single client object.)

Step 6 Click **Save**.

Edit or Delete an IP Network Group

Procedure

Step 1 From the DNA Center home page, choose **Policy > Registry > IP Network Groups**.

Step 2 In the **IP Network Groups** table, check the check box next to the group that you want to edit or delete.

Step 3 Do one of the following tasks:

- To make changes to the group, click **Edit**. For field definitions, see Create an IP Network Group, on page 125.
- To delete the group, click **Delete** and then click **Yes** to confirm.

Create a Traffic Copy Destination

Procedure

Step 1 From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Destination**.

Step 2 Enter a name and description for the traffic copy destination.

Step 3 Select the device and one or more ports.

Step 4 Click **Save**.

Edit or Delete a Traffic Copy Destination

Procedure

Step 1 From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Destination**.

Step 2 Check the check box next to the destination that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the group, click **Delete**.

Create a Traffic Copy Contract

Procedure

Step 1 From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Contracts**.

Step 2 Click **Add**.

Step 3 In the dialog box, enter a name and description for the contract.

Step 4 From the **Copy Destination** drop-down list, choose a copy destination..

Note You can have only one destination per traffic copy contract.

If no copy destinations are available for you to choose, you can create one. For more information, see Create a Traffic Copy Destination, on page 130

Step 5 Click **Save**.

Edit or Delete a Traffic Copy Contract

Procedure

Step 1 From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Contracts**.

Step 2 Check the check box next to the contract that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**make the necessary changes, and click **Save**.
- To delete the contract, click **Delete**.

Create a Traffic Copy Policy

Procedure

Step 1 From the DNA Center home page, chooo **Policy > Policy Administration > Traffic Copy Policies**.

Step 2 Enter the following information:

- **Policy Name—**Name of the policy.
- **Description—**Word or phrase that identifies the policy.

Step 3 In the **Contract** field, click **Add Contract**

Step 4 Click the radio button next to the contract that you want to use and then click **Save**.

Step 5 Drag and drop groups from the **Available Groups** area to the **Source** area.

Step 6 Drag and drop groups from the **Available Groups** area to the **Destination** area.

Step 7 Click **Save**.

Edit or Delete a Traffic Copy Policy

Procedure

Step 1 From the DNA Center home page, choose **Policy > Policy Administration > Traffic Copy Policies**.

Step 2 Check the check box next to the policy that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the policy, click **Delete**.

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 133.
- **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 133.

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 137. 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 33: Marking, Queuing, and Dropping Treatments

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
Relevant	VoIP [1]	Expedited Forwarding (EF)	Priority Queuing (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.

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
	Transactional Data (Low-Latency Data)	AF21	BW Queue and DSCP WRED	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 deferential service classes, the vast majority of applications continue to default to this best-effort service.
Irrelevant	Scavenger	CS1	Minimum BW Queue (Deferential) 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 the DNA Center NBAR2 application registry. An orange bar is displayed next to custom applications to distinguish them from the standard NBAR2 applications and application sets. You can define URL-based and server IP address-based applications for wired devices. You cannot define custom applications for wireless devices.

When you define an application according to its server IP address, 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 142.

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 34: Default SLA Attributes for SP Profiles with 4-Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Default	0	—	—	31

Table 35: 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 36: 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 37: Default SLA Attributes for SP Profiles with 8-Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Network-Control Management	CS6	—	—	5
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

LAN Queuing Profiles

LAN Queuing profiles allow you to define an interface's bandwidth allocation based on the interface speed and the traffic class.

Important LAN 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 LAN 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) LAN queuing policy.

If you change the LAN 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 LAN queuing policies:

- If you update a LAN 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 38: 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	
3. Favorite application, gss-http	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-http is in the Ops Admin Mgmt traffic class, it is processed first, followed by the corba-iiop application, which is in the Trasactional 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 Preview

You can preview the command line interface (CLI) commands that DNA Center sends to a device when you apply the policy. At any time, for example, after a policy change, you can generate the specific commands for a specified device. After reviewing the commands, you can deploy the policy to all of the devices in the scope, or you can continue to make changes to the policy.

Note You cannot preview policies for wireless devices.

Policy Scheduling

After you create or change a policy, you need to 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 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 up until the time that it is deployed. Once deployment begins, you cannot 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. You can 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 application sets referenced in an application policy.
- Change to interfaces, such as SP Profile assignment, SP Profile modification, WAN sub-line rate, or WAN or LAN marking.
- 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

- Wireless policies do not support policy preview, restore, abort, or Fastlane.
- 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 > Registry > 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-Based Custom Application

If you have applications that are not in the NBAR2 application registry, you can add them as custom applications.

Procedure

Step 1 From the DNA Center home page, click **Policy Registry > Applications**.

Step 2 Click **+ Add Application**.

Step 3 In the dialog box, configure the following fields:

- **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 a server.
- **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 the NBAR2 application registry, you can add them as custom applications.

Procedure

Step 1 From the DNA Center home page, click **Policy > Registry > Applications**.

Step 2 Click **+ Add Application**.

Step 3 In the dialog box, configure the following fields:

- **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, category, and subcategory settings 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.

Procedure

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

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 > Registry > Application Sets**.

Step 2 Use the **Search**, **Show**, or **View By** fields to locate the applications 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 > Registry > 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 > Registry > 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 138.

Procedure

Step 1 From the DNA Center home page, choose **Policy > Registry > 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.
- 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 159.
- 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 38.

Create an Application Policy

You can 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 38.
- Add devices to sites. For more information, see Add Devices to Sites, on page 162.
- 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 137.
- 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 101.
- 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 149.

Procedure

Step 1 From the DNA Center home page, choose **Policy > Policy Administration > 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 specific interfaces from being configured with the policy.

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 **Exclude Interfaces** next to the device you are interested in.

c) From the list of interfaces, click the toggle button in the **Exclude from Policy** column next to the interfaces that you want to exclude.

d) Click **< Back to Devices in *Site-Name*.**

e) Click **< Back to Site Scope**.

Step 7 For WAN devices, you can configure SP Profiles on 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.

c) In the **WAN Interface** column, click the **Select Interface** drop-down field and choose an interface.

d) In the **Service Provider Profile** column, click the **Select Profile** drop-down field and choose an SP profile.

e) (Optional) If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.

f) (Optional) To configure additional WAN interfaces, click + and repeat Step c through Step e.

g) Click **Save**.

h) Click **< Back to Site Scope**.

Step 8 From the **Site Scope** pane, click **OK**.

Step 9 (Optional) If the Cisco Validated Design (CVD) LAN queuing profile does not meet your needs, create a custom LAN queuing profile. For more information, see LAN Queuing Profiles, on page 140.

a) Click **LAN Queuing Profiles**.

b) Click +.

c) 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.

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.

d) (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. For more information, see Marking, Queuing, and Dropping Treatments, on page 135.
To customize DSCP code points required within a service provider cloud, configure a service provider profile.

e) Click **Save**.

Step 10 (Optional) If this policy is for traffic that is destined for a service provider, customize the service provider profile SLA attributes.

Note For more information about service provider profiles, see Service Provider Profiles, on page 138.

a) Click **SP Profile**.
b) Choose a SP profile.
c) Customize the SLA attributes (**DSCP**, **SP Bandwidth %**, and **Queuing 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. For more information, see Business-Relevance Groups, on page 134.

Step 12 (Optional) Customize applications by creating consumers and assigning them to applications or by marking an application as bidirectional.

a) Expand the application group.
b) Click the gear icon next to the application that you are interested in.
c) From the **Traffic Direction** field, select the **Unidirectional** or **Bi-directional** radio button.
d) 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**.
e) 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 Click **Deploy**.
You are prompted to deploy your policy now or to schedule it for a later time.

Step 15 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.

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 > Policy Administration > Application Policies**.

Step 2 Sort the policies by name or filter them by name, status, or description.

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, 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.
- **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 > Policy Administration > 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 150.

Step 6 Click **Deploy**.
You are prompted to deploy your policy now or to schedule it for a later time.

Step 7 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.

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 > Policy Administration**.

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

Note This function is not supported for policies of wireless devices.

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 > Policy Administration > 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 > Policy Administration > 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 150.

Step 6 Click **Deploy**.

Restore Application Policy

Note This function is not supported for policies of wireless devices.

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 132.

Procedure

Step 1 From the DNA Center home page, choose **Policy > Policy Administration > 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 **Restore**.

Step 6 Click **OK** to confirm the change or **Cancel** to abort it.

Step 7 Click **Deploy**.

Preview an Application Policy

Note This function is not supported for policies of wireless devices.

Before you deploy a policy, you can generate the CLI that will be applied to a device and preview the configuration.

DNA Center generates the CLI commands for the policy and compares them with the running configuration on the device. DNA Center removes any CLIs that are already in the running configuration and generates the only the remaining CLI commands required to configure the policy on your device. For example, if the device has already been configured to match the policy, the policy preview has no CLIs in it.

Procedure

Step 1 From the DNA Center home page, click **Policy > Policy Administration > Application Policies**.

Step 2 Create or edit a policy, as described in Create an Application Policy, on page 150 or Edit an Application Policy, on page 154.

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**
DNA Center generates the CLIs for the policy.

Step 5 Click **View** to view the CLIs or copy them to the clipboard.

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.

Before You Begin

Procedure

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

Step 6 Click **Ok** to confirm the rollback procedure.
The rolled back version becomes the newest version.

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 138.

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 > Policy Administration > 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 135.
- **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 150.

Procedure

Step 1 From the DNA Center home page, click **Policy > Policy Administration > 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 Scope**pane, 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 **Service Provider Profile** column, click the **Select Profile** drop-down field and choose an SP profile.

Step 9 If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.

Step 10 To configure additional WAN interfaces, click + and repeat Step c through Step e.

Step 11 Click **Save**.

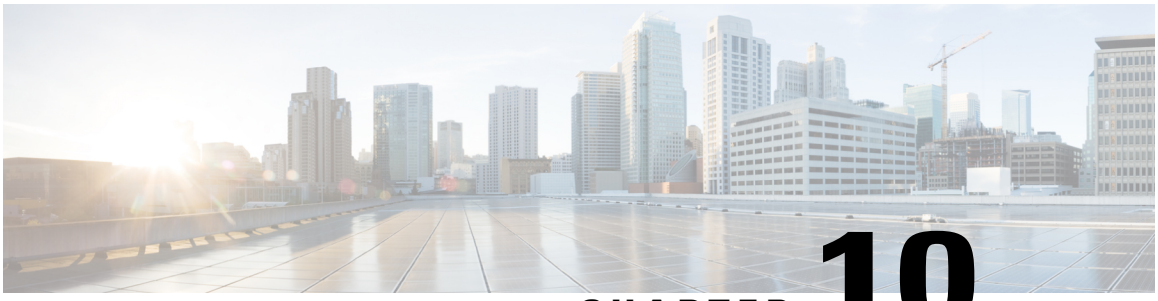
Step 12 Click **< Back to Site Scope**.

Step 13 Click **OK**.

Step 14 Click **Deploy**.
You are prompted to deploy your policy now or to schedule it for a later time.

Step 15 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.



CHAPTER 10

Provision Your Network

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 you have defined the following global network settings before provisioning a Cisco WLC:
  - Network servers, such as AAA, DHCP, and DNS Servers—(See Configure Global Network Servers, on page 102.)
  - Device credentials such as CLI, SNMP, HTTP, and HTTPS credentials—(See Configure CLI Credentials, on page 95, Configure SNMPv2c Credentials, on page 96, Configure SNMPv3 Credentials, on page 97, and Configure HTTPS Credentials, on page 99.)
  - IP address pools—(See Configure IP Address Pools, on page 101.)
  - Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—(See Configure Global Wireless Settings, on page 82.)
- Make sure you have Cisco WLC in your inventory. If not, discover Cisco WLC using the Discovery function. (See Discover Your Network, on page 7.)
- Make sure Cisco WLC is added to a site. (See Add Devices to Sites, on page 162.)

Procedure

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

Step 2 Click the **Device Inventory** tab. All the discovered controllers are displayed.

Step 3 Check the check box(es) adjacent to the controller device name that you want to provision.

Step 4 From the **Action** drop-down list, choose **Provision**.

Step 5 In the **Assign Site** window, assign a site for the controller. In the **Find Site** field, enter the name of the site to which you want to associate the controller. To assign multiple controllers to the same site, check the **All Same Site** check box.

Step 6 Click **Next**.
The **Configuration** window appears.

Step 7 In the **Managed AP Locations** field, enter the AP locations managed by controller. Here you have the option to change, remove, or reassign the site.
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 8 Click + **Add** to configure interface and VLAN. On the Configure Interface and VLAN window, configure the following:

a) Select the interface name from the Interface Name drop-down list.
b) Enter the **INTERFACE IP ADDRESS**.
c) Enter the **INTERFACE NET MAS**.
d) Enter the **GATEWAY IP ADDRESS**.
e) Enter the **LAG/PORT NUMBER**.
f) Click **OK**.

Step 9 Click **Next**.

Step 10 The **Summary** page displays the following information:

- System Details
- Global Setting
- SSID
- Managed Sites
- Interfaces

Step 11 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 168.

2 Configure settings for the various kinds of devices ("hosts") that can access the fabric domain. See Configure Host Onboarding.

Provision a Cisco AP - Day 1 AP Provisioning

Before You Begin

Make sure you have Cisco AP in your inventory. If not, discover APs using the Discovery function. (See Discover Your Network, on page 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(es) adjacent to the AP device name that you want to provision.

Step 4 From the **Action** drop-down list, choose **Provision**.

Step 5 In the **Assign Site** window, assign an AP to the site . In the **Find Site** field, enter the name of the site to which you want to associate the AP. To assign multiple APs to the same site, check the **All Same Site** check box.

Step 6 Click **Next**.
The **Configuration** window appears.

Step 7 From the **RF Profile** drop-down list, choose the RF profile for the AP. The options are: **High**, **Typical**, and **Low**. The AP group is created based on the RF profile selected.

Step 8 Click **Deploy** to provision the AP.
You are prompted with message saying that Creation/modification of AP groups in progress. After completion, these devices will go for a reboot.

Step 9 Click **OK**.
The **Status** column in the **Device Inventory** window shows **SUCCESS** if a deployment is successful.

Provision a Sensor Device

Provisioning a sensor device is applicable for AP 1800S 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 90.
- 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 162.)
- 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 102.)
  - Device credentials such as CLI, SNMP, HTTP, and HTTPS credentials—(See Configure CLI Credentials, on page 95, Configure SNMPv2c Credentials, on page 96, Configure SNMPv3 Credentials, on page 97, and Configure HTTPS Credentials, on page 99.)
  - IP address pools—(See Configure IP Address Pools, on page 101.)
- 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.

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:

- **Pool Name**—Unique name for the reserved IP address pool.
- **Pool Type**—Type of IP address pool. For LAN automation, select **LAN**.
- **Global Pool**—IP address pool from which you want to reserve all or part of the IP addresses.

- **Subnet/Mask—**IP subnet and mask addresses used to reserve all or part of the global IP address pool.

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.

- **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**.

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 controle plane or border devices within the fabric network.

Before You Begin

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

Create a Fabric Domain

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

To add a new fabric domain:

Procedure

Step 1 From the DNA Center **Home** page, click **Provision**.

Step 2 Click the **New Fabric** tab.

Step 3 Enter a name for the fabric.

Step 4 From the **Select Auth** field, select an authentication protocol. This determines the type of access that devices can have when connecting to the network. The protocol selected here is applied to all devices in the fabric.

Step 5 Click **Add**.

Configure a Fabric Domain

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

Add Devices to a Fabric

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

Note It is optional to designate the devices in a fabric domain as control plane nodes or border nodes. You may have devices that do not play these roles. However, every fabric domain must have at least one controle 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**. Befor 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: • 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	Add the selected device as a control plane and a border node. In the pop-up window, enter the following options: • Set as default border—Select the check box if you want the device to act as a default border node. • Routing Protocol—Select the routing protocol for the device. • Routing Process—Select the routing process for the device.

Field	Description
Enable Guests	In the pop-up window that is displayed, enter the following options: • 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**. **Note** Ensure that you have created a guest virtual network in the **Policy** applicatin. See Create a Virtual Network, on page 119.
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**.
- 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 links 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.

Field	Description
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
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:

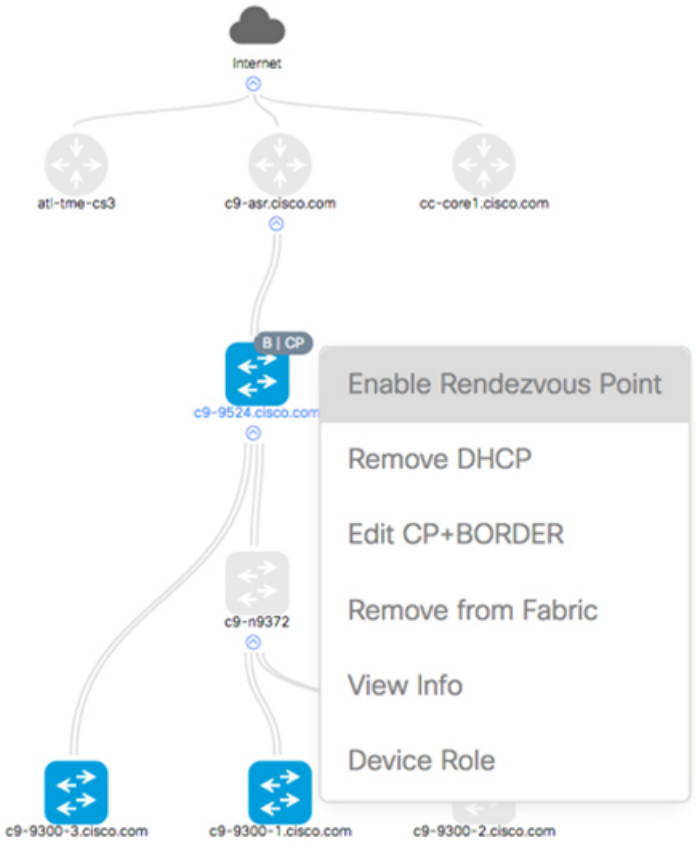
Procedure

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.

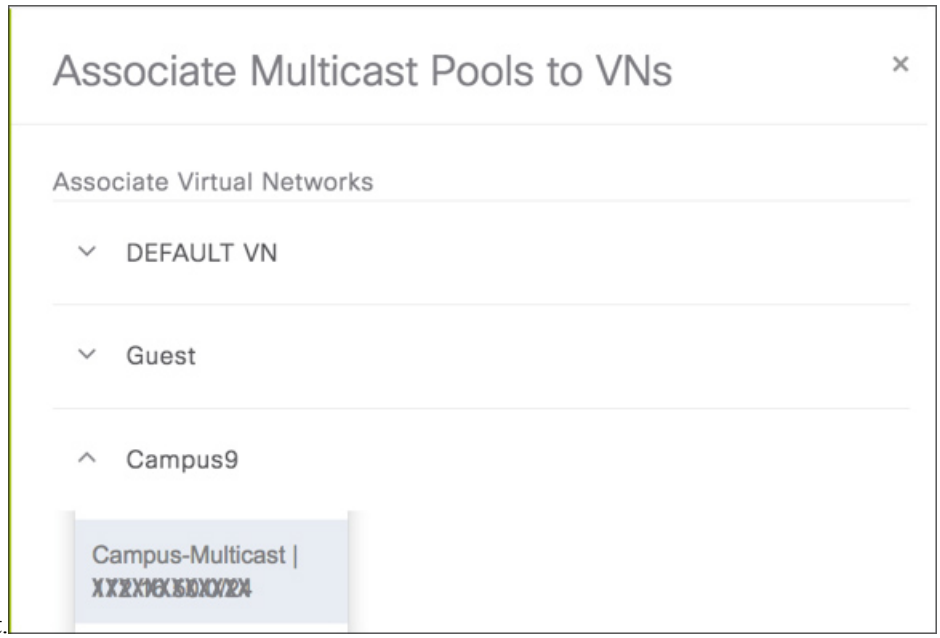
Step 3 From the **Provision - Fabric** page, select a fabric. The screen displays the **Fabric - Devices** page, with all of the devices in the network. Any device that is added to the fabric is highlighted in blue color.

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



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.

Associate Virtual Network and click **Enable**.

Step 7 Click **Save** on the main screen. **Apply** the changes.

Verification

Procedure

	Command or Action	Purpose
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.	

	Command or Action	Purpose
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 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.

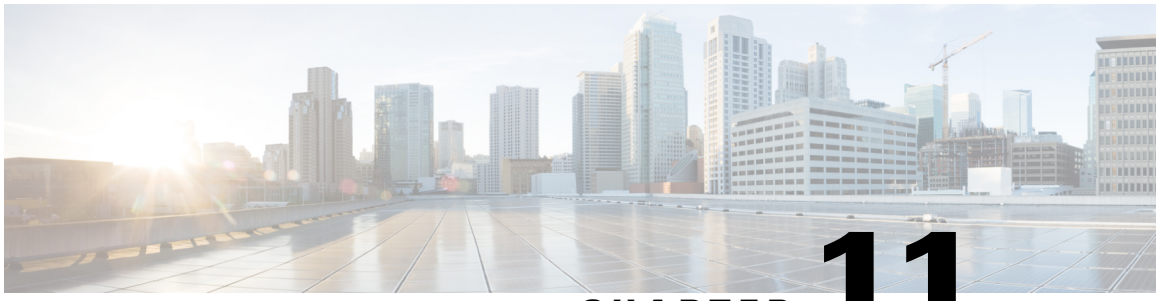
Step 3 From the **Provision - Fabric** page, select a fabric. The screen displays the **Fabric - Devices** page, with all of the devices in the network. Any device that is added to the fabric is highlighted in blue color.

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 11

Assure the Health of Your Network

DNA Center Assurance Overview

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.

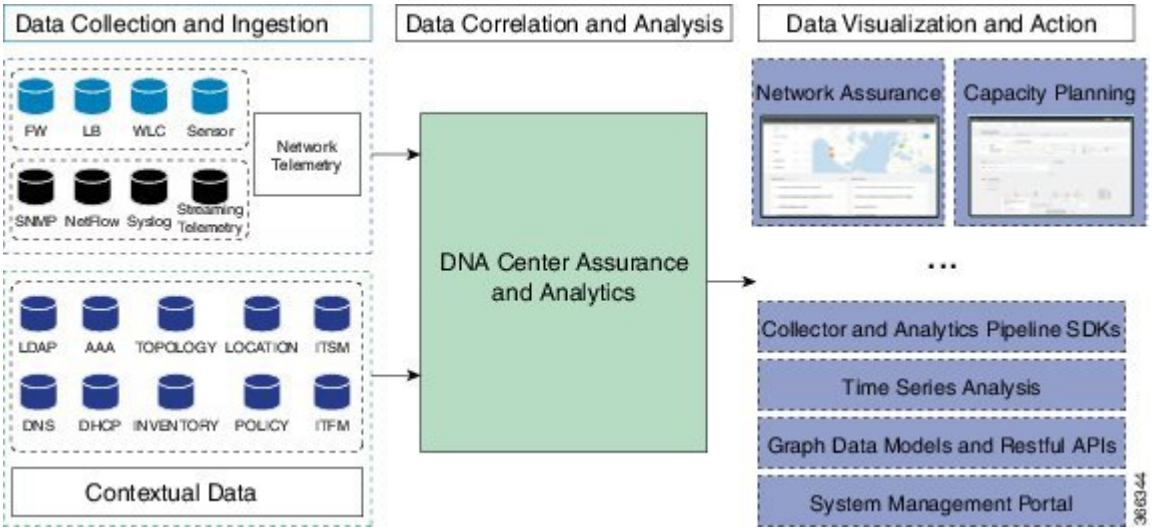
DNA Center Assurance is a multipurpose, real-time, network data collection and analytics engine used to significantly increase the business potential of network data.

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 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 6: 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

Assurance Application

DNA Center Assurance provides actionable insights into network, client, and application related issues. It provides suggestions to troubleshoot and fix issues through enhanced visibility, industry-leading knowledge base, and holistic network data analytics. From the Assurance application, you can do the following:

Table 39: 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 182.
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 186.
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 192.
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 197.
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 204.

Task	Navigation	Reference
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 219.
Manage sensor-driven tests.	**Assurance > Sensor Management**	See About Sensors and Sensor-Driven Tests, on page 211.
Manage and create custom dashboards.	**Assurance > Dashboards > Dashboard Library**	See Manage Dashboards, on page 215.

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

- 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 20 or Discover Your Network Using CDP, on page 11.
- Configure the location of the device, such as area, site, building, and floor. See Create Sites in the Network Hierarchy, on page 61, and Add Floors to Buildings, on page 64.

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.

- Add devices to the sites. See Add Devices to Sites, on page 162.

- 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 69.
- Enable Telemetry collection. Telemetry using SNMP poling is enabled by default. For information about Telemetry, see the *Cisco Digital Network Architecture Center Administrator Guide*.
- 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*.

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—Inactive. Health score is 0.

Table 40: Overall Health Page

Item	Description
Buttons located above the Overall Health Map	• **Hide or Show**—Hides or displays the Overall Health Map dashlet when clicked. By default, the Overall Health Map dashlet is displayed. • **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 click **Edit Dashboards** from the drop-down list. See Edit or Delete a Dashboard, on page 217 and Create a Custom Dashboard, on page 215.

Item	Description
Overall Site Hierarchy table	• **Hide or Show—**Hides or displays the Overall Site Hierarchy table dashlet when clicked. By default, the table is hidden. The table provides a view of % healthy clients and devices broken by type for each site or all sites with a link to the network and client health for each site. • **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 Sites—**Allows you to select a site or building from the drop-down list. Based on what you select, the page refreshes with the relevant information. • **Actions—**Allows you to select a particular site and view the devices, clients, and dashlets related to that site. See Edit or Delete a Dashboard, on page 217 and Create a Custom Dashboard, on page 215.
Overall Health Map dashlet	Geographic location-oriented health map of the enterprise. The health of all the components in the enterprise is represented on a map. By default, the sites that are represented are color coded according to the severity of the problem. Click a site to view details, such as the location of the site and health scores. 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 special score of 0 for Inactive clients. **Note** To hide this dashlet, click the **Hide or Show** toggle button on top of the map.

Item	Description
Overall Health Summary dashlet	Contains the following: • **Network** area—Provides the following: ◦ **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 190. ◦ **Device Category Health Score**—Provides the score distribution between device categories: Access, Distribution, Core, Router, and Wireless. The device category score is the percentage of healthy (good) devices in a particular device category. **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. Click **View Network Health** to open the Network Health page. • **Clients** area—Provides the following: ◦ **Client Score**—Percentage of healthy (good) wired and wireless client devices in your overall enterprise. See, Client Health Summary Score, on page 203. ◦ **Wired and Wireless Score**—Provides the score distribution between wired and wireless clients. Click **View Client Health** to open the Client Health page.
Issues dashlet	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**. For information about the types of issues, see Issues Detected by DNA Center Assurance, on page 219.

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

- 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 20 or Discover Your Network Using CDP, on page 11.

Note When the WLC moves to a managed state on discovery process, DNA enables network assurance functionality on the WLC. Ensure the following to have a successful Assurance enablement.

  - On Cisco WLC 5508, you must use the **config dx enable** command on the WLC followed by manual reboot.
  - Time on DNA and the WLC must synchronize.

- Configure the location of the device, such as area, site, building, and floor. See Create Sites in the Network Hierarchy, on page 61, and Add Floors to Buildings, on page 64.

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.

- Add devices to the sites. See Add Devices to Sites, on page 162.
- 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 69.

- Enable Telemetry collection. Telemetry using SNMP poling is enabled by default. For information about Telemetry, see the *Cisco Digital Network Architecture Center Administrator Guide*.
- 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*.

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—Inactive. Health score is 0.

Table 41: Network Health Page

Item	Description
Buttons located above the Network Health Map	• **Hide or Show**—Hides or displays the Network Health Map dashlet when clicked. By default, the Network Health Map dashlet displays. • **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 domain. Default is all domains. To view information about the Fabric domain, click the drop-down list and choose the appropriate option. • **All Sites**—Allows you to select a site, building, or floor from the drop-down list. Based on what you select, the page refreshes with the relevant information. • **Actions**—Allows you to make changes to the dashboard display when you click **Edit Dashboards** from the drop-down list. See Edit or Delete a Dashboard, on page 217 and Create a Custom Dashboard, on page 215. • **Timeline**—The timeline slider allows you to change the time in the timeline widget.

Item	Description
Network Health Map or **Network Topology** dashlet	Contains two buttons that allow you to display the health of the network in a map view or in a topology view. • **Network Health Map—**The health of all the network sites is represented 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 special score of 0 for Inactive clients. • **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**. **Note** To hide this dashlet, click the **Hide or Show** toggle button on top of the map.
Network Health Summary or **Site Health Summary** dashlet	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 190. This dashlet includes the following charts: • **Last 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.

Item	Description
Network Health By Device Role/Type dashlet	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. **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 191 **Analytic Charts—**Click a device category tab, to display analytic charts (donut chart) for that device type. Click the analytic chart to open a side bar with additional details. The following analytic charts are provided: Depending on the device category you click, the metrics that display in the analytic charts vary. • **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. **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. **Note** For information about how the individual device health score is computed, see Individual Device Health Score, on page 191.

Item	Description
Network Devices Table dashlet	Allows you to filter, view, and export network device information: • Filter the table based on device, type, overall health, or add custom filters: ◦ **Device—**Monitored and Unmonitored. ◦ **Type—**All, Access, Core, Distribution, Router, Wireless, and Other. ◦ **Overall Health—**Poor, Fair, and Good. ◦ **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 over a 5 minute interval.

For example: 90% health score = 90 network devices with health score between 8 to 10 / total 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 over a 5 minute interval.

For example: 90% health score = 90 network devices in a target category with health score between 8 to 10 / total 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 42: Device 360 Page

Item	Description
Device **Health Score**	Health score of a device: • **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 194. • **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 195. • **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 195. • **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 196. 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 special score of 0 for Inactive clients. • 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—Inactive. 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	Health information about the selected network device over a period of time. 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. 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.

Step 4 View information about issues, physical neighbor topology, path trace, application experience, and detail information under the appropriate category.

Table 43: 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**. For information about the types of issues, see Issues Detected by DNA Center Assurance, on page 219.
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 207.
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.

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 MAP Server(s)—Fabric Devices Only (Edge and Border)**:
  - If MSMR is reachable, the score is 10.
  - If MSMR is unreachable, the score is 1.

Note If there is more than one MSMR in a fabric domain, and all the MSMRs are reachable, the score is 10; otherwise, the score is 1.

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 the score is the minimum subscore of the following parameters:

- **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.
- **Free Timer Score**:
  - If number of free timers is 20 percent or more, the score is 10.

- If number of free timers is 20 percent or less, the score is 1.

- **Free Memory Buffers (MBufs)**:
  - If number of free memory buffer is 20 percent or more, the score is 10.
  - If number of free memory buffer is less than 20 percent, the score is 1.

- **Work Queue Element (wqe) Pool Score**:
  - If wqe pool is greater than wqe pool threshold, the score is 10.
  - If wqe pool is at, or lower than wqe pool threshold, the score is 1.

- **Packet Pools**:
  - If packet pool is greater than packet pool threshold, the score is 10.
  - If packet pool is at, or lower than 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 MAP Server(s)—Fabric WLC Only**:
  - If MSMR is reachable, the score is good.
  - If MSMR is unreachable, the score is poor.

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

- 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 20 or Discover Your Network Using CDP, on page 11.
- Configure the location of the device, such as area, site, building, and floor. See Create Sites in the Network Hierarchy, on page 61, and Add Floors to Buildings, on page 64.
- Add devices to the sites. See Add Devices to Sites, on page 162.
- Assign APs and position them on a floor map. See Add, Position, and Delete APs, on page 69.
- Enable Telemetry collection. Telemetry using SNMP poling is enabled by default. For information about Telemetry, see the *Cisco Digital Network Architecture Center Administrator Guide*.

- 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*.

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—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—Inactive. Health score is 0.

Table 44: Client Health Page

Item	Description
Buttons located above the Client Health Map	Contains the following buttons: • **Hide or Show**—Hides or displays the Site Hierarchy site selector or the Client Health map, depending on the toggle selection. • **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. • **All Sites**—Allows you to select a site or building from the drop-down list. Based on what you select, the page refreshes with the relevant information. • **Actions**—Allows you to make changes to the dashboard display when you click **Edit Dashboards** from the drop-down list. See Edit or Delete a Dashboard, on page 217 and Create a Custom Dashboard, on page 215. • **Timeline**—The timeline slider allows you to change the time in the timeline widget.

Item	Description
Client Health Map	Depending on what you select from the **All Sites** list, this dashlet displays a client health map. • **Client Health Map—**The health of all the clients detected in a given site is represented on a geographic location-oriented client healthmap. By default, the client 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 special score of 0 for Inactive clients.
Client Health dashlet	This dashlet includes the following information: • **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 203. • **Wireless** and **Wired** areas**—**Contains the following: ◦ **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 203. ◦ **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. ◦ Red**—**Poor devices. Health score range is 1 to 3. ◦ Orange**—**Fair devices. Health score range is 4 to 7. ◦ Green**—**Good devices. Health score range is 8 to 10. ◦ Grey**—**Inactive devices. Health score is 0. Click the **Wireless** or **Wired** area to open a side bar with additional details.

Item	Description
Onboarding, Connectivity RSSI, and Connectivity Physical Link dashlets	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. • **Client Attempts by 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 Physical Link—**Distribution of wired client device link state: the number of devices that had their physical links up, down, and had errors.

Item	Description
Client Devices Table dashlet	

Item	Description
	Allows you filter, view, and export client device information: • Filter the table based on client type, client health, and data. ◦ **Client Type—**Options are wired and wireless clients. ◦ **Client Health—**Options are: ◦ **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. To determine the threshold values for onboarding, association time, DHCP, and AAA, click the **Client Attempts on Onbording Time** dashlet, to open a side bar. From the side bar, click the appropriate option, and then view the value in the Threshold legend. To determine the threshold value for RSSI, see the Threshold legend in the **Connectivity RSSI** dashlet. • 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: ◦ **Overall Health Score—**This score is the sum of the onboarding and connected scores. ◦ **Onboarding Score—**Indicates the experience of a client device *while* connecting to the network; whether the client connected (onboarded) to the network successfully or not. For more information, see Client Onboarding Score, on page 203. ◦ **Connected Score—**Indicates the experience of a client device *after* the device is connected to the network. For more information, see Client Connectivity Score, on page 204. ◦ **Connected To—**Provides the following information: ◦ **Wireless Clients—**Provides the name of the AP or Cisco WLC to which the client device is connected.

Item	Description
	◦ **Wired Client—**Provides the name of the switch to which the client device is connected. • 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 over a 5-minute interval.

Example: 90% health score = 90 client devices with health score between 8 to 10 / total 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 over a 5-minute interval.

For example: 90% health score = 90 client devices in a target category with health score between 8 to 10 / total 100 network 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 special case of Inactive clients that get a score of 0. 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 the RSSI is equal to or greater than -72 dBm.

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 range determines the Connectivity score and the resulting Overall Health score as shown below:
  - If RSSI is less than -72 dBm, the Connectivity score is 0 and the Overall Health score is 4.
  - If RSSI is equal to -71 dBm, the Connectivity score is 1 and the Overall Health score is 5.
  - If RSSI is equal to -70 dBm, the Connectivity score is 2 and the Overall Health score is 6.
  - If RSSI is equal to -69 dBm, the Connectivity score is 3 and the Overall Health score is 7.
  - If RSSI is equal to or greater than -68 dBm and less than -55 dBm, the Connectivity score is 4 and the Overall Health score is 8.
  - If RSSI is equal to or greater than -55 dBm and less than -45 dBm, the Connectivity score is 5 and the Overall Health score is 9.
  - If RSSI is equal to or greater than -45 dBm, the Connectivity score is 6 and the Overall Health score is 10.

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 45: Client 360 Page

Item	Description
Individual Client Health Score	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 207. If you search by MAC address or IP address, the Individual Client Health score is the health score for that client device. 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 special score of 0 for Inactive clients. • 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—Inactive. Health score is 0.
Client Device tabs	Details about each of the client's devices is represented in a separate tab, for example, *username-macbook* or *username-iphone*. Hover your cursor over a tab to view details about a device, such as device type, OS version, MAC address, and IP address.

Item	Description
Historical Health Graph area	Health information about the selected client device over a period of time. 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. 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, Connectivity, and so on) is also refreshed.

Step 4 View information about issues, onboarding, path trace, application experience, and detail information under the appropriate category.

Table 46: Categories in the Client 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**. For information about the types of issues, see Issues Detected by DNA Center Assurance, on page 219.
Onboarding category	Topology of how a client got on the network, including information about the following services: AAA, DHCP, and DNS. Example of wired client topology: Client > Switch > Router Example of wireless client topology: Client > SSID > Access Point > WLC
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 207.
Application Experience category	Applications running on a client device with their qualitative and quantitative metrics displayed in a table format and chart format. See About Application Experience, on page 209 and View the Application Experience of a Client Device, on page 210.

Category	Description
Detail Information category	Contains the following tabs: Device, RF, and IOS Analytics. Click each tab to get the appropriate information.

Individual Client Health Score

The Individual Client Health score is the minimum score of all monitored items during the observed time interval.

- **Wired Client—**Link to the first switch is up, authentication and authorization is successful, and IP address is received. The client score is 10.
- **Wireless Client—**Client joined the network and the RSSI is equal to or greater than -72 dBm.

See the following topics:

- Client Onboarding Score, on page 203
- Client Connectivity Score, on page 204

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 20 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.

Monitor Application Health

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.

AppX is supported only for Client 360 view, that is, applications as seen by the client. 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 209.

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 Configure Easy Performance Monitoring (ezPM) context for application-performance profile on the device. Use the following commands.

Note Performance profile must be enabled on routers only.

```
Router#configure terminal
Router(config)#performance monitor context Context_Name profile application-performance

Router(config-perf-mon)#exporter destination DNA_Center_IP_Address source
Router's_Interface_Used_to_Reach_DNA_Center transport udp port 6007
Router(config-perf-mon)#traffic-monitor application-client-server-stats
Router(config-perf-mon)#traffic-monitor application-response-time
Router(config-perf-mon)#end
```

Example:

```
performance monitor context my-pm-ctx-8 profile application-performance
exporter destination 172.16.0.1 source GigabitEthernet0/0/1 transport udp port 6007
traffic-monitor application-client-server-stats
traffic-monitor application-response-time
```

2 Attach the context to the interface on which the NetFlow records must be collected. Use the following commands:

```
Router#configure terminal
Router(config)#interface Interface_for_NetFlow_Collection
Router(config-if)#performance monitor context Context_Name
Router(config-if)#end
Router#
```

Example:

```
interface GigabitEthernet0/0/3
ip address 10.0.0.1 255.255.255.0
performance monitor context my-pm-ctx-8
```

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 20 or Discover Your Network Using CDP, on page 11.
- Enable Cisco NetFlow collection on the device. See Enable Cisco NetFlow Collection , on page 209.

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 Score—**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.
- **Destination—**The location of the application server.
- **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.

Step 2 To view the application experience in a chart format, select the radio button next to an application in the table, the charts refresh with the appropriate information.
By default, the charts that display correspond to the first application listed in the table.

Manage Sensor Tests

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 WLC controller and AP 1800S sensor images:

- Cisco WLC controllers (35xx, 55xx, 85xx) software image—8.5.115.0
- Cisco Sensor Device 1800S software image—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 covert the XOR radio as a dedicated sensor.

Note **Sensor Device—**A dedicated AP 1800S 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).

See the following topics for more information:

- View Sensor-Driven Tests, on page 212
- Add a Sensor-Driven Test, on page 213
- Edit, Delete, or Run a Sensor-Driven Test, on page 214
- Provision the Wireless AP1800S Sensor Device, on page 215

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 20 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 **Results-Latest** column displays a red box. Click **Fail** to display information about the failed 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 20 or Discover Your Network Using CDP, on page 11.
- If you are using AP 1800S sensors 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 AP1800S Sensor Device, on page 215

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 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) 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.

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.

Step 5 Click **Next**. The third step, **Select Sensors**, is dispalyed.
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.

Step 6 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.

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 more 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 more 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 more 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 213. You can schedule to run the test on a particular day and time only once.

Provision the Wireless AP1800S Sensor Device

Procedure

Step 1 Create a sensor profile for the AP 1800S sensor device. See Create a Wireless Sensor Device Profile, on page 90.

Note The AP 1800S sensor device with wired connection is supported. To provision the AP 1800S sensor device with wired connection, see the Note in the Create a Wireless Sensor Device Profile, on page 90.

Step 2 Provision the AP 1800S sensor device. See Provision a Sensor Device, on page 164.

Step 3 (Optional) After the sensor device is available in the device inventory, you can choose to upgrade the software image. See Provision Software Images, on page 52.

Manage 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.

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 **Category** 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 **Save** to save the dashboard.
A confirmation dialog is displayed.

Step 12 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, or OS version.

Procedure

Step 1 From the DNA Center home page, choose **Assurance > Dashboards > Dashboard Library**.
The Dashboard Library page appears, listing all the templates and defined dashboards.

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 14 if you selected an existing scope, or continue with Step 6 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 Choose one or more network device models to include in the scope by checking or unchecking the check boxes next to them. Type in the search field to filter devices.

Step 11 Click on **Network OS** to 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.

Step 12 Click **Save Scope** 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**.

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.

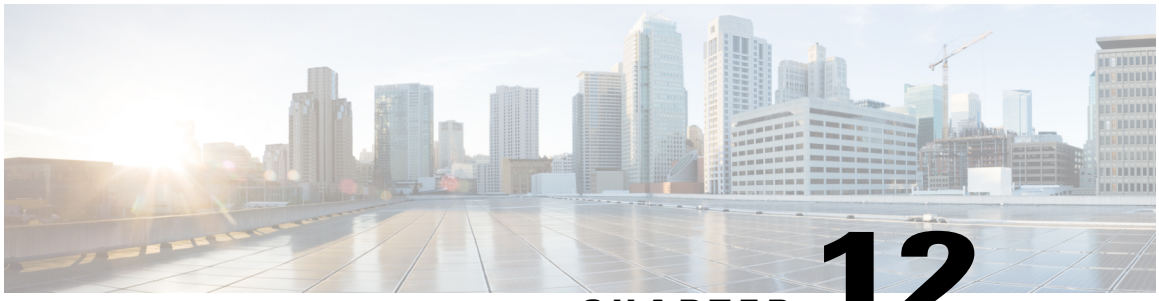
Step 7 Click **OK**.

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.



CHAPTER 12

Issues Detected by DNA Center Assurance

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**.

Issue Catalog

The **Issue Catalog** page shows all the issues that Assurance is capable of monitoring in a customer environment. The page shows the type of issues that are open in a customer environment and the root cause of the issues. To view the Issue Catalog, click **Assurance > Issues > View Issue Catalog**.

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-realted issues such as CPU, memory, fan, and so on.
- **Availability—**Displays device availability issues for APs, WLCs, and so on.
- **Utilization—**Displays utilization issues of APs, WLCs, radios, and so on.
- **Application—**Displays Application Experience issues.
- **Sensor Test—**Displays sensor global issues.

Click an issue to display more information about it. For each issue, the number of open instances of the issue, the root cause of the issue, description of the issue, and the license type are displayed.

Note All the issues are available as part of the Essential subscription license type, which is the base license.

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 *SSID* on *AP Name* (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.

Issue	Description
Value Clients Unable to Connect to SSID—Credentials Rejected	*Value* clients failed to connect to *SSID* 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 *SSID* because of a AAA failure during the authentication phase. **Note** This issue is applicable for both single clients and global clients.
Value Clients Unable to Connect to SSID—Authentication Parameters Rejected	*Value* clients failed to connect to *SSID* 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 *SSID* on *AP Name* (2.4 GHz | 5 GHz) and *WLC Name* because the WLC did not receive a response from the AAA server *IP Address*. **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.
Value Clients Unable to Connect to SSID on WLC—WLC Operational Errors	*Value* clients failed to connect because of operational errors on *WLC Name* 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 *WLC Name* configuration.
Value Clients Unable to Connect to SSID on WLC—WLC Operational Errors	Clients experienced WLC operational errors. *Value* clients failed to connect because of configuration issues in the *WLC Name* during the authentication process.
Client Unable to Connect to SSID through AP and WLC—Client PMK Not Found	This client failed to connect to *SSID* through the *AP Name* (2.4 GHz | 5 GHz) and *WLC Name* because the client Pairwise Master Key (PMK) was not found on the AP and the WLC. Client was roaming from *WLC Name* and *AP Name* [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 *client-name* is experiencing high network latency for application *app-name* located at site *site-name*.
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 *SSID* and *AP Name*, which is connected to *WLC Name*.

Issue	Description
Wireless Client Exhibiting Sticky Behavior	This client is maintaining an association with *AP Name* at *rssiThreshold* 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 *SSID* on *frequency* GHz radio on *AP Name* in location *siteHierarchy*. The AP is connected to *WLC Name*.
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:

Issue	Description
Client Associated with AP Experiencing Poor RF Condition on SSID	This client's RSSI has been below *Value* dBm for more than *Value* 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 *Value* clients that have RSSI Values below *Value* dBm for more than *Value* 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 *AP-Name* and *AP-Name*. 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 *SSID* and *SSID*. 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 *AP-Name*.

DHCP Issues

The following table provides a list of DHCP issues detected by DNA Center Assurance:

Issue	Description
Value Clients Experiencing DHCP Failure on DHCP Server	*Value* clients have not been assigned an IP Address from the DHCP server *Server IP*.

Issue	Description
Value Clients in AP Group Experiencing DHCP Failure	*Value* clients assigned to *AP Group Name* have not been assigned an IP address from the DHCP server *Server IP*.
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 *SSID* on *AP Name* and *WLC Name* because the DHCP IP addressing from the DHCP server *Server IP* timed out. **Note** This issue is applicable for both single clients and global clients.
Value Clients Failing DHCP Attempts in AP Group Because DHCP IP Addressing Timed Out	• DHCP Server: *Value* clients timed out and have not been assigned an IP Address from the DHCP server *Server IP*. • AP Group: *Value* clients assigned to *AP Group Name* timed out and have not been assigned an IP address from the DHCP server *Server IP*.
Client on SSID and Associated with AP (2.4 GHz | 5 GHz) Failed to Obtain IPv4 Address from DHCP Server	This client has not been assigned an IPv4 address by DHCP server *Server IP* on *SSID* over VLAN *VLAN-ID*. This DHCP server has not responded to DHCP discover requests. This client is currently associated with *AP Name* (2.4 GHz | 5 GHz). **Note** This issue is applicable for both single clients and global clients.
Value Wireless Clients Failed to Connect to SSID—No Response form DHCP Server	*Value* clients assigned to VLAN *VLAN-ID* in *Location* have not been assigned an IP address. The DHCP server *Server IP* is not responding to DHCP requests.
Client on SSID and Associated with AP (2.4 GHz | 5 GHz) Failed to Obtain IPv4 Address—Client Side Root Cause	Client failed to complete the DHCP transaction with DHCP server *Server IP*. Client is associated to *SSID* on *AP Name* (2.4 GHz | 5 GHz) radio. **Note** This issue is applicable for both single clients and global clients.
Value Wireless Clients Failed to Connect to SSID—Client Side Root Cause	*Value* assigned to VLAN *VLAN-ID* in *Location* failed to complete the DHCP transaction with DHCP server *Server IP*.
Client Failed to Obtain IPv4 Address from DHCP Server	This client with *MAC Address* was has not been assigned an IPv4 address from the DHCP server *Server IP*. This DHCP server is not responding to DHCP discover requests.

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	This Apple iOS client, running Apple iOS *iOS version*, 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 *SSID* on *AP Name* in *Location*. **Note** This issue is applicable for both single clients and global clients.
Apple iOS Client Disconnected from SSID on AP—Decryption Failure	This Apple iOS client failed to decrypt multiple frames from the AP, and consequently disconnected from the *SSID* on *AP Name* radio *radio-index*. **Note** This issue is applicable for both single clients and global clients.
Apple iOS Client Disconnected from SSID on AP—Captive Portal Verification Failure	This Apple iOS client disconnected from *SSID* on *AP Name* because the captive-portal internet verification process failed. **Note** This issue is applicable for both single clients and global clients.

Client Excessive Onboarding Issues

The following table provides a list of client excessive onboarding issues detected by DNA Center Assurance:

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	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). **Note** This issue is applicable for both single clients and global clients.
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	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). **Note** This issue is applicable for both single clients and global clients.

Issue	Description
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on IP Addressing	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds).
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on Onboarding	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Association took *Value* seconds (expected time should be less than *Value* seconds). • Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). • IP Addressing took *Value* seconds (expected time should be less than *Value* seconds). **Note** This issue is applicable for both single clients and global clients.
Wireless Clients Taking a Long Time to Connect to SSID—Excessive Time on Authentication and Key Exchange Time from the Network/Server Side	*Value* clients taking longer than expected time to connect to *SSID* in *Location*. The server is taking longer than usual time to respond: • These clients took *Value*% longer than association time baseline of *Value Time-Unit* . • These clients took *Value*% longer than authentication and 4-way handshake time baseline of *Value Time-Unit*.
Clients Experiencing Excessive Onboarding Time—Excessive IP Addressing on DHCP Server	*Value* clients are taking longer than expected time to connect through DHCP Server *Server IP*: • Onboarding took an average of *Value* seconds (expected time should be less than *Value* seconds). • IP Addressing took an average of *Value* seconds (expected time should be less than *Value* seconds).

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 WLC Issues	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). The WLC was identified as the slow component in the process. **Note** This issue is applicable for both single clients and global clients.
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	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). The client was slow to respond to network messages. **Note** This issue is applicable for both single clients and global clients.
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	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). The network was slow to carry the authentication messages. **Note** This issue is applicable for both single clients and global clients.
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	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). The network was slow to carry the authentication messages. **Note** This issue is applicable for both single clients and global clients.

Issue	Description
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	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • IP addressing took *Value* seconds (expected time should be less than *Value* seconds). **Note** This issue is applicable for both single clients and global clients.
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz) - Excessive Association Time	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Association took *Value* seconds (expected time should be less than *Value* seconds). **Note** This issue is applicable for both single clients and global clients.
Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Association Failures	This client is taking longer than expected time to connect to *SSID* on *AP Name* (2.4 GHz | 5 GHz): • Onboarding took *Value* seconds (expected time should be less than *Value* seconds). • Association took *Value* seconds (expected time should be less than *Value* seconds). **Note** This issue is applicable for both single clients and global clients.
Client Device Authentication Failed—Dot1.x Failure	The client device *Device Name*" could not be authenticated because *Failure Reason*.
Client Device Authentication Failed—MAB Failure	The client device *Device Name* could not be authenticated because *failure reason*.
Client Failed to Obtain a Response from DNS Server	The client *MAC Address* failed to obtain a response from the DNS Server *DNS Server IP* 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 *WLC Name* due to *Value* or more failed AAA authentication attempts within *Value* 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 *AP Name* (2.4 GHz | 5 GHz) on *SSID*. This client has been excluded by *WLC Name* on Web authentication server (LWA/redirect Value/CWA Value) due to *Value* or more failed Web authentication attempts within *Value* seconds.
Wireless Client Unable to Roam to AP—IDS Shunned List	This client is unable to roam to *AP Name* (2.4 GHz | 5 GHz) on *SSID*. This client was identified by Intrusion Detection System (IDS) as a threat and was shunned.
Value Wireless Clients Failed to Roam on *SSID* as Clients were Excluded Before Roaming—Too Many Web Authentication Failures	*Value* clients connected to *SSID* in *Location* have been excluded due to *Value* or more failed Web authentication attempts on Web authentication server (LWA/redirect Value/CWA Value) within *Value* seconds. As these clients were excluded, they could not roam.
Value Wireless Clients Failed to Roam on *SSID* as Clients were Excluded Before Roaming—Too Many Failed Authentication	*Value* clients connected to *SSID* in *Location* have been excluded due to *Value* or more failed AAA authentication attempts within *Value* seconds. As these clients were excluded, they could not roam.
Client Excluded on SSID on AP (2.4 GHz | 5GHz)—Too Many Authentication Failures	This client has been excluded by *WLC Name* due to *Value* or more failed AAA authentication attempts within *Value* seconds. This client is probably failing authentication because of invalid username or password.
Value Clients Excluded by WLC—Authentication Failures	*Value* clients have been excluded by *WLC Name* due to *Value* or more failed AAA authentication attempts within *Value* seconds. These clients are probably failing authentication on AAA server *Server IP* because of invalid usernames or passwords.
Client Excluded on SSID on AP (2.4 GHz | 5 GHz)—Too Many Web Authentication Failures	This client has been excluded by *WLC Name* on Web authentication server (LWA/redirect Value/CWA Value) due to *Value* or more failed Web authentication attempts within *Value* 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.
Client Excluded on SSID and WLC—IP Theft Issue	This client was excluded on *SSID* and *WLC Name*. 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.
Client Excluded on SSID and WLC—IDS Shunned List	This client was excluded on *SSID* on *AP Name* (2.4 GHz | 5 GHz) and *WLC Name*. 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.

Issue	Description
Client Excluded on SSID and WLC—Too Many Association Failures	This client was excluded on *SSID* on *AP Name* (2.4 GHz | 5 GHz) and *WLC Name* 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:

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 *AP Name* to *AP Name* because the AAA server *IP Address* 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 *AP Name* and *WLC Name* to *AP Name* and *WLC Name* 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 *SSID* through the *AP Name* (2.4 GHz | 5 GHz) and *WLC Name* because the client Pairwise Master Key (PMK) was not found on the AP and WLC. Client was roaming from *WLC Name* and *AP Name* [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 *WLC Name* configuration. Client was roaming from *AP Name* on *WLC Name*.
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 *SSID* while roaming to *AP Name* (2.4 GHz | 5 GHz) and *WLC Name* because the WLC did not receive a response from the AAA server *IP Address*.
Client Unable to Roam on SSID on AP (2.4 GHz | 5GHz)—Client Side Timeout	This client failed to connect to *SSID* while roaming to *AP Name* (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 *SSID* while roaming on *WLC Name* because of internal failures in the WLC, such as insufficient buffer or insufficient memory.

Switch and Fabric Issues

DNA Center Assurance provides suggested actions for switch and fabric issues similar to the following:

Issue	Description
Device Experiencing High CPU Utilization	CPU utilization on *Device Name* has exceeded *threshold*% in the last 30 minutes.
Device Experiencing High Memory Utilization	Memory utilization on *Device Name* has exceeded *threshold*% in the last 30 minutes.
Device Experiencing High Temperature	The temperature on *Device Name* has exceeded *threshold*% degree Celsius in the last 30 minutes.
Network Device Unreachable from Controller	This network *Network Device Name* is unreachable from controller. The device role is *Fabric or Device Role*.
Fan Failure on Device	The fan(s) in *Device Name* have failed critically.
Power Supply Failure on Device	The power supply(ies) in *Device Name* have failed critically.
Switch Rebooting	This *Switch Name* is rebooting because of a power outage or system crash.
Interface Name Flapping in the Network	The switch port *Interface Name* has flapped *Value* times within the past *Value* minutes.
Applications Experiencing Slow Response Time—High Input Utilization on Interface	Applications are experiencing slow response time because of *Input Utilization*% input utilization on *Interface Name*.
Applications Experiencing Slow Response Time—High Output Utilization on Interface	Applications are experiencing slow response time because of *Output Utilization*% output utilization on *Interface Name*.
Applications Experiencing Slow Response Time—Input Errors on Interface	Applications are experiencing slow response time because of *Input Errors*% input errors on interface *Interface Name*.
Applications Experiencing Slow Response Time—High Output Utilization on Interface	Applications are experiencing slow response time because of *Output Utilization*% output utilization on *Interface Name*.
Applications Experiencing Slow Response Time—Input Errors on Interface	Applications are experiencing slow response time because of *Input Errors*% input errors on *Interface Name*.
Status Down on *Role* Node Fabric-Facing Interface	The status of the *Role* node fabric-facing *Interface Name* is down, which is impacting many fabric services from functioning properly.
Reachability Issue Between Fabric Edge and Fabric Border in Overlay *vrf*	In overlay *vrf*, the Fabric Edge device *Source Device IP* failed to reach the Fabric Border device *Destination Device IP*, which is impacting many fabric services from functioning properly.

Issue	Description
Reachability Issue Between Fabric Edge Device and Fabric Border Device in Underlay	There is a connectivity failure between the Fabric Edge device *Source Device IP* and the Fabric Border device *Destination Device IP* 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 *Source Device IP* and the Fabric Control Plane device *Destination Device IP* 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 *Source Device IP* and the Fabric Control Plane device *Destination Device IP* 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 *Source Device IP* and the ISE/AAA server *Destination Device IP*, which is impacting many fabric services from functioning properly.
Network Device Lost Connectivity to the DHCP Server in Underlay	The network device *Device IP* cannot reach the DHCP server *DHCP Server IP* in underlay.
Network Device Lost Connectivity with External Services	The network device *Device IP* cannot reach the *Destination IP*. The device has lost connectivity to external services.
Network Device Lost Connectivity to the DHCP Server in Overlay *vrf*	The network device *Device IP* cannot reach the DHCP server *DHCP Server IP* in overlay *vrf*.
Border Network Device Lost Connectivity to External URL	The border network device *Device IP* cannot reach user-provisioned external URL *Destination IP*.
Reachability Issue Between Network Device and LISP Control Plane "	There is a connectivity failure between the network device *Device IP* and LISP Control Plane *Map Server* , which is impacting many fabric services from functioning properly.
Map Cache Entries Exceeded Limit	The SNMP map cache Limit *Map Cache Size* has exceeded the threshold *Map Cache Limit* in the last 5 minutes.
High CPU Utilization on Network Device	Network device *Device Name* is experiencing *Value*% CPU utilization.
High Memory Utilization on Network Device	Network device *Device Name* is experiencing *Value*% memory utilization.
High Temperature on Network Device	Network device *Device Name* is experiencing *Value* degree Celsius temperature.
Controller Unable to Reach Network Device	This network device *Device Name* with *Device Role* is unreachable from the controller.

Issue	Description
Fan Failure on Network Device	The fans in the network device *Device Name* have failed.
Power Supply Failure on Network Device	The power supplies in the network device *Device Name* have failed.
Switch Rebooting	This switch *Switch Name* is rebooting.
Interface Name Flapping in the Network	The switch port *Interface Name* is flapping.
High Input/Output Utilization on Interface	Interface *Interface Name* is experiencing high input/output utilization: Rx *Rx Input Utilization*% Tx *Tx Output Utilization*%
High Input/Output Errors on Interface	Interface *Interface Name* is experiencing high input/output errors: Rx *Rx Error Percent*% Tx *Tx Error Percent*%
Stackmember Running an Incompatible Image	Stackmember is running an incompatible image.
Stackmember Removed from Stack	Stackmember has been removed from the stack.
PoE Power Controller: *Error Message*	PoE power controller error *Error Message* detected on the switch.
Interface Power Overdrawn	The power on the *Interface Name* is overdrawn.
Switch Experiencing TCAM Exhaustion	The switch *Switch Name* has a TCAM area that exceeds a threshold of 95%.

Interface Issues

DNA Center Assurance provides suggested actions for interface issues similar to the following:

Issue	Description
Interface Name Flapping in the Network	The switch port *Interface Name* has flapped *Value* times within the past *Value* minutes.
Applications Experiencing Slow Response Time—High Input Utilization on Interface	Applications are experiencing slow response time because of *Input Utilization*% input utilization on *Interface Name*.

Issue	Description
Applications Experiencing Slow Response Time—High Output Utilization on Interface	Applications are experiencing slow response time because of *Output Utilization*% output utilization on *Interface Name*.
Applications Experiencing Slow Response Time—Input Errors on Interface	Applications are experiencing slow response time because of *Input Errors*% input errors on *Interface Name*.

Fabric Issues

DNA Center Assurance provides suggested actions for switch and fabric issues similar to the following:

Issue	Description
Status Down on *Role* Node Fabric-Facing Interface	The status of the *Role* node fabric-facing *Interface Name* 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 *Source Device IP* and the Fabric Border device *Destination Device IP* 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 *vrf*	In overlay *vrf*, the Fabric Border device *Source Device IP* failed to reach the DHCP Server *Destination Device IP*, 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)"	*Router IP Address* at *Router location*—Border Gateway Protocol (BGP) peering with neighbor *Interface IP address* 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	*Router IP Address* at *Router location*—BGP is flapping on *Interface IP Address* because of missing BGP hello keepalives or because of a peer terminating the session.

Issue	Description
Process 1, Nbr on Went From FULL to DOWN Status, Neighbor Down	OSPF adjacency failed with *IP Address* at *Device Location* on *Interface Name*: dead timer expired.
SIP0/1 Interface State Changed to Down on Router	*Router Name* at *Router location* - *Interface Name* state changed to Down.
High Input/Output Utilization on Router Interface	High Input/Output utilization Rx *Value*% Tx *Value*% on *Interface Name*
Router Experiencing High Memory Utilization	Memory utilization has exceeded *Value*% over the last *Value* minutes on *Router Name*.
Router Experiencing High CPU Utilization	CPU Utilization has exceeded *Value*% over the last *Value* minutes on *Router Name*.
Router Experiencing High Temperature	The temperature of *Router Name* 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 *AP Name* is no longer connected to a WLC. This AP was previously connected to the switch *Switch Name* and *port ID*.
AP Flapping Between WLC(s)	The *AP Name* has disconnected from *Old WLC Name* and reconnected to *Current WLC Name.*
AP Experiencing High CPU Utilization	CPU utilization for the *AP Name* has exceeded the *Theshold* % threshold. This issue is potentially impacting *Value* client(s).
AP Experiencing High Memory Utilization	Memory utilization for the *AP Name* has exceeded the *Theshold* % threshold. This issue is potentially impacting *Value* client(s).
AP Rebooted Due to a Hardware or Software Crash	The *AP Name* 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 *AP Name* has exceeded the *Theshold* % threshold and is currently experiencing *Utilization* % utilization. This issue is impacting *Value* client(s).
The 5 GHz Radio on AP Experiencing High Utilization	The 5 GHz radio on the *AP Name* has exceeded the *Theshold*% threshold and is currently experiencing *Utilization* % utilization. This issue is impacting *Value* client(s).

Issue	Description
AP Experiencing a Coverage Hole	The *AP Name* is currently experiencing a coverage hole. *Value* 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 *WLC Name* has exceeded the *Theshold* % threshold in the past 15 minutes. This issue is potentially impacting *Value* client(s).
WLC Rebooted	The *WLC Name* has rebooted due to a hardware or software crash.
High AP License Utilization on WLC	The *WLC Name* is licensed to support *Max-Count* AP(s) and it currently has *In Use Count* AP(s). If this trend continues, this WLC will exhaust all of its AP license(s).
Power Supply on WLC Failed	The *Power Index* power supply has failed on the *WLC Name.*This WLC is now operating with a single power supply.
WLC Not Exporting Data	The *WLC Name* is not exporting WSA data. It was previously connected to the switch *NW Device Name* and port *Target Interface Name*. The switch port is currently *Link Status*.
WLC Not Exporting AP Data	The *WLC Name* is not exporting WSA AP data since the last 15 mintutes.
WLC Not Exporting Client Data	The *WLC Name* is not exporting Client data since the last 15 mintutes.
WLC AP License Exhaustion	The *WLC Name* is currently licensed to support *Max-Count* AP(s) and is now operating at its full licensed capacity. No additional AP can join this WLC.

Sensor Issues

The following table provides a list of sensor issues detected by DNA Center Assurance:

Issue	Description
Value Sensors Failed to Connect to the Wireless Network	*Value* sensors from *Location* failed to connect to *SSID*. They either failed to associate, or authenticate, or get an IP address.
Value Sensors Failed to Get an IPv4 Address from the DHCP Server	*Value* sensors from *Location* have failed to get an IPv4 address from DHCP server *IP Address* in *VLAN ID*. The DHCP server is reachable.

Issue	Description
Value Sensors Slow to Get an IPv4 Address from the DHCP Server	*Value* sensors from *Location* are slow to get an IPv4 address from DHCP server *IP Address*. The sensors are getting an IPv4 address on an average in *Value* 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.
Value Sensors Unable to Reach the the DNS Server	*Value* sensors from *Location* are unable to reach the DNS server *IP Address*. Pings are failing, which will impact user connectivity.
Value Sensors Failed to Resolve Domain Name with the DNS Server	*Value* sensors from *Location* are unable to resolve the given *Test Domain Name* with the DNS server *IP Address*. This will impact connectivity. The DNS server is reachable.
Value Sensors Experiencing Slow Response from the DNS Server Host	*Value* sensors from *Location* are reporting slow response from the DNS server host *IP Address*. The ping response time to the host is on an average *Value* seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
Value Sensors Experiencing Slow Name Resolution from the DNS Server	*Value* sensors from *Location* are reporting slow name resolution time from the DNS Server *IP Address*. The name resolution time is on an average *Value* 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.
Value Sensors Not Able to Reach the Test Host	*Value* sensors from *Location* are not able to reach test host *IP Address*. Pings to the hosts are failing.
Value Sensors Experiencing Slow Response from the Host	*Value* sensors from *Location* are reporting slow response from the host *IP Address*. The ping response time to the host is on an average *Value* seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
Value Sensors Experiencing Slow Response from the Local Gateway	*Value* sensors from *Location* are reporting slow response from their local gateway in VLAN *x, y*. The ping response time to the gateway is on an average *Value* seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
Value Sensors Not Receiving a Response from their Local Gateway	*Value* sensors from *Location* are reporting no ping responses from their local gateway in VLAN *x, y*. This might indicate a network issue that could lead to network access problems.
Value Sensors Not Able to Reach the RADIUS Server	*Value* sensors from *Location* are not able to reach the RADIUS server host *IP Address*. Pings are failing.

Issue	Description
Value Sensors Experiencing Slow Response from the RADIUS Server	*Value* sensors from *Location* are reporting slow response from the RADIUS server host *IP Address*. The ping response time to the host is on an average *Value* seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow onboarding.
Value Sensors Experiencing Slow Authentication Time with the RADIUS Server	*Value* sensors from *Location* are reporting slow authentication time with RADIUS server *IP Address*. The sensors are authenticating on an average in *Value* seconds. Clients should be able to authenticate in 3 seconds. This slow authentication could lead to poor onboarding experience.
Value Sensors Failed to Authenticate with the RADIUS Server	*Value* sensors from *Location* are unable to authenticate with the RADIUS server *IP Address*.
Value Sensors Unable to Reach the Outlook Web Access Host	*Value* sensors from *Location* are not able to reach the Outlook Web Access host *IP Address*. Pings to the Outlook Web Access hosts are failing.
Value Sensors Experiencing Slow Response from the Outlook Web Access Host	*Value* sensors from *Location* are reporting slow response from the Outlook Web Access host *IP Address*. The ping response time to the host is on an average *Value* 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.
Value Sensors Experiencing Slow Response from the Outlook Web Access' First Hop Gateway	*Value* sensors from *Location* 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 *Value* seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
Value Sensors Experiencing Slow Mail Connection Time to Outlook Web Access	*Value* sensors from *Location* are reporting slow connection time to the Outlook Web Access *IP Address*. The sensors are connecting to the Outlook Web Access on an average in *Value* seconds. Clients should be able to connect to the Outlook Web Access in *Value* seconds. This might lead to poor mail experience.
Value Sensors Failed to Connect to the Outlook Web Access	*Value* sensors from *Location* are unable to connect to the Outlook Web Access. Users might not be able to send mail.
Value Sensors Unable to Reach the Web Server	*Value* sensors from *Location* are not able to reach the Web server host *IP Address*. Pings to the web server hosts are failing.
Value Sensors Experiencing Slow Response from the Web Server	*Value* sensors from *Location* are reporting slow response from the Web server host *IP Address*. The ping response time to the host is on an average *Value* 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
Value Sensors Experiencing Slow Response from the Web Server First Hop Gateway	*Value* sensors from *Location* are reporting slow response from their Web server's first hop gateway in VLAN *x,y*. The ping response time to the gateway is on an average *Value* seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.
Value Sensors Experiencing Slow Web Response Time from the Web Server	*Value* sensors from *Location* are reporting slow web page load time from the Web server *IP Address*. The sensors are connecting and loading the web page on an average in *Value* seconds. Clients should be able to load the page in *Value* seconds. This could lead to poor web experience.
Value Sensors Failed to Load Page from the Web Server	*Value* sensors from *Location* are unable to load a page with the Web server *IP Address*.
Value Sensors Unable to Reach the SSH Server	*Value* sensors from *Location* are not able to reach the SSH server host *IP Address*. Pings are failing.
Value Sensors Experiencing Slow Response from the SSH Server	*Value* sensors from *Location* are reporting slow response from the SSH server host *IP Address*. The ping response time to the host is on an average *Value* seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow SSH performance.
Value Sensors Experiencing Slow SSH Login Time	*Value* sensors from *Location* are reporting slow SSH login time to SSH server *IP Address*. The sensors are connecting on an average in *Value* seconds. Clients should be able to connect in *Value* seconds. This could lead to poor SSH experience.
Value Sensors Unable to Connect with the SSH Server	*Value* sensors from *Location* are unable to connect with the SSH server *IP Address*.
Value Sensors Unable to Reach the Mail Server	*Value* sensors from *Location* are not able to reach the Mail server host *IP Address*. Pings are failing.
Value Sensors Experiencing Slow Response from the Mail Server	*Value* sensors from *Location* are reporting slow response from the Mail server host *IP Address*. The ping response time to the host is on an average *Value* seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow mail performance.
Value Sensors Experiencing Slow Connection Time to the Mail Server	*Value* sensors from *Location* are reporting slow connection time to the Mail server *IP Address*. The sensors are connecting to the Mail server on an average in *Value* seconds. Clients should be able to connect in *Value* seconds. This can lead to poor mail experience.
Value Sensors Unable to Connect to the Mail Server	*Value* sensors from *Location* are unable to connect to the Mail server *IP Address*. Users might not be able to use mail services.

Issue	Description
Value Sensors Unable to Reach the FTP Server	*Value* sensors from *Location* are not able to reach the FTP server host *IP Address*. Pings are failing.
Value Sensors Experiencing Slow Response from the FTP Server	*Value* sensors from *Location* are reporting slow responses from the FTP server host *IP Address*. The ping response time to the host is on an average *Value* 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	*Value* sensors from *Location* are reporting slow FTP transfer time with the FTP server *IP Address*. The sensors are transferring a file size *Value* on an average in *Value* seconds. Clients should be able to do this in *Value* seconds. This could lead to poor FTP application experience.
Value Sensors Failed to Transfer File with the FTP Server	*Value* sensors from *Location* are unable to transfer file with the FTP server *IP Address*. Users might not be able to use FTP services on this server.
Value Sensors are Unable to Connect to the FTP Server	*Value* sensors from *Location* are unable to connect to FTP server *IP Address*. Users might not be able to use FTP services on this server.