



Configure Network Settings

- [Network Settings Overview](#), on page 1
- [Add Cisco ISE or Other AAA Servers](#), on page 2
- [Configure Global Network Servers](#), on page 3
- [Global Device Credentials Overview](#), on page 3
- [Configure IP Address Pools](#), on page 12
- [Configure Service Provider Profiles](#), on page 17
- [Configure Global Wireless Settings](#), on page 18

Network Settings Overview

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 DHCP, DNS, AAA, NTP, and so on; IP address pools; Device Credential profiles; Telemetry settings such as Syslog, Traps, and Netflow.
- **Site settings:** Settings defined here override global settings and can include settings for servers, IP address pools, and device credential profiles.



Note Changes in network settings that are being used by the active fabric are not supported. These network settings include site hierarchy, renaming IP pools, and several other features.



Note Certain network settings can be configured on devices automatically using the Device Controllability feature. When Cisco DNA Center configures or updates devices, the transactions are captured in the Cisco DNA Center audit logs. You can use the audit logs to help you track changes and troubleshoot issues.

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

- Network servers, such as AAA, DHCP, and DNS—For more information, see [Configure Global Network Servers](#), on page 3.

- Device credentials, such as CLI, SNMP, and HTTP(S)—For more information, see [Configure Global CLI Credentials, on page 4](#), [Configure Global SNMPv2c Credentials, on page 4](#), [Configure Global SNMPv3 Credentials, on page 6](#), and [Configure Global HTTPS Credentials, on page 7](#).
- IP address pools—For more information, see [Configure IP Address Pools, on page 12](#).
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—For more information, see [Configure Global Wireless Settings, on page 18](#).
- Configure global telemetry settings, such as syslog, SNMP, and NetFlow Collector servers using telemetry.

Add Cisco ISE or Other AAA Servers

You can define Cisco Identity Services Engine (ISE) servers or other, similar AAA servers for network, client, and endpoint authentication at the site or global level. For network authentication, RADIUS and TACACS protocols are supported. For client and endpoint authentication, only RADIUS is supported. Only one Cisco ISE is supported per Cisco DNA Center.

You can configure the source interface under the RADIUS or TACACS server group to support multi-ISE configuration, wherein each Cisco ISE cluster has its own server group. The source interface used for RADIUS and TACACS servers is determined in the following way:

- If the device has a Loopback0 interface configured, Loopback0 is configured as the source interface.
- Otherwise, the interface that Cisco DNA Center uses as the management IP is configured as the source interface.

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 with a /32 mask. Subsequently, any changes to those devices in Cisco ISE are sent automatically to Cisco DNA Center.

For FIPS mode of deployment the shared secret consists of shared secret, keywrap and message authenticator code key.

Step 1 Click the menu icon () and 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 Set the AAA server for network users, client/endpoint users, or both.

Step 5 Check the **Network** and/or **Client/Endpoint** check boxes and configure servers and protocols for the AAA server.

Step 6 Choose the **Servers** for authentication and authorization: **ISE** or **AAA**.

- If you choose **ISE**, configure the following:
 - From the **Network** drop-down list, choose the IP address of the Cisco 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 Cisco DNA Center home page. Selecting a Cisco ISE IP populates the primary and additional IP address drop-down lists with Policy Service Nodes (PSN) IP addresses for the selected Cisco ISE. You can either enter an IP address for the AAA server or choose the PSN IP address from the **IP Address (Primary)** and **IP Address (Additional)** drop-down lists.
 - Choose the **Protocol**: **RADIUS** or **TACACS**.

Note AAA settings for a physical and managed site for a particular wireless controller must match, or provisioning fails.

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

Step 7 Click **Save**.

Configure Global Network Servers

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



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

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

Step 2 In the **DHCP Server** field, enter the IP address of a DHCP server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.
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 can click the plus icon and enter both IPv4 and IPv6 addresses.
You must define at least one DNS server in order to create IP address pools.

Step 4 Click **Save**.

Global Device Credentials Overview

"Global device credentials" refers to the common CLI, SNMP, and HTTPS credentials that Cisco DNA Center uses to discover and collect information about the devices in your network. Cisco DNA Center uses global credentials to authenticate and access the devices in a network that share these configured device credentials. You can add, edit, and delete global device credentials. You can also associate credentials to the Global site or a specific site.

Configure Global CLI Credentials

You can configure and save up to 10 global CLI credentials.

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

Step 2 With the Global site selected, in the **CLI Credentials** area, click **Add**.

Step 3 Enter information in 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	<p>Password that is used to log in to the CLI of the devices in your network.</p> <p>For security reasons, re-enter the password as confirmation.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Enable Password	<p>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</p> <p>For security reasons, re-enter the enable password.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Step 4 Click **Save**.

To apply the credential to a site, click on the site in the hierarchy on the left, select the button next to the credential, then 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 **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **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 Global SNMPv2c Credentials

You can configure global SNMPv2c credentials to monitor and manage your network devices.



Note Cisco DNA Center does not support SNMPv2c device credentials when FIPS mode is enabled. You must specify SNMPv3 credentials instead.

Before you begin

You must have your network's SNMP information.

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

Step 2 With the Global site selected, in the **SNMP Credentials** area, click **Add**.

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

Table 2: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Read Community: Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Write Community: Write community string used to make changes to the SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Step 4 Click **Save**.

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

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **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 Global SNMPv3 Credentials

You can configure global SNMPv3 credentials to monitor and manage your network devices.

Before you begin

You must have your network's SNMP information.

Step 1 Click the menu icon () and choose **Design > Network Settings > Device Credentials**.

Step 2 With the Global site selected, in the **SNMP Credentials** area, click **Add**.

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

Table 3: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv: Does not provide authentication or encryption. • AuthNoPriv: Provides authentication, but does not provide encryption. • AuthPriv: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Privacy Type	<p>Privacy type. (Enabled if you select AuthPriv as Mode.) Choose one of the following privacy types:</p> <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • 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 **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **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 Global HTTPS Credentials

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

Step 2 With the Global site selected, in the **HTTPS Credentials** area, click **Add**.

Step 3 Enter the following information:

Table 4: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .
Read	<p>You can configure up to 10 HTTPS read credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>
Write	<p>You can configure up to 10 HTTPS write credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>

Step 4 Click **Save**.

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

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **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.

Guidelines for Editing Global Device Credentials

The following are guidelines and limitations for editing existing global device credentials:

- Cisco DNA Center uses the following process when you edit, save, and then apply a global device credential:
 1. Cisco DNA Center pushes the credential to the device that has local authentication. With local authentication, credential changes are applied and Cisco DNA Center manages the devices using these credentials.

(Cisco DNA Center does not push CLI credential changes to a device that is under a site with an inherited or configured AAA server. With AAA authentication, credential changes are not applied. Cisco DNA Center manages the devices using these credentials only if the same credentials exist on the AAA server.)
 2. After successfully pushing the credential to the device, Cisco DNA Center confirms it can reach the device using the new credential.



Note If this step fails, Inventory uses the old credentials to manage the device even though Cisco DNA Center pushed the new credentials to the device. In this case, the **Provision > Inventory** window might indicate that the device is Unmanaged if you updated an existing credential.

3. After successfully reaching the device using the new credential, the Cisco DNA Center Inventory starts managing the device using the new credential.
- Sites can contain devices that use SNMPv2c and SNMPv3 credentials. When you edit and save global SNMPv2c or SNMPv3 credentials, Cisco DNA Center pushes those changes to devices and enables that credential. For example, if you have a device that uses SNMPv2c, but you edit and save the SNMPv3 global credential, Cisco DNA Center pushes the new SNMPv3 credential to all devices in the associated site and enables it, meaning that all devices will be managed using SNMPv3, even the devices that previously had SNMPv2c enabled.
 - To avoid any possible disruptions, modify the **User Name** when you edit CLI credentials. This creates a new CLI credential and leaves any existing CLI credentials unchanged.

Edit Global Device Credentials

You can edit and save global device credentials without Cisco DNA Center applying those credential changes until you're ready. When you decide to apply the changes, Cisco DNA Center searches all sites that reference the device credential you changed and pushes the change to all the devices.

You can update or create new global device credentials, but Cisco DNA Center never removes any credentials from devices.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > Device Credentials**.
- Step 2** With the Global site selected, click **Manage Credentials**, check the check box for the device credential that you want to change, and choose **Actions > Edit**.
- Step 3** In the **Edit Credentials** dialog box, make any changes, and click **Save**.
- Note** The CLI password credentials support only *ASCII-printable characters* (character code 32-127; see https://en.wikipedia.org/wiki/ASCII#Printable_characters).
- Step 4** In the credential tile, click **Apply**.
- Step 5** In the **Apply Credentials** dialog box, select whether to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **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.

A status message indicates whether the device credential change succeeded or failed.

- Step 6** To view the status of the credential change, choose **Provision > Network Devices > Inventory**.

The **Credential Status** column displays one of the following statuses:

- Success: Cisco DNA Center successfully applied the credential change.
- Failed: Cisco DNA Center was unable to apply the credential change. Hover over the icon to display additional information about which credential change failed and why.
- Not Applicable: The credential is not applicable to the device type.

If you edited and saved more than one credential (for example, CLI, SNMP, and HTTPS), the **Credential Status** column displays **Failed** if Cisco DNA Center was unable to apply *any* of the credentials. Hover over the icon to display additional information about which credential change failed.

Associate Device Credentials to Sites

The sites you create under the Global site can inherit the global device credentials, or you can create different device credentials specific for a site.

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

Step 2 Select a site from the hierarchy in the left pane.

Step 3 Click **Manage Credentials**.

Step 4 Select the credentials that you want to associate with the selected site and then click **Assign**.

A success message appears at the bottom of the screen indicating the device credential was successfully associated with the site.

Manage Device Credentials

The Manage Credentials workflow allows you to create, edit, assign, and apply credentials to devices.

Credentials are assigned to **Global** or to the sites, buildings, or floors that you choose. If you assign credentials at the global level, all the sites, buildings, and floors inherit the settings from the global level.

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

Step 2 In the left pane, choose **Global** or specific sites, buildings, or floors, as required.

Step 3 Click **Manage Credentials**.

The **Manage Credentials** window opens.

Step 4 From the **Add** drop-down list, choose any of the following credentials:

- CLI
- HTTP(S) Read
- HTTP(S) Write
- SNMPv2c Read
- SNMPv2c Write
- SNMPv3

Step 5 In the **Add New Credentials** window, do the following:

a. Complete the required fields.

b. Check the **Assign credential to site** check box.

Note If the box is not checked, the credential will get created but not assigned to any site.

c. Click **Save**.

The newly created credential appears in the **Manage Credentials** window.

Step 6 Choose the credential that you want to assign and click **Assign**.

Step 7 To apply the credentials, do any one of the following:

- To apply a credential across the entire site hierarchy, go to **Manage Credentials**, hover your mouse over the desired credential's **Actions** menu, and choose **Apply**.

- To apply a credential only to a specific site, choose the desired site in the left pane and click **Assign** on the card corresponding to that credential.

Step 8 In the **Apply Credentials** window, do the following:

- To apply the new credentials now, click the **Now** radio button and click **Apply**.
- To apply the new credentials at a later time, click the **Later** radio button. Then define the date and time of the update and click **Apply**.

The credentials are applied to all the applicable sites.

You can reschedule any apply credentials task that has not yet started.

Step 9 To view the status of your task, do any one of the following:

- In the **Device Credentials** page, click the refresh icon at the top right corner. Hover your cursor over the icon next to the heading in the credential card.
- Choose **Provision > Inventory**. The **Credential Status** column shows the status.
- Choose **Activities > Audit Log**.

Step 10 To edit the credentials, do the following:

- a. Click the edit icon adjacent to the corresponding credential.

Alternatively, in the **Manage Credentials** window, hover your cursor over the ellipsis icon next to the credential name and click **Edit**.

- b. In the **Edit Information** window, click **OK**.
- c. In the **Edit Credentials** window, make the required changes.
- d. Click **Save**.

Step 11 To reschedule the **Start** time of a credential application, do one of the following:

- **Task scheduled globally:** In the **Manage Credentials** window, hover your cursor over the horizontal ellipsis icon next to the credential name and choose **Apply**, and then click **Apply**.
- **Task scheduled from the main page for sites, buildings, or floors:** Return to the sites, buildings, or floors for which the task was originally scheduled and click **Apply** on the corresponding credential card.

Note You cannot change the time zone.

Configure IP Address Pools

Cisco DNA Center supports IPv4 and IPv6 dual-stack IP pools.

You can manually create IPv4 and IPv6 address pools.

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

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.

Step 2 Click **Add** and complete the required fields in the **Add IP Pool** window.

If you have configured Cisco DNA Center to communicate with an external IP address manager, you cannot create an IP pool that overlaps an existing IP address pool in the external IP address manager.

Step 3 Click **Save**.

The newly added pool appears in the IP Address Pools table. You can click the **IPv4** or **IPv6** option in the **SUBNET TYPE** area if you prefer to view only the IPv4 or IPv6 address pools.

Note When you edit an IP address pool and make DHCP changes, you do not need to reprovision devices using that IP address pool.

Import IP Address Pools from an IP Address Manager

You can import IP address pools from Bluecat or Infoblox.



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

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

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.

Step 2 From the **Actions** drop-down list, choose **Import from IPAM Server** and complete the required fields.

Step 3 Enter a CIDR and then click **Retrieve** to get the list of IP pools available to import.

Step 4 Click **Select All** or choose the IP address pools to import, then click **Import**.

Import IP Address Pools from a CSV File

You can import IP address pools from a CSV file.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.

Step 2 From the **Actions** drop-down list, choose **Import from CSV File**.

Step 3 Click **Download Template** to download the latest sample file.

Step 4 Add the IP address pools to the file and save the file.

Step 5 Upload the CSV file by doing one of the following actions:

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

Step 6 Click **Import**.

Reserve an IP Pool

Before you begin

Ensure that one or more IP address pools have been created.

Step 1 Click the menu icon () and choose **Design > Network Settings > IP Address Pools**.

Step 2 Expand the hierarchy pane and choose a site.

Step 3 Click **Reserve** and complete the following fields to reserve all or part of an available global IP address pool for the specific site:

- **IP Address Pool Name:** Unique name for the reserved IP address pool.
- **Type:** Type of IP address pool. For LAN automation, choose **LAN**. Options are:
 - **LAN:** Assigns IP addresses to LAN interfaces for applicable underlays.
 - **Management:** Assigns IP addresses to management interfaces.
 - **Service:** Assigns IP addresses to service interfaces.
 - **WAN:** Assigns IP addresses to WAN interfaces.
 - **Generic:** Used for all other network types.
- **IP Address Space:** IPv4 and IPv6 address pool from which you want to reserve all or part of the IP addresses.
- **CIDR Prefix/Number of IP Addresses:** IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses you want to reserve. If you choose $\backslash 64$ as the **CIDR Prefix** for an IPv6 IP pool, the **SLAAC** option is checked. (When **SLAAC** is selected, the devices automatically acquire IP addresses without the need for DHCP servers.)
- **Gateway:** Gateway IP address.
- **DHCP Servers:** DHCP server IP address(es).
- **DNS Servers:** DNS server address(es).

Step 4 Click **Reserve**.

If you reserve both IPv4 and IPv6 address pools, which means the fabric is provisioned with a dual-stack IP pool, you cannot switch back to a single-stack IP pool if the IPv6 pool is already attached to a VN.

However, if the IPv6 pool is not attached to a VN, you can downgrade it from a dual-stack IPv6 to a single-stack IPv4 pool. To downgrade to a single stack, in the IP Address Pools window, click **Edit** for the dual-stack IP pool. In the **Edit IP Pool** window, uncheck the **IPv6** check box and click **Save**.

Edit IP Pools

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.
- Step 2** Choose the Global site or expand the hierarchy tree and choose the desired site.
- Step 3** To edit all the IP pools in bulk, do the following:
- From the **Actions** drop-down list, choose **Edit All**.
 - Click **Yes** in the **Warning** message.
 - In the **Edit IP Pool** window make the desired changes and click **Save**.
- Step 4** To edit only the desired IP pools, do the following:
- Choose the desired IP pools and from the **Actions** drop-down list, click **Edit Selected**.
You can also click **Edit** corresponding to the chosen IP pools.
 - In the **Edit IP Pool** window make the desired changes and click **Save**.
-

Delete IP Pools

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.
- Step 2** Choose the Global site or expand the hierarchy tree and choose the desired site.
- Step 3** To delete all the IP pools in bulk, do the following:
- From the **Actions** drop-down list, choose **Delete All**.
 - Click **Yes** in the **Warning** message.
- Step 4** To delete only the desired IP pools, do the following:
- Choose the desired IP pools and from the **Actions** drop-down list, click **Delete Selected**.
You can also click **Delete** corresponding to the chosen IP pools.
 - Click **Yes** in the **Warning** message.
-

Clone an IP Pool

You can clone an existing IP pool at the site level. When you clone an IP pool, the DHCP server and DNS server IP addresses are automatically filled.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.
- Step 2** Expand the hierarchy tree, and then choose a site.
- Step 3** Locate the desired IP pool and, in the **Actions** area, click **Clone**.
- Step 4** In the **Clone IP Pool** window, do the following:

- a) Optionally, edit the pool name. (You cannot edit the Type, IP Address Space, or Global Pool values, which are inherited from the pool from which you are cloning.)
 - b) Edit the CIRD prefix values as necessary.
 - c) Click **Clone**.
-

Release IP Pools

You can release single-stack and dual-stack pools that are reserved at the site level.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.
 - Step 2** Choose the Global site or expand the hierarchy tree and choose the desired site.
 - Step 3** To release all the IP pools in bulk, do the following:
 - a) From the **Actions** drop-down list, choose **Release All**.
 - b) Click **Yes** in the **Warning** message.
 - c) At the prompt, click **Release**.
 - Step 4** To release only the desired IP pools, do the following:
 - a) Choose the desired IP pools and from the **Actions** drop-down list, click **Release Selected**.
 - b) At the prompt, click **Release**.
-

View IP Address Pools

This procedure shows how to view 10 or more IP address pools in table view and tree view.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.
 - Step 2** Select a site from the hierarchy in the left pane.
 - Step 3** Use the Toggle button to switch between the Table view and Tree view.
 - When the view contains 10 or more IP pools, by default the GUI displays the pools in table view.
 - When the view contains fewer than 10 IP pools, by default the GUI displays the pools in tree view.
- Note** Toggling between the table and tree map view is based on the pool count not on the user selection on the UI.
- Tree view applies to the Global pool as well as to the site pool.
- Step 4** The **IP Address Pools** table view displays list of IP address pools based on **Name**, **Type**, **IPv4 Subnet**, **IPv4 Used**, **IPv6 Subnet**, **IPv6 Used**, and **Actions**.

- Note**
- Hover your cursor over the **i** icon next to the **IPv4 Used** and **IPv6 Used**. A tooltip appears that displays more information about **IPv4 Used**, **IPv6 Used**, **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP address pool.
 - In the **IPv4** and **IPv6** columns, hover your cursor over the **i** icon next to the corresponding used percentage of **IPv4** and **IPv6** for a given IP address pool. A tooltip displays the percentage of **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP addresses.

Step 5 In the Table view, click the **IPv4 only** or **Dual-Stack** option in the **Subnet Type** area if you prefer to view only the **IPv4** or **Dual-Stack** address pools.

Step 6 In the Tree view, hover your cursor over the IP address pool that you are interested in, and click to view the slide-in pane which contains the following information:

- Subnet type of an IP address pool.
- Percentage of available IP addresses along with **Pool CIDR**, **Gateway**, **DHCP Server(s)**, and **DNS Server(s)** under the respective pool.
- Percentage of used IP addresses under the respective pool.

Step 7 In the **Used** area, click **Assigned** to view the list of assigned IP addresses to a device filtered based on **Device Name**, **IP Address**, and **Site**.

Step 8 Click **Unassignable** to view the list of unassigned IP addresses which cannot be assigned to a device filtered based on **Device Name**, **IP Address**, and **Site**.

Step 9 Click **Edit** to edit an IP address pool.


Step 10 Click **Release** to release an IP address pool.

- Note**
- In the side bar for a global pool, you can view the usage of a given pool across all the child pool.
 - Global and site IP address pool can have blocklisted IP addresses.
 - Subpools cannot have blocklisted IP addresses.
 - Cisco DNA Center rejects the IP address pool creation request of a CIDR address pool if it contains blocklisted IP addresses.
 - In the next free IP address pools request, Cisco DNA Center skips the blocklisted IP addresses to find the next IP address free pool.

Step 11 (Optional) In the side bar click **Export** to export the table data.

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 service models. After you create an 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.

-
- Step 1** Click the menu icon () and choose **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, enter a new service provider, or choose an existing one.
- Step 5** From the **Model** drop-down list, choose a class model: **4 class**, **5 class**, **6 class**, and **8 class**.
- For a description of these classes, see [Service Provider Profiles](#).
-

Configure Global Wireless Settings

Global wireless network settings include settings for Service Set Identifiers (SSIDs), wireless interfaces, RF, and sensors.






Note You can create a wireless sensor device profile for only Cisco Aironet 1800s Active Sensor devices.

Create SSIDs for an Enterprise Wireless Network

The following procedure describes how to configure SSIDs for an enterprise wireless network.



Note The SSIDs are created at the global level. The site, building, and floor inherit settings from the global level.

-
- Step 1** Click the menu icon () and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** In the left pane, select **Global**.
- Step 4** In the **SSID** table, from the  **Add**  drop-down icon, choose **Enterprise**.
- Step 5** In the **Wireless SSID** workflow, complete the **Basic Settings** setup:
- If the **Sensor** toggle button is available, ensure that it is disabled.
 - In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network.
 - For the **Wireless Option** setting, click one of the following radio buttons:
 - **Multi band operation (2.4 GHz, 5 GHz, 6GHz)**: The WLAN is created for 2.4 GHz, 5 GHz, and 6 GHz and band select is disabled.
 - **Multi band operation with band select**: The WLAN is created for 2.4 GHz, 5 GHz, and 6 GHz, and band select is enabled.
 - **5GHz only**: The WLAN is created for 5 GHz, and band select is disabled.
 - **2.4GHz only**: The WLAN is created for 2.4 GHz, and band select is disabled.

- **6GHz only**: The WLAN is created for 6 GHz, and band select is disabled.
- d) From the **Primary Traffic Type** drop-down list, choose one of the following options:
- **VoIP (Platinum)**: QoS on the wireless network is optimized for wireless voice and data traffic.
 - **Video (Gold)**: QoS on the wireless network is optimized for video traffic.
 - **Best Effort (Silver)**: QoS on the wireless network is optimized for wireless data traffic only.
 - **Non-real Time (Bronze)**: QoS on the wireless network is optimized for low-bandwidth usage.
- e) For the **SSID STATE** settings, click the toggle buttons to enable or disable the following settings:
- **Admin Status**: Use this toggle button to turn on or off the radios on the APs. When the **Admin Status** is disabled, the APs remain associated with the wireless controller and accessible, and the APs still require licenses.
 - **Broadcast SSID**: Use this toggle button to enable or disable the visibility of the SSID to all wireless clients within range.

Step 6

Complete the **Security Settings** setup:

- a) For **Level of Security**, choose the encryption and authentication type for the network. Note that the sites, buildings, and floors inherit settings from the Global hierarchy. You can override the level of security at the site, building, or floor level.
- **Enterprise**: You can configure both **WPA2** and **WPA3** security authentication by checking the respective check boxes. By default, the **WPA2** check box is enabled.
- Note** Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP).
- WPA3 is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher-grade security protocols for sensitive data networks.
- For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS Release 17.7 and later.
- **Personal**: If you choose **Personal**, enter the passphrase key in the **Pass Phrase** field. This key is used as the pairwise master key (PMK) between clients and the authentication server.

Note WPA3 Personal brings better protection to individual users by providing more robust password-based authentication, making the brute-force dictionary attack much more difficult and time-consuming.

For WPA2 Personal, you can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floors inherit the new settings. For information, see [Preshared Key Override, on page 22](#).

For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS Release 17.7 and later.

- **Open Secured:** From the **Assign Open SSID** drop-down list, choose an open SSID to redirect the clients to open secured SSID. The open secured policy provides the least security.

Note Fast Transition is not applicable for open-secured SSID.

Since open-secured SSID depends on open SSID, you must have enabled anchor on open SSID before enabling it on open-secured SSID.

- **Open:** The open policy provides no security. It allows any device to connect to the wireless network without any authentication.

- b) For **Authentication, Authorization, and Accounting Configuration**, click **Configure AAA** to add and configure the AAA servers for the enterprise wireless network SSID.

For more information, see [Configure AAA Server for an Enterprise Wireless Network](#).

- c) Check one or more following check boxes:

- **Fast Lane:** Check this check box to enable fastlane capabilities on the network.

Note By enabling fastlane, you can set the iOS devices to receive an optimized level of wireless connectivity and enhanced QoS.

- **Identity PSK** (for Personal Layer 2 Security): Check this check box to enable unique preshared keys that can be created for individuals or groups of users in the SSID.

- **MAC Filtering:** Check this check box to enable MAC-based access control or security on the wireless network.

Note When MAC filtering is enabled, only the MAC addresses that you add to the wireless LAN are allowed to join the network.

- **Deny RCM Clients:** Check this check box to deny clients with randomized MAC addresses.

- **Enable Posture:** Check this check box to enable posture assessment. The **Pre-Auth ACL List Name** drop-down list appears when you enable posture. Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients to access protected areas of a network.

- **Pre-Auth ACL List Name:** From the drop-down list, choose the ACL list name that you already created to map with the SSID.

Note AAA configuration is mandatory for posturing. Click **Configure AAA** to add AAA servers for the enterprise wireless network SSID.

d) Click **Next**.

Step 7

Complete the **Advance Settings** setup:

a) For **Fast Transition (802.11r)**:

- Choose **Adaptive**, **Enable**, or **Disable** mode.

Note 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

- Check the **Over the DS** check box to enable fast transition over a distributed system. By default, fast transition over a distributed system is disabled.

b) For **MFP Client Protection**, choose a setting—**Optional**, **Required**, or **Disabled**.

Note Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between APs and clients. MFP provides both infrastructure and client support.

By default, **Optional** is selected. If you choose **Required**, the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller, and if the client is also configured for WPA2 and supports CCXv5 MFP).

c) For **11K**:

- **Neighbor List**: Check this check box to configure all the 11k-capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

Note To facilitate roaming, a 11k-capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with the Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for next roam from the response frame.

- **Session Timeout**: Check this check box to set the maximum time for a client session to remain active before reauthorization.

Note By default, the **Session Timeout** is enabled with a timeout of 1800 seconds.

- **Client Exclusion**: Check this check box to set the client exclusion timer.

Note When a user fails to authenticate, the wireless controller excludes the client from connecting. The client is not allowed to connect to the network until the exclusion timer expires. By default, the **Client Exclusion** is enabled with a timeout of 180 seconds.

d) For **11v BSS Transition Support** setup:

- **BSS Max Idle Service**: Check this check box to set the idle period timer value. The idle period timer value is transmitted using the association and reassociation response frame from APs to the client.

Note The BSS Max idle period is the time frame during which an AP doesn't disassociate a client because of nonreceipt of frames from the connected client.

- **Client User Idle Timeout**: Check this check box to set the user idle timeout for a WLAN.

Note If the data sent by the client is more than the threshold quota specified as the user idle timeout, the client is considered to be active and the wireless controller begins another timeout period.

By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

- **Directed Multicast Service:** Check this check box to enable directed multicast service.

Note By default, **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer time and saves the battery power.

- e) For **Radius Client Profiling**, use this toggle button to enable or disable RADIUS profiling on a WLAN.

Note At least one AAA or PSN server is required to enable this feature.

- f) (Optional) For the **NAS-ID** setup:

- From the **NAS-ID Opt** drop-down list, choose the required type of network access server identifier (NAS ID).
- (Optional) To specify a custom script for the NAS ID, choose **Custom Option** from the **NAS-ID Opt** drop-down list and enter the custom script in the corresponding **Custom Script for Opt** field. You can enter up to 31 alphanumeric characters, special characters, and spaces for the custom script. Cisco DNA Center doesn't support the special characters ? " < and trailing spaces for the custom script.

Note Cisco DNA Center supports NAS ID with custom script only for Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.7 or later.

- (Optional) Click + to add another network access server identifier. You can add up to three NAS IDs.

Note Cisco DNA Center applies only one NAS ID for Cisco AireOS Controllers. You can overwrite the NAS ID at the site-level from the **Design > Network Settings > Wireless** window.

- g) Click **Next**.

Step 8 Complete the **Associate SSID to Profile** setup:

- a) From the left pane, select a profile and click **Associate Profile**.

If you don't have a profile, click **Add Profile** and configure the profile settings. For information, see [Create Network Profiles for Wireless](#)

- b) Click **Next**.

Step 9 Review the **Summary** settings. If changes are necessary, click **Edit**.

Step 10 Click **Save**.

The SSID is created.

Preshared Key Override


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

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > Wireless**.
- Step 2** In the left pane, choose the site, building, or floor to edit the PSK.
- Step 3** Under **Enterprise Wireless**, click the **Passphrase** field, and enter a new passphrase for the PSK SSID.
- Step 4** Click **Save**.
- A success message saying `Passphrase for the SSID(s) updated successfully` is displayed.
- Hover your cursor over the inherit icon (≡) next to the SSID to view the origin of this setting.
- Step 5** To reset the PSK override, check the check box of the PSK SSID on the site, building, or floor and click **Delete**. The PSK is reset to the global passphrase value.
-


Create Pre-Auth Access Control Lists

Using the Pre-Authentication ACL feature, you can create a pre-authentication ACL for web authentication to allow certain types of traffic before authentication is complete. This ACL is referenced in the access-accept of Cisco Identity Services Engine (ISE) and defines what traffic to be permitted and what traffic to be denied by the ACL. After ACLs are configured on the Cisco Wireless Controller, they can be applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU. You can configure both IPv4 and IPv6 ACLs.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** In the left pane, select **Global**.
- Step 4** Under the **Pre-Auth Access Control Lists** area, click **Add** to create a new pre-auth ACL.
- Step 5** In the **New Pre-Auth ACL** slide-in pane, configure the following:
- In the **Pre-Auth ACL List Name** field, enter a name for the ACL list.
 - In the **Pre-Auth ACL Name** field, enter a name for the pre-auth ACL.
 - Click the **IP Addresses** tab and choose the ACL type you are creating: **IPV4** or **IPV6**.
- Step 6** Click the **IP Addresses** tab and choose the ACL type you are creating: **IPV4** or **IPV6**.
- From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. These are the protocol options: **Any**, **TCP**, or **UDP**.
 - In the **Source Port** field, enter the source port number. The range is 0 to 65535. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.
 - In the **Source IP Address** field, enter the IP address and netmask of the source. If you are configuring an IPv6 ACL, enter the IPv6 address and prefix length of the source in the Source IP Address field.
 - From the **Source Subnet** drop-down list, choose a value for the source subnet.
 - In the **Destination Port**, enter the destination port number.

- In the **Destination IP Address**, enter the IP address and netmask of the destination. If you are configuring IPv6 ACL, enter the IPv6 address and prefix length of the destination.
- From the **Destination Subnet** drop-down list, choose a value for the destination subnet.
- You can add multiple rules by clicking  icon. You can add up to 256 rules.

Step 7 Click the **Walled Garden URLs** tab to add specific URLs to allowed list for web authentication of captive portal and walled garden. Authentication is not required to access the allowed list of URLs. When you try to access sites that are not in allowed list, you are redirected to the Login page.

- In the **URL** field, enter the URL and click  to add the URL to the allowed list for web authentication. You can add up to 32 URL entries.


Step 8 Click **Save**.

Step 9 Map the ACL with the SSID while creating SSIDs for enterprise wireless network.

Configure AAA Server for an Enterprise Wireless Network

Before you begin

- Make sure you have defined the AAA server under **System Settings > External Services > Authentication and Policy Servers** page.
- You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Step 1 Click the menu icon () and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 Ensure that **Global** is selected from the left pane.

Step 4 From the **SSID** table, in the **Action** column, click **Configure AAA** against an SSID for which you want to configure the AAA server.

The **Configure AAA Server** slide-in pane appears.

Step 5 From the **Server** drop-down list, you can either search for a server IP address by entering its name in the **Search** field or choose the AAA IP address.

- Note**
- The **Configure AAA** feature is not supported for Mobility Express devices.
 - Effective with Release 2.3.3.7, you must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Cisco DNA Center pushes the **aaa authentication dot1x default local** command to the wireless controller and the default method list that points to local authentication is mapped to the SSID.

Step 6 Click+ to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of enterprise wireless network for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches.

Step 7 From the **Additional Server** drop-down list, choose the server IP address.

Step 8 (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 9 Click **Configure**.

Note Cisco DNA Center allows you to override the set of AAA server configuration for SSID on the site level. For each set of overridden AAA settings per SSID, Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Cisco DNA Center creates the new WLAN profiles equals to the number of floors.

You must reprovision the device to override the AAA servers on the site level. See [Provision Devices](#).

Create SSIDs for a Guest Wireless Network

This procedure explains how to create SSIDs for a guest wireless network.

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

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, ensure that **Global** is selected.

Step 4 In the **SSID** table, from the **+Add** drop-down icon, choose **Guest**.

Step 5 In the **Wireless SSID** workflow, complete the **Basic Settings** setup:

- a) In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network.
- b) For the **Wireless Option** settings, click one of the following radio buttons:
 - **Multi band operation (2.4 GHz, 5 GHz, 6GHz)**: The WLAN is created for 2.4 GHz, 5 GHz, and 6 GHz and band select is disabled.
 - **Multi band operation with band select**: The WLAN is created for 2.4 GHz, 5 GHz, and 6 GHz, and band select is enabled.
 - **5GHz only**: The WLAN is created for 5 GHz, and band select is disabled.
 - **2.4GHz only**: The WLAN is created for 2.4 GHz, and band select is disabled.
 - **6GHz only**: The WLAN is created for 6 GHz, and band select is disabled.
- c) From the **Primary Traffic Type** drop-down list, choose one of the following options:
 - **VoIP (Platinum)**: QoS on the wireless network is optimized for wireless voice and data traffic.
 - **Video (Gold)**: QoS on the wireless network is optimized for video traffic.
 - **Best Effort (Silver)**: QoS on the wireless network is optimized for wireless data traffic only.
 - **Non-real Time (Bronze)**: QoS on the wireless network is optimized for low-bandwidth usage.

- d) For the **SSID STATE** settings, click the toggle buttons to enable or disable the following settings:
- **Admin Status:** Use this toggle button to turn on or off the radios on the APs. When the **Admin Status** is disabled, the APs remain associated with the wireless controller and accessible, and the APs still require licenses.
 - **Broadcast SSID:** Use this toggle button to enable or disable the visibility of the SSID to all wireless clients within range.

Step 6

Complete the **Security Settings** setup:

- a) For the **L2 Security** setting, choose the L2 encryption and authentication type:
- **Enterprise:** You can configure either the **WPA2** or the **WPA3** security authentication type by checking the respective check boxes. By default, the **WPA2** check box is enabled.

Note Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Fast transition is applicable for enterprise WPA2 SSID.

WPA3 security authentication is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher grade security protocols for sensitive data networks.

For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS Release 17.7 and later.
 - **Personal:** You can configure both **WPA2** and **WPA3** or configure **WPA2** and **WPA3** individually by checking the respective check boxes.

Note WPA3-personal security authentication brings better protection to individual users by providing more robust password-based authentication. This makes the brute-force dictionary attack much more difficult and time-consuming.

Enter the passphrase key in the **Pass Phrase** field. This key is used as the pairwise master key (PMK) between the clients and the authentication server.

For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS Release 17.7 and later.
 - **Open Secured:** From the **Assign Open SSID** drop-down list, choose an open SSID to associate with the open SSID. Associating secures the open SSID. You must have an open SSID created before associating it with the open secured SSID.

Note Fast Transition is not applicable for open-secured SSID.

Since open-secured SSID depends on open SSID, you must have enabled anchor on open SSID before enabling it on open-secured SSID.
 - **Open:** The open policy provides no security. It allows any device to connect to the wireless network without any authentication.

b) For the **L3 Security** setting, choose the L3 encryption and authentication type:

- **Web Policy:** Provides a higher level of L3 security.

For **Authentication Server**, configure these authentication server settings:

Authentication Server Type	Description
<p>Central Web Authentication</p>	<p>Use AAA server for central web authentication (CWA).</p> <p>(Optional) If you choose Cisco ISE for CWA, from the What kind of portal are you creating today? drop-down list, choose the type of portal you want to create:</p> <ul style="list-style-type: none"> • 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 providing any credentials. <p>(Optional) If you choose Cisco ISE for CWA, from the Where will your guests redirect after successful authentication? drop-down list, choose where you want to redirect the guests after successful authentication:</p> <ul style="list-style-type: none"> • Success Page: The guests are redirected to an Authentication Success window. • 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 field.
<ul style="list-style-type: none"> • Web Authentication Internal • Web Authentication External 	<p>Web authentication or Web Auth is a Layer 3 security method that allows a client to pass Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) traffic only until they have passed some form of authentication.</p> <p>For web authentication internal, the client is redirected to a page that is constructed by the Cisco Wireless Controller.</p> <p>For web authentication external, the client is redirected to the specified URL. Enter a redirect URL in the Web Auth Url field.</p>
<ul style="list-style-type: none"> • Web Passthrough Internal • Web Passthrough External 	<p>Web passthrough is a solution that is used for guest access and requires no authentication credentials. In web passthrough authentication, wireless users are redirected to the usage-policy page when they use the internet for the first time. After accepting the policy, users are allowed to use the internet.</p>

- **Open:** There is no security at the Layer 3 level and any device can connect to the SSID.

- c) If you choose **Web Authentication Internal**, **Web Authentication External**, **Web Passthrough Internal**, or **Web Passthrough External**, for **Timeout Settings for sleeping clients** settings, choose the authentication for sleeping clients:
- **Always authenticate**: Enables authentication for sleeping clients.
 - **Authenticate after**: Enter the duration for which sleeping clients are to be remembered before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, and the default duration is 720 minutes.

Note Clients with guest access and web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before reauthentication becomes necessary. The valid range is from 10 minutes to 43200 minutes; the default is 720 minutes. You can configure the duration on a WLAN and on a user group policy that is mapped to the WLAN. The sleeping timer becomes effective after the idle timeout. If the client timeout is less than the time configured on the sleeping timer of the WLAN, the lifetime of the client is used as the sleeping time.

- d) For **Authentication, Authorization, and Accounting Configuration** settings, click **Configure AAA** to add and configure the AAA servers for the guest wireless network SSID.

For more information, see [Configure AAA Server for a Guest Wireless Network](#).

- e) Check one or more of the following check boxes:

- **Fast Lane**: Check this check box to enable fastlane capabilities on the network.

Note By enabling fastlane, you can configure the iOS devices to receive an optimized level of wireless connectivity and enhanced QoS.

- **Identity PSK** (for Personal L2 Security): Check this check box to enable unique preshared keys that can be created for individuals or groups of users in the SSID.

- **MAC Filtering**: Check this check box to enable MAC-based access control or security in the wireless network.

Note When MAC filtering is enabled, only the MAC addresses that you add to the wireless LAN are allowed to join the network.

- **Deny RCM Clients**: Check this check box to deny clients with randomized MAC addresses.

- f) Click **Next**.

Step 7

Complete the **Advance Settings** step:

- a) For the **Fast Transition (802.11r)** settings:

- Choose **Adaptive**, **Enable**, or **Disable** mode.

Note 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

- Check the **Over the DS** check box to enable fast transition over a distributed system. By default, fast transition over a distributed system is disabled.

- b) For the **MFP Client Protection** setting, choose **Optional**, **Required**, or **Disabled**.

Note Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between APs and clients. MFP provides both infrastructure and client support.

By default, **Optional** is selected. If you choose **Required**, the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller, and if the client is also configured for WPA2 and supports CCXv5 MFP).

c) For the **11K** settings:

- **Neighbor List:** Check this check box for all the 11k-capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

Note To facilitate roaming, a 11k-capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with the Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for next roam from the response frame.

- **Session Timeout:** Check this check box to set the maximum time for a client session to remain active before reauthorization.

Note By default, the **Session Timeout** is enabled with a timeout of 1800 seconds.

- **Client Exclusion:** Check this check box to set the client exclusion timer.

Note When a user fails to authenticate, the wireless controller excludes the client from connecting. The client is not allowed to connect to the network until the exclusion timer expires. By default, the **Client Exclusion** is enabled with a timeout of 180 seconds.

d) For the **11v BSS Transition Support** settings:

- **BSS Max Idle Service:** Check this check box to set the idle period timer value. The idle period timer value is transmitted using the association and reassociation response frame from the APs to the client.

Note The BSS Max idle period is the timeframe during which an AP doesn't disassociate a client because of nonreceipt of frames from the connected client.

- **Client User Idle Timeout:** Check this check box to set the user idle timeout period for a WLAN.

Note If the data sent by the client is more than the threshold quota specified as the user idle timeout period, the client is considered to be active and the wireless controller refreshes for another timeout period.

By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

- **Directed Multicast Service:** Check this check box to enable directed multicast service.

Note By default, **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer time and saves the battery power.

e) (Optional) For the **NAS-ID** setup:

- From the **NAS-ID Opt** drop-down list, choose the required type of network access server identifier (NAS ID).

- (Optional) To specify a custom script for the NAS ID, choose **Custom Option** from the **NAS-ID Opt** drop-down list and enter the custom script in the corresponding **Custom Script for Opt** field. You can enter up to 31 alphanumeric characters, special characters, and spaces for the custom script. Cisco DNA Center doesn't support the special characters ? " < and trailing spaces for the custom script.

Note Cisco DNA Center supports NAS ID with custom script only for Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.7 or later.

- (Optional) Click + to add another network access server identifier. You can add up to three NAS IDs.

Note Cisco DNA Center applies only one NAS ID for Cisco AireOS Controllers. You can overwrite the NAS ID at the site-level from the **Design > Network Settings > Wireless** window.

f) Click **Next**.

Step 8


Complete the **Associate SSID to Profile** step:

- Click a profile from the left pane.
- If you don't have a profile, click **Add Profile** and then configure the profile settings:


- **Profile Name:** Enter a name for the wireless profile.
- **Fabric:** Specify whether the SSID is fabric or nonfabric.

Note A fabric SSID is a wireless network, which is a part of Software Defined-Access (SD-Access). SD-Access is a solution that automates and simplifies configuration, policy, and troubleshooting of wired and wireless networks. With fabric SSID, it is mandatory to have SD-Access. Nonfabric is a traditional wireless network that doesn't require SD-Access.

For a nonfabric SSID, choose the following:

- **Interface:** From the **Interface Management** drop-down list, choose an interface or click the plus icon  to add a new wireless interface.

Note This is the VLAN ID that is associated with the wireless interface.

- **VLAN Group:** From the **VLAN Group Name** drop-down list, choose a VLAN group or click the plus icon  to add a VLAN group.

- **Do you need Anchor for this SSID?:** Choose whether the SSID will be an anchor or not.
- **Flex Connect Local Switching:** Check this check box to enable local switching for the WLAN. When you enable local switching, any FlexConnect AP that advertises this WLAN is able to locally switch data packets.

Note If you have enabled **Flex Connect Local Switching** for an SSID, then all the APs on that particular floor where the network profile is mapped will switch to FlexConnect mode.

- Click **Associate Profile** to choose the profile.
- Click **Next**.

Step 9

Review the **Summary** step. If any changes are necessary, click **Edit**.

Step 10

To save the SSID settings, click **Save**.

The SSID is created.

Configure AAA Server for a Guest Wireless Network

Before you begin

- Make sure you have defined the AAA server under the **System Settings > External Services > Authentication and Policy Servers** window.
 - You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.
-

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

Step 2 Click the **Wireless** tab.

Step 3 Ensure that **Global** is selected from the left pane.

Step 4 From the **SSID** table, in the **Action** column, click **Configure AAA** of SSID for which you want to configure the AAA server.

Step 5 From the **Server** drop-down list of the **Configure AAA Server** slide-in pane, you can either search for a AAA IP address by entering its name in the **Search** field or choose AAA IP address.

Note

- You must configure at least one AAA or Policy Service Node (PSN) server for Central Web Authentication (CWA) SSIDs of guest wireless network.
- Cisco DNA Center allows you to map AAA server in any combination of identity services engine PSNs and third-party AAA IPs.
- In the **Server** drop-down list, the **AAA** IP addresses and the **PSN** IP addresses are grouped in the corresponding sections.
- The **Configure AAA** feature is not supported for Mobility Express (ME) devices.
- Effective with Release 2.3.3.7, you must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Cisco DNA Center pushes the **aaa authentication dot1x default local** command to the wireless controller and the default method list that points to local authentication is mapped to the SSID.

Step 6 Click+ to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of guest wireless network for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches.

Step 7 From the **Additional Server** drop-down list, choose the server IP address.

Step 8 (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 9 Click **Configure**.

Note Cisco DNA Center allows you to override the set of AAA server configuration for SSID on the site level. For each set of overridden AAA settings per SSID, Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Cisco DNA Center creates the new WLAN profiles equals to the number of floors.

You must reprovision the device to override the AAA servers on the site level. See [Provision Devices](#).

Configure 802.1x Authentication Settings for APs

You can configure authentication settings to securely onboard APs using PnP. Based on the authentication settings configured at the global or site-level hierarchy in Cisco DNA Center, PnP pushes the 802.1x (Dot1x) supplicant and certificates when claiming an AP. The AP authenticates with Cisco ISE using the 802.1x supplicant.

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

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, ensure that **Global** is selected.

Note The 802.1x authentication, which is created at the global level, can be overridden at the site level.

Step 4 In the **Access Points Authentication for Plug n Play (PnP)** area, complete the following:

a) Choose an authentication method:

- **NO-AUTH:** By default, this authentication method is selected.
- **EAP-TLS:** Extensible Authentication Protocol-Transport Level Security (EAP-TLS) is an authentication method designed to mitigate several weaknesses of EAP. EAP-TLS provides many of the benefits that PEAP provides but differs from it in the lack of support for legacy authentication methods.
- **EAP-PEAP:** EAP-Protected Extensible Authentication Protocol (EAP-PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol.

If you select **EAP-PEAP**, enter the user name and password. A certificate is generated and applied during the PnP claim process.

- **EAP-FAST:** EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) is an authentication protocol that provides mutual authentication and uses a shared secret to establish a tunnel. The tunnel is used to protect weak authentication methods that are based on passwords. The shared secret, referred to as a Protected Access Credentials (PAC) key, is used to mutually authenticate the client and server while securing the tunnel.

If you select **EAP-FAST**, enter the user name and password. A certificate is generated and applied during the PnP claim process.

b) Enter the **Username** and **Password**.

c) Click **Save**.

Create a Wireless Interface

You can create wireless interfaces only in nonfabric deployments.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
 - Step 2** Click the **Wireless** tab.
 - Step 3** Ensure that **Global** is selected from the left pane.
 - Step 4** From the **Wireless Interfaces** table, click **+Add**.
 - Step 5** Configure the wireless interface settings in the **Create a Wireless Interface** slide-in pane:
 - a) In the **Interface Name** field, enter the dynamic interface name.
 - b) In the **VLAN ID** field, enter the VLAN ID for the interface.
 - Step 6** Click **Save**.

The wireless interface is created and appears in the **Wireless Interfaces** table.
-

Design and Provision Interface/VLAN Groups to Nonfabric Deployments

Cisco DNA Center allows you to configure networks with multiple broadcast domains through different VLANs. When the same set of APs broadcast the same WLAN, the broadcast domains are controlled through multiple VLANs on the same WLAN through interface groups.

Cisco DNA Center interface groups are logical groups of interfaces that facilitate user configuration, where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface can be part of multiple interface groups. A WLAN can be associated with an interface or interface group.



Note The interface group name and the interface name cannot be the same.

The Cisco DNA Center VLAN group feature maps a WLAN to a single VLAN or multiple VLANs using VLAN groups. VLAN groups can be associated to policy profiles.

The following procedure explains how to design and provision the interface or VLAN groups for nonfabric deployments.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
 - Step 2** Click the **Wireless** tab.
 - Step 3** For the **VLAN Group** table, click **Add**.

The **Add VLAN Group** slide-in pane appears.
 - Step 4** Enter a valid **VLAN Group Name**, select single or multiple interfaces from the list, and click **Save**.
 - Note** If you select more than 15 interfaces, the selected interfaces might not be displayed correctly onscreen.
 - Step 5** In the **Edit Network Profile** page, the VLAN group is associated with the SSID.

For information on how to create an SSID, see [Create SSIDs for an Enterprise Wireless Network](#).

- Step 6** To add more SSIDs to the VLAN group, click **Add SSID**.
- Step 7** Choose **Interface** or **VLAN** group.
- Step 8** Click the add icon to create a new interface or VLAN group.
- Note** Interface or VLAN group is not applicable for FlexConnect local switching.
- Step 9** Click **Save**.
- Step 10** In **Configure Interface and VLAN**, you can view the list of interface names, interface groups names, and other parameters required to configure the interface and VLAN.
- Note** An interface group cannot contain more than 64 interfaces.
- Step 11** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 12** Select the device.
- Step 13** From the **Actions** drop-down menu, choose **Provision > Provision Device**.
- Step 14** Review the details in the **Assign Site, Configuration, Model Configuration, Advanced Configuration, and Summary** screens. From each screen, click **Next** to advance to the next screen.
- Step 15** Click **Deploy**.
- The **Provision Device** dialog box appears.
- Step 16** Choose **Now** and click **Apply**.
- The message **Task Scheduled view status in Tasks** appears.

Create a Wireless Radio Frequency Profile

You can either use the default radio frequency profiles (LOW, TYPICAL, HIGH), or create custom radio frequency profiles.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the **Wireless Radio Frequency Profile** table, click **Add**.
- The **Wireless Radio Frequency Profile** window appears.
- Step 4** In the **Profile Name** field, enter the RF profile name.
- Step 5** Configure the following for the **2.4 GHz** radio type:
- a. Ensure that the **2.4 GHz** toggle button is enabled.

- Note**
- For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **2.4 GHz** toggle button, Cisco DNA Center disables the Admin status of the **2.4 GHz** RF profile.
 - For Cisco AireOS Wireless Controller, if you disable the **2.4 GHz** toggle button, Cisco DNA Center disables the Admin status of the respective radios on all APs that use this RF profile. We recommend that you disable the Admin status using the **Configure Access Points** workflow. For more information, see [Configure AP Workflow](#).
 - For Cisco AireOS Wireless Controller, when you disable the Admin status for the 2.4-GHz band on the RF profile, Cisco DNA Center changes the dual band (XOR) radio on the APs using that RF profile to manual 5-GHz mode. If you enable the Admin status later and reprovision the AP, Cisco DNA Center changes the radio to automatic mode enabling the usage of 2.4-GHz and 5-GHz bands, and monitor mode. So, if you want to disable the Admin status for the 2.4-GHz band on XOR-capable APs, we recommend that you disable the Admin status of the XOR radio using the **Configure Access Points** workflow. The Admin status configured using the **Configure Access Points** workflow isn't overwritten when the wireless controller or APs are reprovisioned. For more information, see [Configure AP Workflow](#).

- b. Under **Parent Profile**, select **High**, **Medium (Typical)**, **Low**, or **Custom**. (The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates the 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**.) Note that a new RF profile is created only for the select custom profiles.

- Note** Low, Medium (Typical), and High are the default RF profiles. If you select a default RF profile, the respective RF profile on the device is used and the new RF profile is not created on wireless controller.

- c. **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**. Alternatively, check the individual check boxes next to the channel numbers.
- Click **Show Advanced** to select the 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 next to the individual channel numbers. The channel numbers that are available for B profile are **2**, **3**, **4**, **5**, **7**, **8**, **9**, **10**, **12**, **13**, and **14**.

- Note** For Cisco AireOS Wireless Controller, Cisco DNA Center automatically configures the selected DCA channels in the global RRM DCA channel list.

Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

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

- e. Under **Tx Power Configuration**, set the power level and power threshold for an AP.

- **Power Level:** To determine whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the

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

- **Power Threshold:** Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm to 80 dBm and the default threshold is -70 dBm.
- **RX SOP:** Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High**, **Medium**, **Low**, or **Auto** threshold values for each 802.11 band.

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

- Ensure that the **5 GHz** toggle button is enabled.

Note

- For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **5 GHz** toggle button, Cisco DNA Center disables the Admin status of the **5 GHz** RF profile.
- For Cisco AireOS Wireless Controller, if you disable the **5 GHz** toggle button, Cisco DNA Center disables the Admin status of the respective radios on all APs that use this RF profile. We recommend that you disable the admin status using the **Configure Access Points** workflow. For more information, see [Configure AP Workflow](#).
- For Cisco AireOS Wireless Controller, when you disable the Admin status for the 5-GHz band on the RF profile, Cisco DNA Center changes the XOR radio on the APs using that RF profile to manual 2.4-GHz mode. If you enable the Admin status later and reprovision the AP, Cisco DNA Center changes the radio to automatic mode enabling the usage of 2.4-GHz and 5-GHz bands, and monitor mode. So, if you want to disable the Admin status for the 5-GHz band on XOR-capable APs, we recommend that you disable the Admin status of the XOR radio using the **Configure Access Points** workflow. The admin status configured using the **Configure Access Points** workflow isn't overwritten when the wireless controller or APs are reprovisioned. For more information, see [Configure AP Workflow](#).

- From the **Parent Profile** drop-down list, choose **High**, **Medium (Typical)**, **Low**, or **Custom**. (The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates the configurations available in the device for 2.4 GHz. If you change any settings in the populated **Data Rate** and **Tx Configuration** fields, the **Parent Profile** automatically changes to **Custom**.) Note that a new RF profile is created only for select custom profiles.

Note

Low, **Medium (Typical)**, and **High** are the default RF profiles. If you select a default RF profile, the respective RF profile that is already present in the device is used and the new RF profile is not created on wireless controller.

- From the **Channel Width** drop-down list, choose one of the channel bandwidth options: **Best**, **20 MHz**, **40 MHz**, **80 MHz**, or **160 MHz**.
- Set the **DCA Channel** to manage channel assignments:

Note For Cisco AireOS Wireless Controller, Cisco DNA Center automatically configures the selected DCA channels in the global RRM DCA channel list.

Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- **UNII-1 36-48:** The channels available for UNII-1 band are **36, 40, 44, and 48**. Check the **UNII-1 36-48** check box to include all channels, or check an individual check box.
 - **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 an individual check box.
 - **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 an individual check box.
- e. Use the **Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **6, 9, 12, 18, 24, 36, 48, and 54**.
- f. Under **Tx Power Configuration**, set the power level and power threshold for an AP.
- **Power Level:** Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 to 30 dBm and the default is -10 dBm.
 - **Power Threshold:** Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm to 80 dBm and the default threshold is -70 dBm.
 - **RX SOP:** Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an AP's radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High, Medium, Low, or Auto** threshold values for each 802.11 band.

Step 7

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

- a. Ensure that the **6 GHz** toggle button is enabled.

Note For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **6 GHz** toggle button, Cisco DNA Center disables the Admin status of the **6 GHz** RF profile.

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

- Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.
- Click **Show Advanced** to select the remaining DCA channel numbers.
 - **UNII-5 1-93**
 - **UNII-6 97-113**
 - **UNII-7 117-185**

- **UNII-8 189-233**

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **6, 9, 12, 18, 24, 36, 48, and 54**.
- In the **Mandatory Data Rates** area, check the check box next to the individual data rates. You can choose up to two data rates. The available data rates are **6, 9, 12, 18, 24, 36, 48, and 54**.
- Under **Tx Power Configuration**, set the power level and power threshold for an AP.
 - **Power Level:** Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 to 30 dBm and the default is -10 dBm.
 - **Power Threshold:** Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm to 80 dBm and the default threshold is -70 dBm.
 - **RX SOP:** Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an AP's radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High, Medium, Low, or Auto** threshold values for each 802.11 band.

Step 8 Click **Save**.

Step 9 To mark a profile as the default RF profile, check the **Profile Name** check box and click **Mark Default**.

Step 10 In the **Warning** window, click **OK**.

What to do next

You must provision the APs to apply the RF profile on the device. For more information, see [Provision a Cisco AP—Day 1 AP Provisioning](#).

Edit or Delete a Basic Radio Frequency Profile

The following procedure describes how to edit or delete a basic RF profile.

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

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, click the **Global** site.

Step 4 In the **Wireless Radio Frequency Profile** area, click the **Basic RF Profile** tab.

Note The **Basic RF Profile** table lists the number of created basic RF profiles based on **Profile Name**, **Type**, **2.4 GHz Data Rates**, **5 GHz Data Rates**, **6 GHz Data Rates**, **Channel Width**, and **Profile Type**.

Step 5 Check the check box next to the basic profile name that you want to edit.

Step 6 From the **Action** drop-down list, choose **Edit/View**.

Note You can edit one basic RF profile at a time.

Step 7 In the **Edit Wireless Radio Frequency Profile** window, configure the basic RF profile settings. For more information, see [Create a Wireless Radio Frequency Profile, on page 34](#).

Step 8 Click **Save**.

Step 9 To delete a basic RF profile, check the check box next to the basic RF profile name.

Step 10 From the **Action** drop-down list, choose **Delete** and then click **Yes**.

Step 11 To mark a basic RF profile as the default, check the check box next to a basic RF profile name.

Step 12 From the **Action** drop-down list, choose **Mark Default** and then click **Yes**.

What to do next

If you update an RF profile that is already provisioned on a wireless controller and AP, you must reprovision either the wireless controller or AP. Wireless controller reprovision also pushes the RF profiles updates to the devices and reprovisioning the AP is not necessary. For more information about provisioning a wireless controller, see [Provision a Cisco AireOS Controller](#) and [Provision a Cisco Catalyst 9800 Series Wireless Controller](#).

Create an AI Radio Frequency Profile

The following procedure describes how to create an artificial intelligence radio frequency profile for your building.

Before you begin

- You must enable Cisco AI Network Analytics under the system settings. For more information, see **Configure Cisco AI Network Analytics Data Collection** in [Cisco DNA Center Administrator Guide](#).
- You must enable **AI Enhanced RRM** under **Cisco AI Analytics** in the system settings. Click the menu icon (☰) and choose **System > Settings > External Services**.

In the **Cisco AI Analytics** window, under the **AI ENHANCED RRM** area, click the toggle button to enable the AI-enhanced RRM.

- Cisco AI RF profiles are supported only on Cisco Catalyst 9800 Series Wireless Controllers and Cisco IOS-XE 17.7.1 or later.
- To perform the following task, you must be a **Super Admin** or **Network Admin**.

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

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, click the **Global** site.

Step 4 In the **Wireless Radio Frequency Profile** area, from the **Add** drop-down list, choose **AI RF Profile**.

The **Create AI Radio Frequency Profile** window appears.

Step 5 In the **Profile Name** field, enter the RF profile name.

Step 6 Expand **Basic Settings**.

Step 7 In the **Radio Frequency Settings** area, check the **2.4 GHz** or **5 GHz** check box.

The radio frequencies are checked by default. If you uncheck a radio frequency, Cisco DNA Center disables the Admin status of the corresponding RF profile.

Step 8 In the **Busy Hours** area, define the start and end time of the site time zone.

Note Busy hours are dependent upon the timezone of building. You must configure a timezone under network settings for the respective building.

Step 9 In the **Busy Hour Sensitivity** area, click the **Low**, **Medium**, or **High** radio button to define the threshold of Radio Resource Management (RRM) sensitivity for the busy hours interval.

Step 10 In the **Enable RF Settings** area, click the toggle buttons under the **2.4 GHz** or **5 GHz** columns to enable or disable the radio band for the respective RF setting.

The supported RF settings are:

- **Flexible Radio Assignment (FRA)**: FRA optimizes the radio coverage per band and determines the best role assignment for redundant radios.
- **Dynamic Channel Assignment (DCA)**: DCA dynamically manages channel assignment for an RF group and evaluates the assignments on a per-AP radio basis.
- **Transmit Power Control (TPC)**: TPC manages and transmits power for APs. It also maximizes the SNR during the reduction in interference.
- **Dynamic Bandwidth Selection (DBS)**: DBS monitors and adjusts the channel width to balance the performance and interference.

- Note**
- When you disable the 2.4-GHz radio band for FRA, it automatically disables the 5-GHz radio band for FRA, and vice versa.
 - When you disable the 5-GHz radio band for DCA, it disables the 2.4-GHz radio band for FRA and the 5-GHz radio band for FRA and DBS.
 - You can individually enable the 2.4-GHz radio band for DCA and TPC; and the 5-GHz radio band for DCA, TPC, and DBS.

Step 11 Expand **Advanced** and click the **2.4 GHz** toggle button.

- a. In the **DCA Channel** area, check the **Select All** check box to select DCA channels **1**, **6**, and **11**. Alternatively, check the individual check boxes next to the channel numbers.
- b. In the **Advanced Options** area, check the **Select All** check box to select all the DCA channels.
- c. Click **Show Advanced** to select the remaining channel numbers.
- d. Check the check box next to the individual channel numbers. The channel numbers that are available for the profile are **2**, **3**, **4**, **5**, **7**, **8**, **9**, **10**, **12**, **13**, and **14**.

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- e. Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an AP and a client. The available data rates are **1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54**.
- f. In the **Mandatory Data Rates** area, check the check box next to the individual data rates. You can choose up to two data rates. The available data rates are **1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54**.
- g. Check the **Enable 802.11b data rates** check box to enable the 802.11b data rates. This action also enables the 802.11b supported data rate check box in the **Mandatory Data Rates** area.
- h. In the **Tx Power Configuration** area, set the following:
 - **Power Level**: Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference.
 - **Power Threshold**: Is the cutoff signal level used by RRM to determine whether to reduce the power of an AP.
 - **RX SOP**: Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet.
- i. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 to 30 dBm and the default is -10 dBm.
- j. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm to 80 dBm and the default threshold is -70 dBm.
- k. From the **RX SOP** drop-down list, choose **High, Medium, Low, or Auto** threshold values for each 802.11 band.

Step 12 In the **Advanced** area, click the **5 GHz** toggle button.

- a. Use the **DBS Max Width** slider to set the channel width of the AI RF profile.
The available channel width options are **20 MHz, 40 MHz, 80 MHz, or 160 MHz**.
The **Auto Channels Logic** area displays the color-coded channel logics for the channel widths.
You can select **DBS Max Width** only when DBS is enabled.
When you disable the DBS, Cisco DNA Center allows you to select channel width.
- b. Set the **DCA channels** to manage the following channel assignments:
 - **UNII-1 36-48**: The channels available for UNII-1band are **36, 40, 44, and 48**.
 - **UNII-2 52-144**: The channels available for UNII-2band are **52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, and 144**.
 - **UNII-3 149-165**: The channels available for UNII-3 band are **149, 153, 157, 161, and 165**.
- c. Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.
- d. Click **Show Advanced** to select the remaining DCA channel numbers.

- e. Check the **UNII-1 36-48** check box to include all channels, or check an individual check box.
 - f. Check the **UNII-2 52-144** check box to include all channels, or check an individual check box.
 - g. Check the **UNII-3 149-165** check box to include all channels, or check an individual check box.
- Note** Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.
- h. Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an AP and a client. The available data rates are **1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54**.
 - i. In the **Tx Power Configuration** area, set the **Power Level**, **Power Threshold**, and **RX SOP**.
 - j. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 to 30 dBm and the default is -10 dBm.
 - k. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from **-50 dBm to 80 dBm** and the default threshold is -70 dBm.
 - l. From the **RX SOP** drop-down list, choose **High**, **Medium**, **Low**, or **Auto** threshold values.

Step 13 Click **Save**.

What to do next

You must provision the APs to apply the RF profile settings on the device. For more information, see [Provision a Cisco AP—Day 1 AP Provisioning](#).

Edit and Delete an AI Radio Frequency Profile

The following procedure describes how to edit or delete an AI RF profile.

Before you begin

- Cisco AI RF profiles are supported only on Cisco Catalyst 9800 Series Wireless Controllers and Cisco IOS-XE 17.7.1 or later.
- To perform the following task, you must be a **Super Admin** or **Network Admin**.

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

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, click the **Global** site.

Step 4 In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.

The **AI RF Profile** table lists the number of created AI RF profiles based on **Profile Name**, **Busy Hours**, **Busy Hour Sensitivity**, **FRA**, **DCA**, **DBS**, **TPC**, and **Mapped Buildings**.

Step 5 Check the check box next to the AI RF profile that you want to edit.

You can edit one AI RF profile at a time.

- Step 6** Click **Edit/View**.
- Step 7** In the **Edit AI RF Profile** window, configure the AI RF profile settings. For more information, see [Create an AI Radio Frequency Profile, on page 39](#).
- Step 8** Click **Save**.
- Step 9** To delete an AI RF profile, check the check box next to the AI RF profile that you want to delete.
- Step 10** Click **Delete** and then click **Yes**.

Note Cisco DNA Center does not allow you to delete an AI RF Profile which is already assigned to a building.

What to do next

If you update an RF profile that is already provisioned on a wireless controller and AP, you must reprovision either the wireless controller or AP. Wireless controller reprovision also pushes the RF profiles updates to the devices and reprovisioning the AP is not necessary. For more information about provisioning a wireless controller, see [Provision a Cisco Catalyst 9800 Series Wireless Controller](#).

Configure AI Radio Frequency Profile

The following procedure describes how to assign an AI RF profile to a building.

Before you begin

- Cisco AI RF profiles are supported only on Cisco Catalyst 9800 Series Wireless Controllers and Cisco IOS-XE 17.7.1 or later.
- To perform the following task, you must be a **Super Admin** or **Network Admin**.

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure AI RF Profile**.
- Step 2** In the **Assign AI RF Profiles** window, click **Let's Do it** to go directly to the workflow.
- Step 3** The **Configure AI RF Profile** window appears.
- In the **Task Name** field, enter task name.
- Step 4** In the **Select Locations to Assign AI RF Profiles** window, select the locations where you want to assign the AI-enabled RF profiles. You can either search for a site by entering its name in the **Find Hierarchy** field, or expand **Global** and choose the sites.
- The **Site selection summary** table lists the sites based on the site selection in the site hierarchy and displays the **Selected Location** and **Impacted Location** of the selected sites.
- **Selected Locations:** A location that is being enabled for AI RF profile.
 - **Impacted Locations:** A location that is being partially managed by the same wireless controller of selected location.

Note When a controller manages more than one building and if you enable the AI RF profile only on one building, Cisco DNA Center automatically enables other building with same AI RF profile.

For example, if two controllers manage three buildings and when you enable AI RF profile on one building, Cisco DNA Center automatically enables other two buildings with same AI RF profile.

Step 5 In the **Select AI RF Profiles to assign** window, the **Building** table lists AI RF profiles based on **Location**, **Floors**, **Current RF Profiles**, and **Replace with AI RF Profiles**.

- a) In the **Building** table, check the check box next to a location to choose an AI RF profile.
- b) Based on the location, choose an AI-enabled RF profile from the drop-down list under **Replace with AI RF Profiles** to replace with the current AI RF profile.

Note If the AI RF profile is not created, click the three dots under the **Action** column to create a new RF profile, or copy the current RF profile and AI settings.

You can also create an AI RF profile from the **Create a new AI RF Profile to apply** link in the **Select AI RF Profiles to assign** window. For more information, see [Create an AI Radio Frequency Profile, on page 39](#).


Step 6 In the **Details of selected AI RF Profile** window, review the **AI Settings**, **Common Settings**, and **Assignment** details of the AI-enabled RF profiles.

Note AI-enhanced RRM computation occurs every 30 minutes. RRM decisions are updated and pushed to devices after the computation.

Step 7 In the **Summary** window, review the **Task Details**, **Select Locations to Assign AI RF Profiles**, and **Select AI RF Profiles to assign**.

Step 8 In the **Deploy the AI RF Profiles** window, click **Now** to deploy the AI RF profile immediately. Click **Later** to schedule the deployment for a later time.

Step 9 Click **Continue**.
The **Done! AI RF Profiles Assigned** window appears.

Step 10 Click the menu icon () and choose **Activities > Tasks**.

Step 11 In the **Tasks** window, click the task link.

A slide-in pane displays the **Assigned Building(s)**, **Selected AI RF Profile**, and **Provision Details**.

Assign a Location to an Existing AI RF Profile

The following procedure describes how to assign a location to an existing AI RF profile.

Before you begin

- Cisco AI RF profiles are supported only on Cisco Catalyst 9800 Series Wireless Controllers and Cisco IOS-XE 17.7.1 or later.
- To perform the following task, you must be a **Super Admin** or **Network Admin**.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** In the left pane, click the **Global** site.
- Step 4** In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab. The **AI RF Profile** table lists the number of created AI RF profiles.
- Step 5** Click the three dots under the **Action** column for an AI RF profile.
- Step 6** From the drop-down list, choose **Assign Location**.
The **Manage Location Assignment** window appears.
- Step 7** You can either search for a site by entering its name in the **Search** field, or expand **All Sites** to choose the sites.
- Note**
- The site hierarchy shows the AI-enabled locations.
 - Sites or buildings that are not eligible for the AI profile are disabled.
 - You cannot select a floor under a building. When you select a building for an AI-enabled RF profile, the floors underneath are assigned automatically.
- If the same wireless controller manages other buildings, the **Confirm Impacted Sites** window appears.
- Step 8** Review the confirmation and click **Confirm** to assign the chosen sites to the AI-enabled RF profile.
- Step 9** Click **Assign**.
A **Download a Backup of Current RF Settings** window appears that allows you to download the backup of the RF settings across the selected buildings.
- Step 10** (Optional) Click the backup link to download a .csv file to your local machine.
- Step 11** Click **Confirm**.
- Step 12** In the subsequent confirmation window, click **Confirm**.
In the **AI RF Profile** table, the locations assigned to the AI RF profile are displayed under the **Mapped Buildings** column.
-

What to do next

Provision Devices of an AI RF Profile-Enabled Building

The following procedure describes how to provision devices across the locations to deploy the AI RF profile.

1. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
In the **Inventory** window, the **Device** table lists the discovered AI RF profile associated devices.
2. Check the check box next to the AI RF profile associated device name that you want to provision.
3. From the **Actions** drop-down list, choose **Provision > Provision Device**.
4. Proceed through all the steps and in the **Summary** step, click **Deploy**.
5. In the **Summary** window, view the remaining network settings that will be pushed to the device. For more information, see [Wireless Device Provisioning Overview](#).

Unassign a Location from an Existing AI RF Profile

The following procedure describes how to unassign a location from an existing AI RF profile.

Before you begin

- Cisco AI RF profiles are supported only on Cisco Catalyst 9800 Series Wireless Controllers and Cisco IOS-XE 17.7.1 or later.
- To perform the following task, you must be a **Super Admin** or **Network Admin**.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** In the left pane, click the **Global** site.
- Step 4** In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.
The **AI RF Profile** table lists the number of created AI RF profiles.
- Step 5** Click the three dots under the **Action** column for an AI RF profile.
- Step 6** From the drop-down list, choose **Unassign Location**.
The **Unassign AI RF Profile** window appears.
- Step 7** Check the check box next to a site to unassign an AI RF profile.
- Step 8** Click the **Select from available RF Profiles** radio button to select an available RF profile that you want to assign to the chosen location.
- Step 9** From the **Select RF Profile to Replace** drop-down list, choose an RF profile.
The **Select RF Profile to Replace** drop-down list shows AI RF profiles and basic RF profiles.
If you select a basic RF profile from the drop-down list, a **Confirm Impacted Sites** window validates whether the same wireless controller manages the other site.
Review the **Confirm Impacted Sites** window and click **Confirm** to assign the chosen sites to the selected RF profile.
- Step 10** Click **Upload a CSV with RF settings back** to upload a backup of the RF settings from your local machine.
- Step 11** Click **Choose a file** to import the CSV file, or drag and drop the CSV file to the drag and drop area.
Note The maximum size of the CSV file is 10 MB.
From the uploaded CSV file, if you find an RF setting based on the selected location name, a **Confirm RF Settings for Selected Locations** window shows the **Location** and **Matched RF Profiles**.
- Step 12** Review the **Confirm RF Settings for Selected Locations** window and click **Confirm**.
- Step 13** Click **Unassign**.
- Step 14** In the confirmation window, click **Continue**.
- Step 15** Click the menu icon (☰) and choose **Activities > Tasks >** to view upcoming, in progress, completed, and failed unassign location to AI RF profile tasks.
-

What to do next

Provision Devices of an AI RF Profile-Enabled Building

The following procedure describes how to provision the devices across the AI RF profile assigned locations to deploy the AI RF profile.

1. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
In the **Inventory** window, the **Device** table lists the discovered AI RF profile associated devices.
2. Check the check box next to the AI RF profile associated device name that you want to provision.
3. From the **Actions** drop-down list, choose **Provision > Provision Device**.
4. Proceed through all the steps and in the **Summary** step, click **Deploy**.
5. In the **Summary** window, review the remaining network settings that will be pushed to the device. For more information, see [Wireless Device Provisioning Overview](#).

Upgrade a Basic Radio Frequency Profile to an AI Radio Frequency Profile

Before you begin

To onboard a site in an AI-enhanced RRM service, at least one of the following services must be enabled:

- Flexible Radio Assignment (FRA)
- Dynamic Channel Assignment (DCA)
- Transmit Power Control (TPC)
- Dynamic Bandwidth Selection (DBS)

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
 - Step 2** Click the **Wireless** tab.
 - Step 3** In the left pane, click the **Global** site.
 - Step 4** Check the check box next to the basic RF profile name that you want to upgrade to an AI RF profile.
 - Step 5** From the **Action** drop-down list, choose **Upgrade to AI**.
 - Step 6** In the confirmation window, click **Yes**.
 - Step 7** In the **Edit AI RF Profile** window, configure the AI RF profile settings. For more information, see [Create an AI Radio Frequency Profile, on page 39](#).
-

Provision a Cisco Sensor SSID for Nonfabric Deployment

- The Cisco DNA Center sensor uses the Cisco sensor provisioning Service Set Identifier (SSID) to communicate with the Plug and Play (PnP) server and obtain day-0 configurations for running tests.



Note The Cisco sensor provisioning SSID is not applicable for APs working as sensors.

- For fabric deployments, the Cisco sensor provisioning SSID is mapped to an Infrastructure Virtual Network Access Point (INFRA VN-AP) pool to communicate with Cisco DNA Center.
- The following platforms support the Cisco sensor provisioning SSID:
 - Cisco AireOS Controller
 - Cisco Catalyst 9800 Series Wireless Controller (both fabric and nonfabric deployments)
- The Cisco sensor provisioning SSID supports the following network controllers:
 - Cisco Catalyst 9800 Wireless Controllers for Cloud
 - Cisco Catalyst 9800 Series Wireless Controller
 - Cisco AireOS Controller

The following procedure enables you to configure the Cisco sensor provisioning SSID for nonfabric deployments.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the **SSID** table, hover over **+Add** ✓ and choose **Enterprise**.
The **Wireless SSID** workflow appears.
- Step 4** Toggle the **Sensor** field and click **Next**.
Note The parameters for the SSID are automatically populated and cannot be edited.
- Step 5** Click **Next**.
- Step 6** In the **Wireless Profiles** screen, check a profile from the **Profiles** table.
The **Edit Wireless Profile** dialog box appears.
- Step 7** In Fabric, select **Yes** and click **Save**.
The **Success Profile sensorProfile selected** message appears.
- Step 8** Click **Finish**.
- Step 9** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 10** Check a device and from the **Actions** drop-down menu, choose **Provision > Provision Device**.
- Step 11** Review the details under **Assign Site, Configuration, Model Configuration, Advanced Configuration, and Summary**.
Click **Next** after each screen.
- Step 12** Click **Deploy**.
The **Provision Device** dialog box is displayed.

Step 13 Choose **Now** and click **Apply**.

Result: The message **Task Scheduled view status in Tasks** appears at the bottom-right corner.

Manage Backhaul Settings

Use this procedure to view, create, and manage backhaul configurations for wireless sensors. A wireless sensor requires a backhaul SSID to communicate with Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Assurance > Manage > Sensors**.

The **Sensor List** window appears.

Step 2 Hover your cursor over the **Settings** tab and choose **Backhaul Settings**.

Step 3 You can add and manage backhaul SSIDs by doing the following:

a) Click **+ Add Backhaul**.

The **Create Sensor Backhaul SSID Assignment** window appears with two areas: **Wired Backhaul** and **Wireless Backhaul**.

b) In the **Settings Name** field, enter a name for the backhaul SSID.

c) In the **Wired Backhaul** area, configure the following:

- **Level of Security:** Displays the encryption and authentication type used by the selected SSID. The available security options are:

- **802.1x EAP:** Standard used for passing Extensible Authentication Protocol (EAP) over wired LAN.

- **Open:** No security or authentication is used.

- **EAP Method:** If you choose **802.1x EAP**, you must choose one of the following EAP methods for user authentication from the drop-down list:

- **EAP-FAST:** Enter the username and password in the fields provided.

- **PEAP-MSCHAPv2:** Enter the username and password in the fields provided.

- **EAP-TLS:** Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.

- **PEAP-TLS:** Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.

d) In the **Wireless Network Name (SSID)** area, select the wireless network (SSID) and configure the following.

- **Level of Security:** Displays the encryption and authentication type used by the selected SSID. The available 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.
- **WPA2-Personal:** Provides a good security using a passphrase or a preshared key (PSK). This allows anyone with the passkey to access the wireless network.

If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.

- **PSK Format:** The available preshared key formats are:
 - **ASCII:** Supports ASCII PSK passphrase.
 - **HEX:** Supports 64-character HEX key PSK password.
- **Open:** No security or authentication is used.

e) Click **Save**.

Step 4 You can edit the existing backhaul configurations by doing the following:

- Check the check box of the backhaul configuration.
- Hover your cursor over the **Actions** drop-down list and choose **Edit**.

Step 5 You can delete a backhaul configuration by doing the following:

- Check the check box of the backhaul configuration.
- Hover your cursor over the **Actions** drop-down list and choose **Delete**.

About Cisco Connected Mobile Experiences Integration

Cisco DNA Center supports the integration of Connected Mobile Experiences (CMX) for wireless maps. With the CMX integration, you can get the exact location of your wireless clients, rogue access points and interferers on the floor map within the Cisco DNA Center user interface.

Depending on your requirements, you can create CMX settings either at the global level or at the site, building, or floor level. For a small enterprise, you can assign CMX at the global level, which is the parent node. All children inherit their settings from the parent node. For a medium enterprise, you can assign CMX at the building level and for a small enterprise, you can assign CMX at the floor level.



Note CMX should be anonymized for security purposes.

Create Cisco CMX Settings

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

Step 2 From the **External Services** section, click **DNA Spaces/CMX Servers**.

The **DNA Spaces/CMX Servers** window appears.

Step 3 From the **CMX Servers** table, click **Add**.

- Step 4** Complete the fields in the **Add CMX Server** slide-in pane:
- **IP Address:** Enter the valid IP address of the CMX web GUI.
 - **User Name:** Enter the CMX web GUI username.
 - **Password:** Enter the password credentials.
 - **SSH User Name:** Enter the CMX admin username.
 - **SSH Password:** Enter the CMX admin password credentials.

Note Make sure that CMX is reachable.

- Step 5** Click **Add**.
The CMX server is added successfully.

Step 6 To assign a CMX server to a site, building, or a floor, click the menu icon and choose **Design > Network Settings**.

Step 7 Click the **Wireless** tab.

Step 8 In the left tree view menu, select either Global or the area, building, or floor that you are interested in.

Step 9 In the **DNA Spaces/CMX Servers** section, use the drop-down list, choose the CMX server.

Step 10 Click **Save**.

The **Create CMX Settings** page appears.

After the CMX is added, if you make any changes to the floor on the **Network Hierarchy** page, the changes are synchronized automatically with the CMX.

When the CMX is synced, Cisco DNA Center starts querying the CMX for the client location and displays the location on the floor map.

Step 11 From the floor map, you can do the following:

- View the location of the client, which is shown as a blue dot.
- Hover your cursor over an AP. A dialog box is displayed with **Info**, **Rx Neighbor**, and **Clients** tabs. Click each tab for more information. Click **Device 360** to open the Device 360 window and view issues. Click an issue to see the location of the issue and the location of the client device.
- Click an AP to open a side bar with details about the AP.
- Perform real-time client tracking when Intelligent Capture and CMX are integrated.

Step 12 If the CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** page, hover your cursor over the ellipsis **...** next to the building or floor on which you made the changes in the left tree pane, and then choose **Sync: DNA Spaces/CMX** to push the changes manually.

Step 13 To edit the CMX server details or delete a CMX server, do the following:

- a) Click the menu icon (☰) and choose **System > Settings**.
- b) From the **External Services** section, click **DNA Spaces/CMX Servers**.
- c) Select the CMX server that you want to edit, make any changes, and click **Update**.
- d) Select the CMX server that you want to delete and click **Delete**.
- e) Click **OK** to confirm the deletion.

For CMX Authentication Failure

- Check if you are able to log in to the CMX web GUI with the credentials that you provided at the time of CMX settings creation on Cisco DNA Center.
- Check if you are able to log in to the CMX console using SSH.
- Check if you are able to exercise CMX REST APIs using the API Documentation link on the CMX GUI.

If Clients Do Not Appear on the Cisco DNA Center Floor Map

- Check if the Cisco wireless controller on the particular floor is configured with CMX and is active.
- Check if the CMX GUI shows clients on the floor map.
- Use the Cisco DNA Center Maps API to list the clients on the floor: `curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor group id>/clients?associated=true`

About Cisco DNA Spaces Integration

Enterprises operating in the physical world have limited to no visibility into the behavior of people and connected assets within their buildings. Cisco DNA Spaces solves this physical blind-spot problem using location-sensing intelligence from all underlying Cisco wireless networks and translating the data into business-ready insights.

Cisco DNA Center supports the integration of Cisco DNA Spaces. With the Cisco DNA Spaces integration, you can get the exact location of your wireless clients, rogue APs, and interferers on the floor map in the Cisco DNA Center GUI. Depending on your requirements, you can create Cisco DNA Spaces settings either at the global level or at the site, building, or floor level.



Note The Cisco DNA Center and Cisco DNA Spaces integration is currently limited to only automatic map exports and synchronization for the location hierarchy. The integration does not support captive portal-based authentication features.

Integrate Cisco DNA Spaces with Cisco DNA Center

Use this procedure to integrate Cisco DNA Spaces with Cisco DNA Center.

Step 1 Onboard the Cisco DNA Spaces client:

- Log in to Cisco DNA Spaces using your email ID, and click **Continue**.
- From the **Select Customer** drop-down list, choose the Spaces tenant for the Cisco DNA Center instance (for example, dna-center-dev-US), and then click **Proceed**.
- In the Cisco DNA Spaces GUI, click the menu icon and choose **Setup > Wireless Networks**.
- In the **Connect your wireless network** window, complete Steps 1 to 3 as documented in the *Cisco DNA Spaces Configuration Guide* to onboard the Cisco DNA Spaces client.

You can access the *Cisco DNA Spaces Configuration Guide* from the right pane under **Need Help? > View Configuration Steps**.

Step 2 Register Cisco DNA Center with Cisco DNA Spaces:

- a) Log in to Cisco DNA Spaces using your email ID, and click **Continue**.
- b) From the **Select Customer** drop-down list, choose the Spaces tenant for the Cisco DNA Center instance (for example, dna-center-dev-US), and then click **Proceed**.
- c) In the Cisco DNA Spaces GUI, click the menu icon and choose **Integrations > DNA Center**.
- d) In the **DNAC Integration** window, click **Create Token**.

The **Create new token** dialog box appears.

- e) In the **Instance Name** field, enter a unique name for the instance, and then click **Create Token**.

A new token for the instance opens.

- f) Scroll to the right of the token and choose **Copy Token**.
- g) To paste the token in to the Cisco DNA Center GUI, log in to Cisco DNA Center.
- h) In the Cisco DNA Center GUI, click the menu icon (☰) and choose **System > Settings**.
- i) In the left navigation pane, scroll down and choose **DNA Spaces/CMX Servers**.

The **DNA Spaces/CMX Servers** window appears.

- j) From the **DNA Spaces** area, choose **Activate**.

The **Integrate DNA Spaces** dialog box appears.

- k) In the **Tenant Token** text box, press **Ctrl V** to paste the token that you copied from Cisco DNA Spaces, then click **Connect**.

The **Success** dialog box is displayed with the following information:

`This cluster is integrated with Cisco DNA Spaces successfully.`

The DNA Spaces/CMX Servers window displays a green ✓ **Activated** status, and the tenant that you selected in Cisco DNA Spaces (for example, dna-center-dev-US) is displayed in the **Tenant** field.

Step 3 Assign Cisco DNA Spaces to sites in Cisco DNA Center:

- a) In the Cisco DNA Center GUI, click the menu icon (☰) and choose **Design > Network Settings**.
- b) Click the **Wireless** tab.
- c) In the left tree view menu, select either **Global** or the area, building, or floor to which you want to assign Cisco DNA Spaces.
- d) From the **DNA Spaces/CMX Servers** section, use the drop-down list to select a site (for example, DNA Spaces - dna-center-dev-US).
- e) Click **Save**.

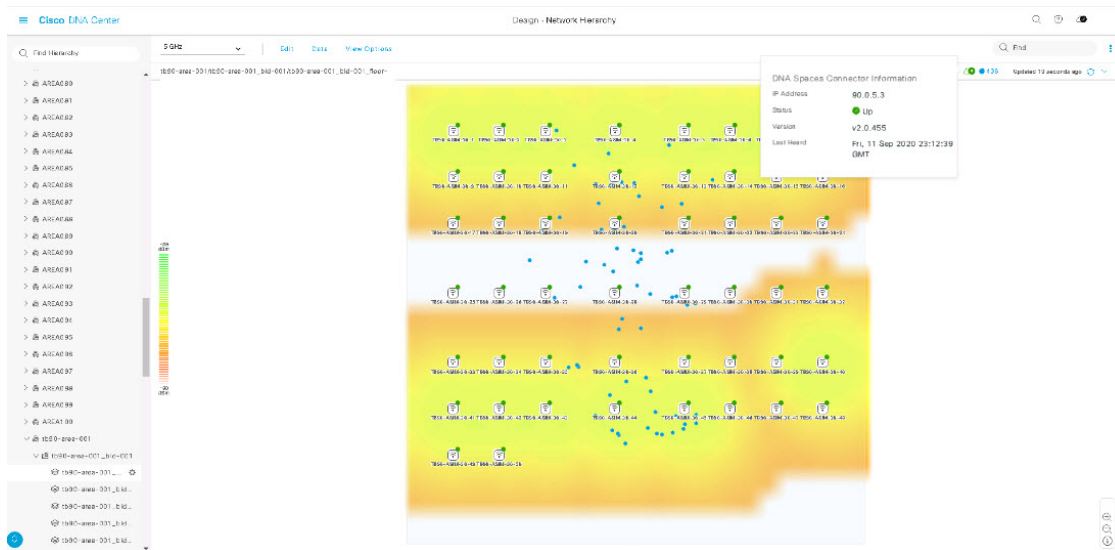
Step 4 Monitor sites in Cisco DNA Center using Cisco DNA Spaces:

- a) In the Cisco DNA Center GUI, click the menu icon (☰) and choose **Design > Network Hierarchy**.
- b) In the left tree view menu, select either **Global** or the area, building, or floor that you want Cisco DNA Spaces to monitor.

Cisco DNA Center deploys the site information to Cisco DNA Spaces automatically.

- c) To confirm that Cisco DNA Spaces is operational, verify that the Cisco DNA Spaces/CMX status icon displays on the floor that you want to monitor, as shown in the following figure.

Figure 1: Cisco DNA Spaces Status Icon



Configure a FlexConnect VLAN

You can configure the following FlexConnect VLAN settings:

- **Native VLAN:** Allows a FlexConnect group to carry the management traffic between APs and Cisco Wireless Controllers.
- **AAA Override VLAN:** Provides dynamic VLAN assignment of locally switched clients.

You can apply these settings at the global level and override them at the site, building, or floor level.

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

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, choose the appropriate scope:

- **Global:** Configures the VLAN at the global level for all sites.
- **Site, Building, or Floor:** Configures the VLAN at the chosen level only.

Step 4 In the **Native VLAN ID** field, enter a value for the VLAN ID. The valid range is from 1 to 4094.

Step 5 For the **AAA Override VLAN** settings, enter a VLAN ID and VLAN name mapping in the corresponding **VLAN ID** and **VLAN Name** fields. To add more mappings, click the Add icon.

Note The maximum VLAN mappings that you can define for a FlexConnect deployment is 16. However, for Cisco Catalyst 9800 Wireless Controllers, this number includes default WLAN VLANs and VLANs pushed by AAA.

Step 6 Click **Save**.

What to do next

Create a wireless network profile *or* configure an SSID:

- **Wireless Network Profile:** If you decide to create a wireless network profile, make sure that the **FlexConnect Local Switching** check box is checked. For more information, see [Create Network Profiles for Wireless](#).
- **SSID:** If you want to configure an SSID, see [Create SSIDs for an Enterprise Wireless Network, on page 18](#) and [Create SSIDs for a Guest Wireless Network, on page 25](#).

For the saved FlexConnect VLAN settings to get configured on the wireless controller, you must provision the wireless controller. For information, see [Provision a Cisco AireOS Controller](#) or [Configure and Provision a Cisco Catalyst 9800 Series Wireless Controller](#).

After provisioning the wireless controller, you must provision the AP that is associated with the controller.

About Wireless Mesh Networks

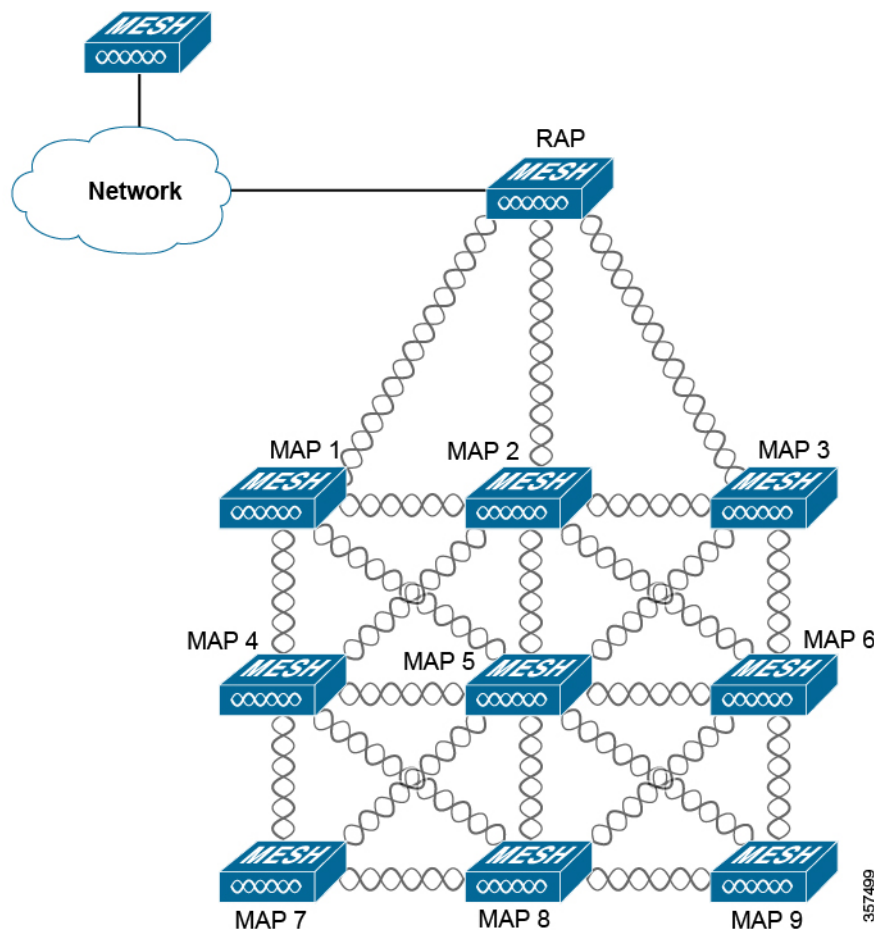
In a Cisco wireless mesh network, Access Points (APs) operate in one of the following two ways:

- Root Access Point (RAP): Connected to the wired network at each location.
- Mesh Access Point (MAP): Communicate wirelessly while providing secure and scalable wireless LAN.



Note All APs are configured and shipped as MAPs. To use an AP as a RAP, you need to reconfigure the it as a RAP. In all mesh networks, make sure that there is at least one RAP.

RAPs are connected to the wired network at each location. All the downstream APs operate as MAPs and communicate using wireless links.



Both MAPs and RAPs can provide WLAN client access. However, typically, the location of RAPs is often not suitable for providing client access.

Some buildings have onsite controllers to terminate CAPWAP sessions from the MAPs, but it is not a mandatory requirement because CAPWAP sessions can be backhauled to a controller over a wide-area network (WAN).

In a Cisco wireless backhaul network, traffic can be bridged between MAPs and RAPs. This traffic can be from wired devices that are being bridged by the wireless mesh or CAPWAP traffic from the MAPs. This traffic is always AES encrypted when it crosses a wireless mesh link such as a wireless backhaul.

For more information about mesh networks, see the latest [Cisco Wireless Mesh Access Points, Design and Deployment Guide](#).

Cisco Wireless Controller Configuration

For mesh networks, you need to configure a list of authorized APs in the controllers. Controllers respond only to requests from the MAPs that are present in its authorization list.



Note Cisco DNA Center supports the configuration of authorization lists on Cisco Catalyst 9800 Wireless Controllers running Cisco IOS Release 17.5 and later.

On both AireOS and Catalyst 9800 Wireless Controllers can use Cisco DNA Center to configure the Bridge Group Name (BGN) and RAP downlink backhaul mesh settings. In Catalyst 9800 Wireless Controllers, you can also configure the maximum range of the MAPs, backhaul client access, and backhaul data rates.

These settings are configured at the floor level using the **Wireless Network Settings** window. For more information, see [Configure Mesh Settings on Cisco Wireless Controllers, on page 57](#).

AP Configuration

If you have existing APs that you want to use in mesh network mode, you must first change the AP Mode to Bridge or Flex+Bridge using the **Configure Access Point** workflow. For information, see [Configure AP Workflow](#).

After an AP is configured for Bridge or Flex+Bridge mode, the **AP 360** window shows the mesh configuration. At this point, you need to provision the APs with the new configuration. [Provision a Cisco AP—Day 1 AP Provisioning](#).

Configure Mesh Settings on Cisco Wireless Controllers

You can configure mesh settings on AireOS and Catalyst 9800 Wireless Controllers.



Note Range, Backhaul Client Access, and Backhaul Data Rates cannot be applied on AireOS Controllers through Cisco DNA Center.

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

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, choose a floor.

Note Mesh settings are configured per floor only.

Step 4 Under **Authorized Access Points**, click **Manage Authorized Access Points**.

Step 5 In the **Manage Authorized Access Points** pane, enter the MAC addresses of MAPs that are allowed to join the controller. The controller responds only to those CAPWAP requests (from MAPs) that are in its authorization list.

Enter the MAC addresses in one of the following ways:

- **Upload a CSV File:** Download the CSV template file and add your MAC addresses to it. Then, upload the CSV file either by dragging and dropping it into the drop area or by clicking **Choose a file** and browsing to select the file.
- **Manually Add MAC Addresses:** If you have only a couple of MAC addresses to configure, click **Add**, and in the field that appears under **MAC Address**, enter the MAC address. To add more MAC addresses, click **Add**.

Step 6 Click **Save**.

Step 7 Under **Mesh Settings**, configure the following parameters:

- **Bridge Group Name:** Enter a name of up to 10 characters for the bridge group. A Bridge Group Name (BGN) controls the association of MAPs. By grouping radios, two networks on the same channel but in different BGNs cannot communicate with one another. This setting is also useful if you have more than one Root Access Point (RAP) in your network in the same sector (area).

A BGN of *NULL VALUE* is assigned by default. Although not visible to you, it allows MAPs to join the network before you assign a network-specific BGN.

- **Range (in Ft):** Maximum range (in feet) of all the MAPs in the network.
- **Backhaul Client Access:** Allows wireless client association over the backhaul radio. Generally, the backhaul radio is a 5-GHz radio for most of the MAPs. This means that a backhaul radio can carry both backhaul traffic and client traffic.

When **Backhaul Client Access** is disabled, only backhaul traffic is sent over the backhaul radio, and client association is only over the secondary radio or radios.

- **RAP Downlink Backhaul:** Click either the **5-GHz** or **2.4-GHz** radio button. If your country prohibits the use of 5-GHz, choose 2.4-GHz, or even if 5-GHz is allowed, you may prefer to use 2.4-GHz, because 2.4 GHz radio frequencies can achieve much larger mesh or bridge distances.

Note When a RAP configuration is changed from 5- to 2.4-GHz, the update is propagated from the RAP to all the MAPs. At this point, the MAPs disconnect from the 5-GHz network and connect to the 2.4-GHz network.

- **Backhaul Data Rates:** From the **5GHz Band Radio Type** and **2.4GHz Band Radio Type** drop-down lists, choose an interface rate. Valid backhaul interface rates are **802.11abg**, **802.11n**, **802.11ac** (5-GHz band radio only), **802.11ax**, and **Auto**, depending on the access point. Backhaul is used to create a wireless connection between the access points. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices.

With the **Auto** data rate, each link can arrive at the best possible rate for its link quality.

We recommend that you configure the mesh backhaul data rate as **Auto**.

Step 8 Click **Save**.
