Configure Network Settings

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 define 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 Catalyst Center configures or updates devices, the transactions are captured in the Catalyst 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 4.

- Device credentials, such as CLI, SNMP, and HTTP(S): For more information, see Configure Global Device Credentials, on page 5.

- IP address pools: For more information, see Configure IP Address Pools, on page 17.

- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles: For more information, see Configure Global Wireless Settings, on page 22.

- Configure global telemetry settings, such as syslog, SNMP, and NetFlow Collector servers using telemetry.

Configure the Time Zone for a Site

A site's time zone is used primarily for scheduling tasks, like assigning a device to a site, provisioning, or updating telemetry settings.

When scheduling a task for a later time, the site's assigned time zone will be used by default.

To configure the time zone for a site, perform the following steps:

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Servers** tab.

Step 3   From the left hierarchy tree, choose your desired site.

Step 4   In the **Time Zone** section, choose your desired time zone from the drop-down list.

Step 5   Click **Save**.

Configure the Message of the Day

The message of the day is the greeting message that is displayed when logging into a device's CLI. This message applies only to routers, switches, and hubs.

To configure the message of the day, perform the following steps:

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Servers** tab.

Step 3   From the left hierarchy tree, choose your desired site.

Step 4   In the **Message of the Day** section, choose one of the following options:

- **Use device's existing message**

This is the default option.

• **Set custom message**

You can enter your own message, but the message must adhere to the following constraints:

- Cannot contain "#" or "<"

- Cannot contain "MLTCMD" or "mltcmd"

- Maximum line length: 80 characters

- Maximum number of lines: 40

Step 5   Click **Save**.

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 Catalyst 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 interface that Catalyst Center uses as the management IP is configured as the source interface for RADIUS and TACACS servers.

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 Catalyst Center.

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

Before you begin

- You must have Read permission on **Advanced Network Settings**.

- You must specify the servers that authenticate Catalyst Center users in **System** > **Settings** window. For information on how to do it, see **Configure Authentication and Policy Servers** in Cisco Catalyst Center Administrator Guide.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Servers**.

Step 2   Expand the **AAA** area.

Step 3   Check the **Add AAA servers** check box under **Network** and/or **Client/Endpoint** tabs and configure servers and protocols for the AAA server.

Step 4   Choose the **Server Type** for authentication and authorization: **ISE** or **AAA**.

- If you choose **ISE**, configure the following:

- Choose the **Protocol**: **RADIUS** or **TACACS**.

  • From the **PAN** drop-down list, choose the IP address of the Cisco ISE server. The **PAN** drop-down list contains all the IP addresses of the Cisco ISE servers that are registered on the **System** > **Settings** window. Selecting a Cisco ISE IP populates the primary and secondary IP address drop-down lists with Policy Service Node (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 **Primary Server** and **Secondary Server** drop-down lists.

  • If you choose **TACACS**, check the **Single Connection** check box to minimize the number of TCP connections opened for duplicate transactions.

  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:

    • Choose the **Protocol**: **RADIUS** or **TACACS**.

    • From the **Primary Server** drop-down list, choose an IP address for the AAA server. Click the ✛ icon and choose an IP address from the **Secondary Server** drop-down list. Click 🗑 icon to delete the server.

    These drop-down lists contain the non-Cisco ISE AAA servers registered on the **System** > **Settings** window.

    Ensure that the AAA server IP address is not part of an existing Cisco ISE cluster.

    • If you choose **TACACS**, check the **Single Connection** check box to minimize the number of TCP connections opened for duplicate transactions.

    Note   If you switch the **Server Type** from ISE (with TACACS) to AAA with TACACS, TACACS will be disabled on the Cisco ISE server because it is no longer used for authentication.

Step 5   Click **Save**.

Configure Global Network Servers

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

✎

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

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.
Step 2   Click the **Servers** tab.
Step 3   Expand the **DHCP** area to specify one or more dedicated Dynamic Host Configuration Protocol (DHCP) servers for managing the client device networking configuration.
Step 4   Check the **Add DHCP servers** check box to view the fields.
Step 5   In the **IP Address** field, enter the IP address of a DHCP server. Click the icon to add an IP address.

Note

> You can click the + icon and enter both IPv4 and IPv6 addresses. Click the 🗑 icon to delete an IP address.
>
> You must define at least one DHCP server in order to create IP address pools.

Step 6 Expand the **DNS** area to configure your network's domain name, and specify Domain Name System (DNS) servers for hostname resolution.

Step 7 Check the **Set a domain name** check box to enter the domain name of a DNS server.

Step 8 Check the **Add DNS servers** check box to enter the IP address.

Note

> You can click the + icon and enter both IPv4 and IPv6 addresses. Click the 🗑 icon to delete an IP address.
>
> You must define at least one DNS server in order to create IP address pools.

Step 9 Expand the **NTP** area to specify one or more Network Time Protocol (NTP) servers to facilitate system clock synchronization for your network.

Step 10 Check the **Add NTP servers** check box to view the fields.

Step 11 In the **IP Address** field, enter the IP address of an NTP server. Click the icon to add an IP address.

Note

> You can click the + icon and enter both IPv4 and IPv6 addresses. Click the 🗑 icon to delete an IP address.

Step 12 Click **Save**.

Configure Global Device Credentials

"Global device credentials" refers to the common CLI, SNMP, and HTTPS credentials that Catalyst Center uses to discover and collect information about the devices in your network. Catalyst Center uses global credentials to authenticate and access the devices in a network that share these configured device credentials.

Configure Global Device Credentials Workflow

To configure global device credentials onto devices in a network, follow these high-level steps:

1. Create the global device credential. See Add Global CLI Credentials, on page 6, Add Global SNMPv2c Credentials, on page 6, Add Global SNMPv3 Credentials, on page 7, and Add Global HTTPS Credentials, on page 10.

2. Assign the global device credential to a site. See Assign Device Credentials to Sites, on page 11.

3. Apply the global device credential to all the devices in the selected site. See Apply Device Credentials to a Site's Devices, on page 12.

4. Manage the global device credential. See Manage Global Device Credentials, on page 12.

Add Global CLI Credentials

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

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, choose a site.

Step 4 Do one of the following:

- If you haven't created any credentials yet, click **Create Credentials**.

- If you have created credentials, click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Add** drop-down list, choose **CLI**.

Step 6 Complete the listed fields using the following table:

Table 1: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password that is used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7 (Optional) Check the **Assign credential to site** check box to assign the CLI credential to the selected site.

Step 8 Click **Save**.

A success message is displayed in the bottom-right corner. You can view the credential in the **Manage Credentials** slide-in pane. However, if you didn't assign the credential to a site, only the **System** focus will display the credential.

Add Global SNMPv2c Credentials

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

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

Before you begin

You must have the SNMP information for your network.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Device Credentials** tab.

Step 3   From the left hierarchy tree, choose a site.

Step 4   Do one of the following:

   • If you haven't created any credentials yet, click **Create Credentials**.

   • If you have created credentials, click **Manage Credentials**.

Step 5   In the **Manage Credentials** slide-in pane, from the **Add** drop-down list, choose **SNMPv2c Read** or **SNMPv2c Write**.

Step 6   Complete the listed fields using the following table:

Table 2: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7   (Optional) Check the **Assign credential to site** check box to assign the SNMPv2c credential to the selected site.

Step 8   Click **Save**.

A success message is displayed in the bottom-right corner. You can view the credential in the **Manage Credentials** slide-in pane. However, if you didn't assign the credential to a site, only the **System** focus will display the credential.

Add Global SNMPv3 Credentials

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

Before you begin

You must have your network's SNMP information.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Device Credentials** tab.

Step 3   From the left hierarchy tree, choose a site.

Step 4   Do one of the following:

- If you haven't created any credentials yet, click **Create Credentials**.

- If you have created credentials, click **Manage Credentials**.

Step 5   In the **Manage Credentials** slide-in pane, from the **Add** drop-down list, choose **SNMPv3**.

Step 6   Complete the listed fields using the following table:

Table 3: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name that is associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.

Auth Type	Authentication type to be used. (This field displays if you select **Authentication and Privacy** or **Authentication, No Privacy** as the authentication mode.) Choose one of the following authentication types:
	
	• **SHA**: Authentication based on HMAC-SHA
	
	• **MD5**: Authentication based on HMAC-MD5
	
	Note • The MD5 authentication type is not recommended.
	
	   • Catalyst Center does not support device provisioning if only MD5 authentication type is configured on the device for software image version 17.14.1 and later.
	
	   If you wish to use MD5 authentication, it is recommended to configure SHA authentication as well for Catalyst Center to discover and manage devices running on software image 17.14.1 and later.

Field	Description
Privacy Type	Privacy type to be used. (This field displays if you select **Authentication and Privacy** as the authentication mode.) Choose one of the following privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **AES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **AES256**: 256-bit CBC mode AES for encryption on Cisco devices. • **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. **Note** The DES privacy type is disabled and not supported.
Auth Password	SNMPv3 password that is used for gaining access to information from devices that use SNMPv3. (This field displays if you select **Authentication and Privacy** or **Authentication, No Privacy** as the authentication mode.) These passwords (or passphrases) must be at least eight characters in length and cannot contain spaces or angle brackets (< >). **Note** • 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 Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. (This field displays if you select **Authentication and Privacy** as the authentication mode.) Passwords (or passphrases) must be at least eight characters long and cannot contain spaces or angle brackets (< >). **Note** • 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 Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7   (Optional) Check the **Assign credential to site** check box to assign the SNMPv3 credential to the selected site.

Step 8   Click **Save**.

A success message is displayed in the bottom-right corner. You can view the credential in the **Manage Credentials** slide-in pane. However, if you didn't assign the credential to a site, only the **System** focus will display the credential.

Add Global HTTPS Credentials

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, choose a site.

Step 4 Do one of the following:

- If you haven't created any credentials yet, click **Create Credentials**.

- If you have created credentials, click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Add** drop-down list, choose **HTTP(S) Read** or **HTTP(S) Write**.

Step 6 Complete the listed fields using the following table:

Table 4: HTTP(S) Credentials

Field	Description
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name that is used to authenticate the HTTPS connection. • **Password**: Password that is used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?). • **Port**: Number of the TCP/UDP port that is used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name that is used to authenticate the HTTPS connection. • **Password**: Password that is used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?). • **Port**: Number of the TCP/UDP port that is used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

Step 7 (Optional) Check the **Assign credential to site** check box to assign the HTTPS credential to the selected site.

Step 8 Click **Save**.

A success message is displayed in the bottom-right corner. You can view the credential in the **Manage Credentials** slide-in pane. However, if you didn't assign the credential to a site, only the **System** focus will display the credential.

Assign Device Credentials to Sites

You can assign global device credentials to a specific site or all the sites in the hierarchy. If you choose **Global**, all sites under **Global** inherit its assigned global device credentials.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, choose the required site.

Step 4 Locate the type of global device credential that you want to assign.

Step 5 Check the corresponding **Assign** check box for the credential.

Step 6 From the **Credential** drop-down list, choose the credential that you want to assign to the selected site.

Step 7 Click **Save**.

The confirmation dialog box is displayed. Do one of the following:

- If you're ready to apply the device credential to the site's devices, click **Yes** and proceed to Apply Device Credentials to a Site's Devices, on page 12.

- If you're not ready to apply the device credential to the site's devices, click **No**.

- If there are no devices in the site, click **OK**. You can apply device credentials to the site's devices after you've added devices to the site.

Step 8 To unassign a device credential from a site, do the following:

a. From the left hierarchy tree, choose the required site.

b. Uncheck the **Assign** check box for the device credential that you want to unassign.

c. Click **Save**.

d. In the confirmation dialog box, click **Yes** to proceed with unassigning the credential from the selected site or click **No** to keep the credential assigned to the selected site.

   If you chose **Yes**, a successful dialog box is displayed, indicating that the updated site may not be in sync with the device credential applied to the site's devices. Do one of the following:

   - If you're ready to apply the device credential to the site's devices, click **Yes** and proceed to Apply Device Credentials to a Site's Devices, on page 12.

   - If you're not ready to apply the device credential to the site's devices, click **No**.

   - If there are no devices in the site, click **OK**. You can apply device credentials to the site's devices after you've added devices to the site.

Note	Unassigning a device credential from a site doesn't change the credential currently applied to all the devices in that site. To update the device credential on all the devices in a site, see Update Device Credentials on Devices, on page 16.

Manage Global Device Credentials

You can manage global device credentials in the **Manage Credentials** slide-in pane. Depending on the focus of the data (**Current site** or **System**), you can perform specific actions to manage your global device credentials. The **Current site** focus displays only global device credentials that are assigned to the selected site. In this focus, you can add and apply global device credentials to only the currently selected site. The **System** focus displays the system's pool of global device credentials. In this focus, you can add, edit, and delete global device credentials. Also, from this focus, you can apply a device credential to all the sites in the hierarchy.

Apply Device Credentials to a Site's Devices

With the **Focus** drop-down list, you can apply a global device credential either to devices in all sites or a specific site. If you apply a device credential using the **System** focus, Catalyst Center checks if any of the sites in the hierarchy are assigned to use this device credential. Then it pushes the change to those devices. If you apply a device credential using the **Current site** focus, Catalyst Center checks if the currently selected site and its child sites are assigned to use this device credential. Then it pushes the change to those devices.

Before you begin

Make sure that you assigned the device credential (that you want to apply) to the required sites. For more information, see Assign Device Credentials to Sites, on page 11.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, choose the required site.

Step 4 Click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose a focus (**Current site** or **System**) to define where you want to apply the credential.

Step 6 In the credential's corresponding **Actions** column, hover your cursor over **…** and choose **Apply**.

Step 7 In the **Apply** slide-in pane, schedule when you want to apply the credential (**Now** or **Later**).

If you choose **Later**, indicate the time zone that you want to deploy the task in by either checking the **Site Settings** check box or unchecking the **Site Settings** check box and choosing a location.

Step 8 Click **Apply**.

A success message is displayed in the bottom-right corner. To view the task details, go to the **Activities** > **Tasks** window.

Reschedule the Application of Device Credentials

If you want to reschedule a device credential task (applying the device credential to a site's devices), use this procedure.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 Do one of the following:

- If you used the **Current site** focus when you applied the device credential, choose the same site from the left hierarchy tree that you applied the device credential to.

- If you used the **System** focus when you applied the device credential, proceed to .

Step 4 Click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose the same focus that you used to apply the device credential.

Step 6 In the **Manage Credentials** table, locate the device credential with the scheduled application that you want to reschedule.

Step 7 In the device credential's corresponding **Actions** column, hover your cursor over **...** and choose **Reschedule**.

> **Note** If **Reschedule** is not displayed and instead **Apply** is displayed, make sure that you chose the same focus and same site as you did in the scheduled application of the device credential. Clicking **Apply** creates a new task; it doesn't reschedule the existing task.

Step 8 Reschedule the date and time of the task, and then click **Apply**.

> **Note** You cannot change the time zone.

A success message is displayed in the bottom-right corner, indicating that the device credential was successfully rescheduled.

View the Status of a Device Credential

With the **Current site** focus on the **Manage Credentials** slide-in pane, you can view the status of a device credential.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, choose the required site.

Step 4 Click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose **Current site**.

Step 6 In the **Manage Credentials** table, locate the relevant credential.

Step 7 In credential's corresponding **Status** column, view the credential's status.

One of the following statuses is displayed:

- **Synced**: The device credential assigned to selected site matches the device credential applied to the selected site's devices.

- **Not Synced**: The device credential assigned to selected site doesn't match the device credential applied to the selected site's devices.

- **Date and time**: This is the scheduled date and time of the device credential's application. For example, Feb 1, 2024 9:00 AM.

- **Partial Success**: The application of the device credential was partially successful.

- **Failed**: Catalyst Center failed to apply the device credential to at least one of the devices assigned to the selected site.

- **Not Applicable**: The device credential is not supported by any of the site's devices.

- **–-**: The device credential cannot be applied because either the site has no devices or the child sites use a different credential of the same credential type.

Hover your cursor over the credential's status to view additional details.

Tip   To view the latest status in the system, click the refresh icon in the top-right corner of the table.

Step 8   Alternatively, navigate to the **Provision** > **Inventory** window.

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

- **Success**: Catalyst Center successfully applied the credential change.

- **Failed**: Catalyst Center was unable to apply the credential change. Click **See Details** to view additional information about which credential change failed and why.

- **Not Applied**: The device credential applied to the selected site's device does not match the device credential assigned to the selected site.

- **Not Applicable**: The device 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 Catalyst Center was unable to apply *any* of the credentials. Click **See Details** to display additional information about which credential change failed.

Guidelines for Editing Global Device Credentials

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

- Catalyst Center uses the following process when you edit, save, and then apply a global device credential:

  1. Catalyst Center pushes the credential to the device that has local authentication. With local authentication, credential changes are applied and Catalyst Center manages the devices using these credentials.

     (Catalyst 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. Catalyst 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, Catalyst 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 Catalyst 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 Catalyst Center Inventory starts managing the device using the new credential.

- Sites can contain devices that use SNMPv2c and SNMPv3 credentials. When you edit, save, and apply global SNMPv2c or SNMPv3 credentials, Catalyst Center pushes those changes to devices and enables the credentials. For example, if you have a device that uses SNMPv2c, but you edit, save, and apply the SNMPv3 global credential, Catalyst Center pushes the new SNMPv3 credential to all devices in the associated site and enables it. This means 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 Catalyst Center applying those credential changes until you're ready. (For more information about applying device credentials, see Apply Device Credentials to a Site's Devices, on page 12.) If you edit a device credential that was previously applied to a site's devices, the device credential status displays **Not Synced** for all the sites that use this device credential. This status displays because the device credential assigned to the site no longer matches the device credential applied to that site's devices.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 Click **Manage Credentials**.

Step 4 In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose **System**.

Step 5 In the **Manage Credentials** table, locate the credential that you want to edit.

Step 6 In the credential's corresponding **Actions** column, hover your cursor over **...** and choose **Edit**.

Step 7 In the confirmation dialog box, click **OK** to proceed with editing this credential.

Note If this credential is assigned to other sites, any changes to this credential will impact those sites.

Step 8 In the slide-in pane, make the required changes and then click **Save**.

A success message displays in the bottom-right corner, indicating that the device credential was successfully updated.

Note	The CLI password credentials support only *ASCII-printable characters* (character code 32-127; see https://en.wikipedia.org/wiki/ASCII#Printable_characters).

Delete Device Credentials

If you want to delete a device credential, consider first if the device credential is assigned to any sites. If it's not assigned to any sites, you can simply delete the device credential from the system's pool of global device credentials using the **System** focus. If it's assigned to any sites, you must first either unassign the device credential from all sites that use it or delete those sites. Then you can delete the device credential from the system's pool of global device credentials.

Note	Deleting a device credential only removes it from the system's pool of global device credentials. Catalyst Center never removes any credentials from devices.

Before you begin

If the device credential that you want to delete is assigned to any sites, you must first either unassign the device credential from all the sites that use it or delete those sites. For more information, see Create, Edit and Delete a Site or Step 8, on page 11 in Assign Device Credentials to Sites, on page 11.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**

Step 2   Click the **Device Credentials** tab.

Step 3   Click **Manage Credentials**.

Step 4   In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose **System**.

Step 5   In the **Manage Credentials** table, locate the credential that you want to delete.

Step 6   In the credential's corresponding **Actions** column, hover your cursor over **…** and choose **Delete**.

Step 7   In the **Warning** dialog box, click **Yes**.

A success message is displayed in the bottom-right corner, indicating that the device credential was successfully deleted.

Update Device Credentials on Devices

When a device credential is unassigned from a site, the credential currently applied on that site's devices isn't automatically updated. The devices retain the existing credential until a new one is applied, so the device always has credentials configured. You can update the device credentials on all the devices in a site by following these high-level steps.

Step 1   Unassign the device credential from the required site. See Step 8, on page 11 in Assign Device Credentials to Sites, on page 11.

Step 2   Assign the new device credential to the same site. See Assign Device Credentials to Sites, on page 11.

Alternatively, you can unassign and assign in one step by clicking **Save** on the **Device Credentials** window.

Step 3   Apply the new device credential to that site's devices. See Apply Device Credentials to a Site's Devices, on page 12.

Step 4   Alternatively, you can log in to the device and manually update the device credential.

Configure IP Address Pools

Catalyst Center supports IPv4 and IPv6 dual-stack IP pools.

You can manually create IPv4 and IPv6 address pools.

You can also configure Catalyst Center to communicate with an external IP address manager. For more information, see the *Cisco Catalyst Center Administrator Guide*.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2   Click **Add IP Pool** and complete the required fields in the **Add IP Pool** slide-in pane.

If you have configured Catalyst 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 is displayed in the **IP Address Pools** table. You can click the **IPv4** tab or **IPv6** tab 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 Catalyst Center to communicate with an external IP Address Manager (IPAM). For more information, see the *Cisco Catalyst Center Administrator Guide*.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2   From the **Import** drop-down list, choose **Import from IPAM Server**.

Step 3   In the slide-in pane, 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.

Step 5   Click **Import**.

Import IP Address Pools from a CSV File

You can import IP address pools from a CSV file.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

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

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

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

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

a) Drag and drop the file into the drag and drop area.

b) Click **Choose a file** and then select the file from your local machine.

Step 6 Click **Import**.

Reserve an IP Address Pool

Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the left hierarchy tree, choose the required site.

Step 3 Click **Reserve IP Pool**.

Step 4 In the slide-in pane, 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**. The following options are available:

    - **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.

- **Prefix length / 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 \64 as the **Prefix length** 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 Server(s)**: DHCP server IP address(es).

• **DNS Server(s)**: DNS server address(es).

Step 5   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, do the following:

a) In the **IP Address Pools** window, from the **Actions** column, hover your cursor over ellipsis icon (⋯) and click **Edit** for the dual-stack IP pool.

b) In the **Edit IP Pool** slide-in pane, uncheck the **IPv6** check box.

c) Click **Save**.

Edit IP Address Pools

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2   From the left hierarchy tree, choose the required site.

Step 3   To edit all the IP address pools in bulk, do the following:

a) From the **More Actions** drop-down list, choose **Edit all**.

b) In the **Warning** dialog box, click **Yes**.

c) In the **Edit IP Pools** slide-in pane, make the desired changes and click **Save**.

Step 4   To edit only specific IP address pools, do the following:

a) Check the check box next to the desired IP address pools.

b) From the **More Actions** drop-down list, choose **Edit**.

Alternatively, from the **Actions** column, hover your cursor over the ellipsis icon (⋯) and click **Edit** for one of the selected IP address pools.

c) In the **Edit IP Pools** slide-in pane, make the desired changes and click **Save**.

What to do next

If the updated IP address pools are used in a fabric network, you must reconfigure the corresponding fabric on the **Provision** > **Fabric Sites** window. For more information, see Reconfigure a Fabric.

Delete IP Address Pools

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2   From the left hierarchy tree, choose the required site.

Step 3 To delete all the IP address pools in bulk, do the following:

    a) From the **More Actions** drop-down list, choose **Delete all**.

    b) In the **Warning** dialog box, click **Yes**.

Step 4 To delete only specific IP address pools, do the following:

    a) Check the check box next to the desired IP address pools.

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

       Alternatively, from the **Actions** column, hover your cursor over the ellipsis icon (**...**) and click **Delete** for one of the selected IP address pools.

    c) In the **Warning** dialog box, click **Yes**.

Clone an IP Address Pool

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

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the left hierarchy tree, choose the required site.

Step 3 Locate the desired IP address 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 Address Pools

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

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the left hierarchy tree, choose the required site.

Step 3 To release all the IP address 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 address pools, do the following:

    a) Choose the desired IP address 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   From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2   From the left hierarchy tree, choose the required site.

Step 3   Use the toggle button to switch between the table view and tree view.

- When the view contains 10 or more IP address pools, by default the GUI displays the pools in the table view.

- When the view contains fewer than 10 IP address pools, by default the GUI displays the pools in the 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 and site pool.

Step 4   The **IP Address Pools** table view displays a 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 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.
	• Catalyst 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, Catalyst 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 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 a service provider 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 From the top-left corner, click the menu icon and choose **Design** > **Service Provider Profiles**.

Step 2 If there are no existing service provider profiles, click **Create**.

Step 3 Click the plus icon (+).

Step 4 In the **Profile Name** field, enter a name for the service provider profile.

Step 5 In the **WAN Provider** field, enter a name for the WAN provider.

Step 6 From the **Model** drop-down list, choose a class model: **4 class**, **5 class**, **6 class**, or **8 class**.

For a description of these classes, see Service Provider Profiles.

Step 7 Click **Save**.

Note	You cannot create duplicate service provider profiles.

Configure Global Wireless Settings

Global wireless network settings include settings for the following:

- Service Set Identifiers (SSIDs)

- RF profiles

- Wireless interfaces and VLAN groups

- AP profiles

> • FlexConnect
>
> • Anchor groups
>
> • Security
>
> • Power profiles
>
> • Antenna radio profiles
>
> • Cisco Spaces and Cisco Connected Mobile Experiences (CMX) servers
>
> • Remote teleworker

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

You can use the **Search All Settings** field in the wireless network settings dashboard to find specific wireless network settings. You can customize the wireless network settings dashboard using **Edit Dashboard**. For more information about customizing the wireless network settings dashboard, see Customize the Wireless Network Settings Dashboard, on page 23.

Customize the Wireless Network Settings Dashboard

You can customize the wireless network settings dashboard to update the priorities of the network settings displayed in the dashboard using the **Edit Dashboard** option. Catalyst Center applies the dashboard customizations to all the sites in the wireless network settings dashboard.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **Edit Dashboard**.

Step 5 In the **Customize Wireless Settings Dashboard** slide-in pane, drag and drop the required network settings to the new positions to change their priority in the dashboard.

Step 6 Click **Save**.

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. Sites, buildings, and floors inherit settings from the global level.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **SSIDs**.

Step 5   In the **SSID** table, hover your cursor over **Add**, and choose **Enterprise**.

Step 6   In the **Wireless SSID** workflow, complete the **Basic Settings** setup:

a) If the **Sensor** toggle button is available, ensure that it's disabled.

b) In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network.

c) In the **WLAN Profile Name** field, enter a name for the WLAN profile.

Based on the WLAN profile name, Catalyst Center autopopulates the policy profile name for Cisco Catalyst 9800 Series Wireless Controller.

d) In the **Radio Policy** area, do the following:

- Check the **2.4GHz** check box to create the WLAN for 2.4-GHz.

- Check the **5GHz** check box to create the WLAN for 5-GHz.

- Check the **6GHz** check box to create the WLAN for 6-GHz. This band is supported for devices running Cisco IOS XE Release 17.7 or later.

- From the **802.11b/g Policy** drop-down list, choose a policy.

    Note   This drop-down list is available only when you check the **2.4GHz** check box.

- Check the **Band Select** check box to choose the required band.

    Note   This check box is available only when you check both the **2.4GHz** and **5GHz** check boxes.

- Check the **6 GHz Client Steering** check box to enable client steering.

    Note   This check box is available only when you check the **6GHz** check box.

e) In the **Quality of Service(QoS)** area, do the following:

- From the **Egress** drop-down list, choose an egress QoS.

- From the **Ingress** drop-down list, choose an ingress QoS.

    Note   Ingress QoS is applicable only for Cisco IOS XE wireless controllers.

The QoS selection isn't applicable when **Fast Lane** is enabled. For Cisco IOS XE wireless controllers, QoS (both egress and ingress) is set to empty. For Cisco AireOS Wireless Controllers, the egress QoS is set to **VoIP (Platinum)**.

f) In the **SSID STATE** area, click the toggle buttons to enable or disable the following settings:

- **Admin Status**: Use this toggle button to turn on or turn off the radios on the APs. When the **Admin Status** is disabled, the APs remain associated with the wireless controller and are accessible, and the APs still require licenses.

- **Broadcast SSID**: Use this toggle button to enable or disable the visibility of the SSID to all the wireless clients within range.

Step 7   Complete the **Security Settings** setup:

a) For **Level of Security**, choose the encryption and authentication type for the network. 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.

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. WPA3 is supported on Cisco AireOS Wireless Controllers running Release 8.10 and later, and Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 16.12 and later.
	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 XE Release 17.7 and later. WPA2 isn't supported for the 6-GHz band.

- **Personal**: You can configure both **WPA2** and **WPA3** security authentication by checking the respective check boxes. By default, the **WPA3** check box is enabled. If you choose **Personal**, in the **Pass Phrase** field, enter the passphrase key. This key is used as the pairwise master key (PMK) between the clients and authentication server.

Note	WPA3-Personal brings better protection to individual users by providing a more robust password-based authentication. This authentication makes the brute-force dictionary attack 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 more information, see Configure Site-Level Overrides for an SSID for Enterprise Networks, on page 30.
	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 XE Release 17.7 and later. WPA2 isn't supported for the 6-GHz band.

(Optional) For WPA2-Personal, do the following to configure multi-preshared key (MPSK) support:

1. Click **Configure MPSK**.

2. In the **Configure MPSK** dialog box, click **Add** to add an MPSK.

   You can add up to five MPSKs.

3. From the **Priority** drop-down list, choose a priority.

Note	If the priority 0 key isn't configured in the central web authentication (CWA) Flex mode, client connection to the WLAN may fail.

4. From the **Passphrase Type** drop-down list, choose a passphrase type.

5. In the **Passphrase** field, enter a passphrase.

6. Click **Save**.

MPSK isn't supported on Cisco AireOS Wireless Controllers. MPSK applies to Layer 2 security configuration for WPA2-Personal.

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

Note	Fast Transition isn't applicable for open-secured SSID.
	Because an open-secured SSID depends on an open SSID, you must have enabled anchor on an open SSID before enabling it on an open-secured SSID.

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

Note	If you chose only the **6GHz** radio policy in the **Basic Settings** window, the **Open** option is dimmed.

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, on page 33.

c) Check the **AAA Override** check box to enable the AAA override functionality.

By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.

d) Check one or more of the following check boxes:

• **Fast Lane**: Check this check box to enable fastlane capabilities on the network. When fastlane capabilities are enabled, QoS selection isn't applicable. For Cisco IOS XE wireless controllers, QoS (both egress and ingress) is set to empty. For Cisco AireOS Wireless Controllers, the egress QoS is set to **VoIP (Platinum)**.

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 the creation of unique preshared keys for individuals or groups of users in the SSID. If you check this check box, the **Enable Posture** check box is displayed.

• **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. This option is supported for Cisco AireOS Wireless Controllers running Release 8.10 MR5 and later, and Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.5 and later.

• **Enable Posture**: Check this check box to enable posture assessment. The **Pre-Auth ACL List Name** drop-down list is displayed 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' access to 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. |

e) Click **Next**.

Step 8 Complete the **Advance Settings** setup:

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

• Choose a mode: **Adaptive**, **Enable**, or **Disable**.

| **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. We recommend that you disable fast transition for WLANs using open authentication. Cisco AireOS Wireless Controllers don't support the **Adaptive** fast transition mode. |

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

b) For **MFP Client Protection**, 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 the client is also configured for WPA2 and supports CCXv5 MFP).
	MFP client protection is supported only on Cisco AireOS Wireless Controllers. MFP client protection isn't supported for the 6-GHz band.

c) For **Protected Management Frame (802.11w)**, choose the required option.

Note	The options available under **Protected Management Frame (802.11w)** vary based on the settings that you chose under **Level of Security**. The following options may be available:
	• **Optional**
	• **Required**
	• **Disabled**

d) Under **WPA2 Encryption** or **WPA3 Encryption** or **WPA2/WPA3 Encryption**, choose an available option.

The options available under this section vary based on the settings that you chose under **Level of Security**. The following options may be available: **AES(CCMP128)**, **GCMP128**, **CCMP256**, and **GCMP256**

| **Note** | This section is not available for the **Open** security under **Level of Security**. |

e) Under **Auth Key Management**, check the check box next to the required options.

| **Note** | This section is not available for the **Open** security under **Level of Security**. |

The options available under this section vary based on the fast transition settings. The following options may be available:

- For **AES(CCMP128)**: **OWE**, **802.1x (802.1X-SHA1)**, **FT + 802.1x**, **CCKM**, **802.1x-SHA256 (802.1X-SHA2)**, **PSK**, **FT + PSK**, **Easy-PSK**, **PSK-SHA256 (PSK-SHA2)**, **SAE**, and **FT + SAE**

- For **GCMP128**: **SUITEB-1X**

- For **CCMP256**: **SUITEB192-1X**

- For **GCMP256**: **SUITEB192-1X**

- **Timestamp Tolerance (in milliseconds)** (for CCKM): Enter the CCKM tolerance level in milliseconds. The valid range is from 1000 through 5000. The default value is 1000. Authenticated client devices can roam from one AP to another AP without any perceptible delay during reassociation. CCKM tolerance level isn't applicable for Cisco AireOS Wireless Controllers.

f) 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 the 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, **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 denies the client connection. The client isn't allowed to connect to the network until the exclusion timer expires. By default, **Client Exclusion** is enabled with a timeout of 180 seconds.

g) For **11v BSS Transition Support**:

- **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 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 for a WLAN.

    Note   If the data sent by the client is more than the threshold quota specified by 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 period and saves the battery power.

h) 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.

i) (Optional) For **NAS-ID**:

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

   To specify a custom script for the NAS ID, from the **NAS-ID Opt** drop-down list, choose **Custom Option** 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. Catalyst Center doesn't support the special characters ? " < and trailing spaces for the custom script.

   Note Catalyst 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.

2. (Optional) Click + to add another NAS ID. You can add up to three NAS IDs.

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

j) (Optional) Under **Configure Client Rate Limit**, enter a value for the client rate limit in bits per second. The valid range is from 8000 through 100000000000. The value must be a multiple of 500.

   Note This configuration is applicable for Cisco AireOS Wireless Controllers. To configure client rate limit for Cisco AireOS Wireless Controllers, click the menu icon and choose **Design** > **Feature Templates** > **Wireless** > **Advanced SSID Configuration**. For more information, see Create a Model Config Design for Advanced SSID.

   The following lists the valid ranges for client rate limit on Cisco IOS XE devices:

   - The valid range for Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-40 Wireless Controller, and Cisco Catalyst 9800-80 Wireless Controller is from 8000 through 67000000000 bits per second.

   - The valid range for Cisco Catalyst 9800-CL Wireless Controllers is from 8000 through 10000000000 bits per second.

   - The valid range for Cisco Embedded Wireless Controller on Catalyst Access Points is from 8000 through 2000000000 bits per second.

   - The valid range for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches is from 8000 through 100000000000 bits per second.

k) (Optional) Use the **Coverage Hole Detection** toggle button to enable or disable the coverage hole detection functionality.

l) Click **Next**.

Step 9 (Optional) Complete the **Associate Model Config to SSID** setup:

a) Check the check box next to the required model configuration design.

If you want to create a model configuration design, click **Add** and configure the required settings. For more information, see Create a Model Config Design for Advanced SSID.

b) Click **Next**.

Step 10 Complete the **Associate SSID to Profile** setup:

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

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

b) Click **Next**.

Step 11 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 12 Click **Save**.

The SSID is created.

Configure Site-Level Overrides for an SSID for Enterprise Networks

You can create SSIDs at the Global hierarchy. The areas, buildings, and floors inherit settings from the Global hierarchy. You can override the following settings at the area, building, or floor level:

- **WLAN Profile Name**

- **Level of Security**

- **Configure AAA**

- **Mac Filtering**

- **Fast Transition (802.11r)**

- **Protected Management Frame (802.11w)**

- **WPA2 Encryption**, **WPA3 Encryption**, or **WPA2/WPA3 Encryption**

- **Auth Key Management**

- **NAS-ID**

- **Configure Client Rate Limit**

For more information about configuring these settings, see .

If you override a setting at the building level, the subsequent floor inherits the new setting. The following procedure describes how to configure site-level overrides for an SSID for enterprise networks.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 2 From the left hierarchy tree, choose the site, building, or floor for which you want to configure the overrides.

Hover your cursor over the inherit icon ☰ next to the SSID to view the origin of this setting.

Step 3 Check the check box next to the SSID, and click **Edit**.

Step 4   In the **Basic Settings** window, update the name for the WLAN profile in the **WLAN Profile Name** field.

Note	• While configuring site-level overrides for the SSID, we recommend that you enter a unique name for the WLAN profile across the sites that are managed by the same wireless controller. Provsioning a wireless controller with the SSID overriden at different sites but with the same WLAN profile name or policy profile name results in provisioning failure.
	• If an SSID with site-level overrides is associated with a network profile, Catalyst Center uses the WLAN profile name available in the overriden SSID during provisioning for the corresponding sites.

Step 5   (Optional) In the **Security Settings** window, do the following:

a)   To update the encryption and authentication type for the network, under **Level of Security**, choose the required settings.

b)   To update the AAA server configuration, under **Authentication, Authorization, and Accounting Configuration**, click **Configure AAA**.

c)   To enable the AAA override functionality, check the **AAA Override** check box.

By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.

d)   To enable MAC-based access control or security on the wireless network, check the **MAC Filtering** check box.

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

Step 6   (Optional) In the **Advanced Settings** window, do the following:

a)   For **Fast Transition (802.11r)**, do the following:

• Choose a mode.

• To enable fast transitions over a distributed system, check the **Over the DS** check box.

b)   For **Protected Management Frame (802.11w)**, choose the required option.

c)   Under **WPA2 Encryption** or **WPA3 Encryption** or **WPA2/WPA3 Encryption**, choose an available option.

The options available under this section vary based on the settings that you chose under **Level of Security**.

Note	This section is not available for the **Open** security under **Level of Security**.

d)   Under **Auth Key Management**, check the check box next to the required options.

Note	This section is not available for the **Open** security under **Level of Security**.

The options available under this section vary based on the fast transition settings.

• **Timestamp Tolerance (in milliseconds)** (for CCKM): Enter the CCKM tolerance level in milliseconds. The valid range is from 1000 through 5000. The default value is 1000. CCKM tolerance level isn't applicable for Cisco AireOS Wireless Controllers.

e)   For **NAS-ID**, choose the required NAS ID.

f)   Under **Configure Client Rate Limit**, enter a value for the client rate limit in bits per second.

Step 7   In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 8   Click **Save**.

Site-level overrides are configured for the SSID.

Create Preauthentication Access Control Lists

Using the Preauthentication ACL feature, you can create a preauthentication 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 the traffic that is permitted and the traffic that is denied by the ACL. After the 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 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **Security Settings**.

Step 5 Click the **Pre-Auth ACLs** tab.

Step 6 Under the **Pre-Auth Access Control Lists** area, click **Add** to create a preauthentication ACL.

Step 7 In the **New Pre-Auth ACL** slide-in pane, do the following:

    a. In the **Pre-Auth ACL List Name** field, enter a name for the ACL list to be used on Catalyst Center.

    b. In the **Pre-Auth ACL Name** field, enter a name for the ACL to be configured on wireless controller.

Step 8 Click the **IP Addresses** tab and do the following:

    a. Choose the ACL type that you're creating: **IPV4** or **IPV6**.

        Note   IPv6 isn't supported for the custom preauthentication ACLs.

    b. Use the **Include auto rules generated by Catalyst Center** toggle button to enable or disable pushing the Catalyst Center-generated rules to the applicable SSIDs.

    By default, this toggle button is enabled. When this toggle button is enabled, Catalyst Center pushes the autogenerated rules to the applicable SSIDs. Autogenerated rules include allowing DHCP, DNS, AAA, and other applicable ports and IPs that are created as part of the default preauthentication rule.

        Note   If you disable this toggle button, you must ensure that the custom preauthentication ACL rule includes all the DHCP, DNS, and AAA servers that are mapped to WLANs.

    c. From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL.

    d. In the **Source Port** field, enter the source port number. The valid range is from 0 through 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.

    e. In the **Source IP Address** field, enter the IP address and netmask of the source. If you're configuring an IPv6 ACL, enter the IPv6 address and prefix length of the source in the **Source IP Address** field.

    f. From the **Source Subnet** drop-down list, choose a value for the source subnet.

g. In the **Destination Port** field, enter the destination port number.

h. In the **Destination IP Address** field, enter the IP address and netmask of the destination. If you're configuring an IPv6 ACL, enter the IPv6 address and prefix length of the destination.

i. From the **Destination Subnet** drop-down list, choose a value for the destination subnet.

j. To add multiple rules, click the plus icon (⊕). You can add up to 256 rules.

> **Note** For Cisco AireOS Wireless Controller, you can configure up to 64 rules.

Step 9 Click the **Walled Garden URLs** tab to add specific URLs to the allowed list for the web authentication of captive portal and walled garden.

Authentication isn't required to access the allowed list of URLs. When you try to access sites that aren't in the allowed list, you're redirected to the login window.

a. In the **URL** field, enter the URL and click the plus icon (⊕) to add the URL to the allowed list for web authentication. You can add up to 32 URL entries.

- For Cisco AireOS Wireless Controller: A valid URL must have at least one period (.). Other special characters aren't supported. For example, cisco.com and www.cisco.com.

- For Cisco Catalyst 9800 Series Wireless Controller: A valid URL must have at least one period (.). The special characters . * - _ are supported. For example, www.cisco.com, *.cisco.com, and www.cisco-.com.

Step 10 Click **Save**.

What to do next

Map the ACL with the SSID while creating SSIDs. For more information, see Create SSIDs for an Enterprise Wireless Network, on page 23 and Create SSIDs for a Guest Wireless Network, on page 34.

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**.

- 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 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **SSIDs**.

Step 5   From the **SSID** table, in the **AAA Servers** column, click **Configure AAA** for the SSID for which you want to configure the AAA server.

Step 6   From the **Configure Authentication and Authorization Server** drop-down list of the **Configure AAA Server** slide-in pane, 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** option is not supported for the Mobility Express (ME) devices.
>
> • 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, Catalyst 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 7   Click + to add an **Additional Server**.

> **Note**   You can configure a maximum of six AAA servers for an SSID of enterprise wireless network.

Step 8   From the **Additional Server** drop-down list, choose the server IP address.

Step 9   To use the AAA server for accounting, check the **Copy Same Servers for Accounting** check box.

> **Note**   You must configure an accounting server for an SSID to push the accounting configuration for the SSID.

Step 10   To configure a different accounting server for an SSID, do the following:

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

b) Click + to add an **Additional Server**.

> **Note**   You can configure a maximum of six accounting servers for an SSID of enterprise wireless network.

c) From the **Additional Server** drop-down list, choose the server IP address.

Step 11   Click **Configure**.

> **Note**   Catalyst Center allows you to override the set of AAA server configurations for the SSID at the site level. For each set of overridden AAA settings per SSID, Catalyst 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, Catalyst Center creates the new WLAN profiles equal to the number of floors.
>
> You must reprovision the device to override the AAA servers at the site level. See Wireless Device Provisioning Overview.

Create SSIDs for a Guest Wireless Network

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

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **SSIDs**.

Step 5   In the **SSID** table, hover your cursor over **Add**, and choose **Guest**.

Step 6   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) In the **WLAN Profile Name** field, enter a name for the WLAN profile.

Based on the WLAN profile name, Catalyst Center autopopulates the policy profile name for Cisco Catalyst 9800 Series Wireless Controller.

c) In the **Radio Policy** area, do the following:

- Check the **2.4GHz** check box to create the WLAN for 2.4-GHz.

- Check the **5GHz** check box to create the WLAN for 5-GHz.

- Check the **6GHz** check box to create the WLAN for 6-GHz. This band is supported for devices running Cisco IOS XE Release 17.7 or later.

- From the **802.11b/g Policy** drop-down list, choose a policy.

   Note   This drop-down list is available only when you check the **2.4GHz** check box.

- Check the **Band Select** check box to choose the required band.

   Note   This check box is available only when you check both the **2.4GHz** and **5GHz** check boxes.

- Check the **6 GHz Client Steering** check box to enable client steering.

   Note   This check box is available only when you check the **6GHz** check box.

d) In the **Quality of Service(QoS)** area, do the following:

- From the **Egress** drop-down list, choose an egress QoS.

- From the **Ingress** drop-down list, choose an ingress QoS.

   Note   Ingress QoS is applicable only for Cisco IOS XE wireless controllers.

The QoS selection isn't applicable when **Fast Lane** is enabled. For Cisco IOS XE wireless controllers, QoS (both egress and ingress) is set to empty. For Cisco AireOS Wireless Controllers, the egress QoS is set to **VoIP (Platinum)**.

e) In the **SSID STATE** area, toggle the toggle buttons to enable or disable the following settings:

- **Admin Status**: Use this toggle button to turn on or turn off the radios on the APs. When the **Admin Status** is disabled, the APs remain associated with the wireless controller and are accessible, and the APs still require licenses.

- **Broadcast SSID**: Use this toggle button to enable or disable the visibility of the SSID to all the wireless clients within range.

Step 7   Complete the **Security Settings** setup:

a) For the **L2 SECURITY** area, 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 XE Release 17.7 and later. WPA2 isn't supported for the 6-GHz band.

- **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 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 XE Release 17.7 and later. WPA2 isn't supported for the 6-GHz band.

(Optional) For WPA2-Personal, do the following to configure multi-preshared key (MPSK) support:

1. Click **Configure MPSK**.

2. In the **Configure MPSK** dialog box, click **Add** to add an MPSK.

   You can add up to five MPSKs.

3. From the **Priority** drop-down list, choose a priority.

Note	If the priority 0 key is not configured in central web authentication (CWA) Flex mode, client connection to the WLAN may fail.

4. From the **Passphrase Type** drop-down list, choose a passphrase type.

5. In the **Passphrase** field, enter a passphrase.

6. Click **Save**.

MPSK is not supported on Cisco AireOS Wireless Controllers. MPSK applies to Layer 2 security configuration for WPA2- Personal.

- **Open Secured**: From the **Select existing 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.
	Because 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 authentication.

Note	If you chose only the **6GHz** radio policy in the **Basic Settings** window, the **Open** option is dimmed.

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
Central Web Authentication	Use AAA server for central web authentication (CWA). (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: • **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. (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: • **Success Page**: The guests are redirected to the **Authentication Success** window. • **Original URL**: The guests are redirected to the URL that 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.
• **Web Authentication Internal** • **Web Authentication External**	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. For web authentication internal, the client is redirected to a window that is constructed by the Cisco Wireless Controller. For web authentication external, the client is redirected to the specified URL. Enter a redirect URL in the **Web Auth Url** field.

Authentication Server Type	Description
• **Web Passthrough Internal** • **Web Passthrough External**	Web passthrough is used for guest access and doesn't requires authentication credentials. In web passthrough authentication, wireless users are redirected to the Usage Policy window when they use the internet for the first time. After accepting the policy, users are allowed to use the internet.

• **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**, In the **Timeout Settings for sleeping clients** area, choose an authentication setting for sleeping clients:

- • **Always authenticate**: Enables authentication for sleeping clients.

- • **Authenticate after**: Enter how many minutes you want sleeping clients to be remembered for before reauthentication becomes necessary. The valid range is from 10 minutes through 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 reauthenticate through the login window. You can configure how long a client is remembered on a WLAN and 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**, 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, on page 44.

e) Check the **AAA Override** check box to enable the AAA override functionality.

By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.

f) Check one or more of the following check boxes:

- • **Fast Lane**: Check this check box to enable fastlane capabilities on the network. When fastlane capabilities are enabled, QoS selection isn't applicable. For Cisco IOS XE wireless controllers, QoS (both egress and ingress) is set to empty. For Cisco AireOS Wireless Controllers, the egress QoS is set to **VoIP (Platinum)**.

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 the creation of unique preshared keys 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. This option is supported for Cisco AireOS Wireless Controllers running Release 8.10 MR5 and later, and Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.5 and later.

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

g) Click **Next**.

Step 8   Complete the **Advance Settings** setup:

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

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

> **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. We recommend that you disable fast transition for WLANs using open authentication. Cisco AireOS Wireless Controllers don't support the **Adaptive** fast transition mode.

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

b) For **MFP Client Protection**, 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 MFP is negotiated (that is, if WPA2 is configured on the wireless controller, and the client is also configured for WPA2 and supports CCXv5 MFP).
>
> MFP client protection is supported only on Cisco AireOS Wireless Controllers. MFP client protection isn't supported for the 6-GHz band.

c) For **Protected Management Frame (802.11w)**, choose the required option.

> **Note** The options available under **Protected Management Frame (802.11w)** vary based on the settings that you chose under **Level of Security**. The following options may be available:
>
>   - **Optional**
>
>   - **Required**
>
>   - **Disabled**

d) Under **WPA2 Encryption** or **WPA3 Encryption** or **WPA2/WPA3 Encryption**, choose an available option.

The options available under this section vary based on the settings that you chose under **Level of Security**. The following options may be available: **AES(CCMP128)**, **GCMP128**, **CCMP256**, **GCMP256**

> **Note** This section is not available for the **Open** security under **Level of Security**.

e) Under **Auth Key Management**, check the check box next to the required options.

Note This section is not available for the **Open** security under **Level of Security**. The following options may be available:

- For **AES(CCMP128)**: **OWE**, **802.1x (802.1X-SHA1)**, **FT + 802.1x**, **CCKM**, **802.1x-SHA256 (802.1X-SHA2)**, **PSK**, **FT + PSK**, **Easy-PSK**, **PSK-SHA256 (PSK-SHA2)**, **SAE**, **FT + SAE**

- For **GCMP128**: **SUITEB-1X**

- For **CCMP256**: **SUITEB192-1X**

- For **GCMP256**: **SUITEB192-1X**

The options available under this section vary based on the fast transition settings.

- **Timestamp Tolerance (in milliseconds)** (for CCKM): Enter the CCKM tolerance level in milliseconds. The valid range is from 1000 through 5000. The default value is 1000. Authenticated client devices can roam from one AP to another AP without any perceptible delay during reassociation. CCKM tolerance level isn't applicable for Cisco AireOS Wireless Controllers.

f) For **11K**:

- **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 the 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, **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 denies the client connection. The client is not allowed to connect to the network until the exclusion timer expires. By default, **Client Exclusion** is enabled with a timeout of 180 seconds.

g) For **11v BSS Transition Support**:

- **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 period of time and saves the battery power.

h) (Optional) For **NAS-ID**:

1. 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. Catalyst Center doesn't support the special characters ? " < and trailing spaces for the custom script.

Note	Catalyst 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.

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

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

i) (Optional) Under **Configure Client Rate Limit**, enter a value for the client rate limit in bits per second. The valid range is from 8000 through 100000000000. The value must be a multiple of 500.

Note	This configuration is not applicable for Cisco AireOS Wireless Controllers. To configure client rate limit for Cisco AireOS Wireless Controllers, click the menu icon and choose **Design** > **Feature Templates** > **Wireless** > **Advanced SSID Configuration**. For more information, see Create a Model Config Design for Advanced SSID.

    The following lists the valid ranges for client rate limit on Cisco IOS XE devices:

    - The valid range for Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-40 Wireless Controller, and Cisco Catalyst 9800-80 Wireless Controller is from 8000 through 67000000000 bits per second.

    - The valid range for Cisco Catalyst 9800-CL Wireless Controller is from 8000 through 10000000000 bits per second.

    - The valid range for Cisco Embedded Wireless Controller on Catalyst Access Points is from 8000 through 2000000000 bits per second.

    - The valid range for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches is from 8000 through 100000000000 bits per second.

j) (Optional) Use the **Coverage Hole Detection** toggle button to enable or disable the coverage hole detection functionality.

k) Click **Next**.

Step 9 (Optional) Complete the **Associate Model Config to SSID** setup:

a) Check the check box next to the required model configuration design.

    If you want to create a model configuration design, click **Add** and configure the required settings. For more information, see Create a Model Config Design for Advanced SSID.

      b) Click **Next**.

Step 10 Complete the **Associate SSID to Profile** setup:

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

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

      b) Click **Next**.

Step 11 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 12 Click **Save** to save the SSID settings.

      The SSID is created.

Configure Site-Level Overrides for an SSID for Guest Networks

You can create SSIDs at the Global hierarchy. The areas, buildings, and floors inherit settings from the Global hierarchy. You can override the following settings at the area, building, or floor level:

- **WLAN Profile Name**
- **Level of Security**
- **Configure AAA**
- **Mac Filtering**
- **Fast Transition (802.11r)**
- **WPA2 Encryption**, **WPA3 Encryption**, or **WPA2/WPA3 Encryption**
- **Auth Key Management**
- **NAS-ID**
- **Configure Client Rate Limit**

For more information about configuring these settings, see Create SSIDs for a Guest Wireless Network, on page 34.

If you override a setting at the building level, the subsequent floor inherits the new setting. The following procedure describes how to configure site-level overrides for an SSID for guest networks.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 2 From the left hierarchy tree, choose the site, building, or floor for which you want to configure the overrides.

      Hover your cursor over the inherit icon ≡ next to the SSID to view the origin of this setting.

Step 3 Check the check box next to the SSID, and click **Edit**.

Step 4 In the **Basic Settings** window, update the name for the WLAN profile in the **WLAN Profile Name** field.

Note	• While configuring site-level overrides for the SSID, we recommend that you enter a unique name for the WLAN profile across the sites that are managed by the same wireless controller. Provsioning a wireless controller with the SSID overriden at different sites but with the same WLAN profile name or policy profile name results in provisioning failure.
	• If an SSID with site-level overrides is associated with a network profile, Catalyst Center uses the WLAN profile name available in the overriden SSID during provisioning for the corresponding sites.

Step 5 (Optional) In the **Security Settings** window, do the following:

a) To update the encryption and authentication type for the network, under **Level of Security**, choose the required settings.

b) To update the AAA server configuration, under **Authentication, Authorization, and Accounting Configuration**, click **Configure AAA**.

c) To enable the AAA override functionality, check the **AAA Override** check box.

By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.

d) To enable MAC-based access control or security on the wireless network, check the **MAC Filtering** check box.

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

Step 6 (Optional) In the **Advanced Settings** window, do the following:

a) For **Fast Transition (802.11r)**, do the following:

• Choose a mode.

• To enable fast transitions over a distributed system, check the **Over the DS** check box.

b) Under **WPA2 Encryption** or **WPA3 Encryption** or **WPA2/WPA3 Encryption**, choose an available option.

The options available under this section vary based on the settings that you chose under **Level of Security**.

Note	This section is not available for the **Open** security under **Level of Security**.

c) Under **Auth Key Management**, check the check box next to the required options.

Note	This section is not available for the **Open** security under **Level of Security**.

The options available under this section vary based on the fast transition settings.

• **Timestamp Tolerance (in milliseconds)** (for CCKM): Enter the CCKM tolerance level in milliseconds. The valid range is from 1000 through 5000. The default value is 1000. CCKM tolerance level isn't applicable for Cisco AireOS Wireless Controllers.

d) For **NAS-ID**, choose the required NAS ID.

e) Under **Configure Client Rate Limit**, enter a value for the client rate limit in bits per second.

Step 7 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 8 Click **Save**.
Site-level overrides are configured for the SSID.

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   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **SSIDs**.

Step 5   From the **SSID** table, in the **AAA Servers** column, click **Configure AAA** for the SSID for which you want to configure the AAA server.

Step 6   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.

- Catalyst Center-generated preauthentication ACLs are created only for the configured AAA or PSN servers for CWA SSIDs of guest wireless networks. If you upgrade from an earlier release, to ensure that there is no compliance mismatch, you must reprovision the wireless controller.

- Catalyst 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** option is not supported for Mobility Express (ME) devices.

- 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, Catalyst 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 7   Click + to add an **Additional Server**.

Note   You can configure a maximum of six AAA servers for an SSID of guest wireless network.

Step 8   From the **Additional Server** drop-down list, choose the server IP address.

Step 9   (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 10   To use the AAA server for accounting, check the **Copy Same Servers for Accounting** check box.

Note   You must configure an accounting server for an SSID to push the accounting configuration for the SSID.

Step 11   To configure a different accounting server for an SSID, do the following:

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

b) Click + to add an **Additional Server**.

> **Note** You can configure a maximum of six accounting servers for an SSID of enterprise wireless network.

c) From the **Additional Server** drop-down list, choose the server IP address.

Step 12 Click **Configure**.

> **Note** Catalyst Center allows you to override the set of AAA server configurations for the SSID at the site level. For each set of overridden AAA settings per SSID, Catalyst 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, Catalyst Center creates the new WLAN profiles equal to the number of floors.
>
> You must reprovision the device to override the AAA servers at the site level. See Wireless Device Provisioning Overview.

Create SSID Scheduler

You can create an SSID scheduler to enable or disable WLAN based on time zone.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **SSIDs**.

Step 5 In the **SSID** table, click **SSID Scheduler**.

Step 6 In the **SSID Scheduler** window, click **Add**.

Step 7 In the **Create Scheduler** slide-in pane, do the following:

a) Enter a unique name for the SSID scheduler that you want to create.

b) Click the **Client Deny** radio button for denying clients from joining SSID.

c) Click the **Enable SSID** radio button to schedule SSID broadcasting.

d) Choose the **Scheduler Type Daily**, **Weekly**, or **Monthly** and complete the required settings.

e) From the **Time Zone** drop-down list, choose the time zone.

f) Click **Save**.

The created SSID scheduler appears in the **SSID Scheduler** table.

Step 8 To edit the SSID scheduler, do the following:

a) From the **SSID Scheduler** table, choose the SSID scheduler and click **Edit**.

b) In the **Edit SSID Scheduler** slide-in pane, make the required changes and click **Save.**

Step 9 To delete the SSID scheduler, choose the SSID scheduler and click **Delete.**

Step 10 To view the details of the SSID scheduler, choose the SSID scheduler and click **Scheduler History**.

| **Note** | To view the **Scheduler History**, you must install the Assurance package. |

What to do next

Enable the SSID scheduler for wireless controller. For more details, see Add SSIDs to a Network Profile.

Create a Wireless Interface

You can create wireless interfaces only in nonfabric deployments.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **Interfaces & VLAN Groups**.

Step 5 Click the **Interfaces** tab.

Step 6 From the **Wireless Interfaces** table, click **Add**.

Step 7 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.

     For Cisco AireOS Wireless Controllers, the valid range is from 1 through 4094. For Cisco Catalyst 9800 Series Wireless Controllers, the valid range is from 2 through 4094.

Step 8 Click **Save**.

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

Design and Provision Interface/VLAN Groups for Nonfabric Deployments

Catalyst 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.

Catalyst 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 Catalyst 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   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **Interfaces & VLAN Groups**.

Step 5   Click the **VLAN Groups** tab.

Step 6   From the **VLAN Group** table, click **Add**.

Step 7   In the **Add VLAN Group** slide-in pane, do the following:

a) Enter a valid **VLAN Group Name**
b) Select single or multiple interfaces from the list.
c) Click **Save**.

Note   If you select more than 15 interfaces, the selected interfaces might not be displayed correctly onscreen.

Step 8   In the **Edit Network Profile** window, 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 9   To add more SSIDs to the VLAN group, click **Add SSID**.

Step 10   Choose **Interface** or **VLAN** group.

Step 11   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 12   Click **Save**.

Step 13   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 14   From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

Step 15   Select the device.

Step 16   From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

Step 17   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 18   Click **Deploy**.

The **Provision Device** dialog box opens.

Step 19   Choose **Now** and click **Apply**.

The message **Task Scheduled view status in Tasks** is displayed.

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   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **RF Profiles**.

Step 5   In the **Wireless Radio Frequency Profile** area, hover your cursor over **Add**, and choose **Basic RF Profile**.

Step 6   In the **Profile Name** field of the **Create Wireless Radio Frequency Profile** window, enter the RF profile name.

Step 7   Configure the following in the **2.4 GHz** tab:

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, Catalyst 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 and reprovision the wireless controller or AP, Catalyst Center creates the RF profile for the corresponding band and maps it to the AP group (instead of configuring it as **None**) and disables the Admin status of the corresponding radios on the APs.

- For Cisco AireOS Wireless Controller, when you disable the Admin status for the 2.4-GHz band on the RF profile, Catalyst Center changes the 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, Catalyst 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 APs.

b) Under **Parent Profile**, click **High**, **Medium (Typical)**, **Low**, or **Custom**. (The available data rates and power configuration values change depending on the parent profile chosen. For example, if you choose **High**, it populates the profile configurations available in the device for 2.4-GHz. If you change any settings in the populated data rates and power configurations, the **Parent Profile** automatically changes to **Custom**.) A new RF profile is created only for the selected custom profiles.

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

c) **DCA Channel** dynamically manages the 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.

- If the individual channel numbers aren't already displayed, 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 available channel numbers are **2**, **3**, **4**, **5**, **7**, **8**, **9**, **10**, **12**, **13**, and **14**.

Note	• For Cisco AireOS Wireless Controller, Catalyst 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) Under **Supported Data Rate**, configure the following:

- Check the **Enable 802.11b data rates** check box to enable the 802.11b data rates.

- Use the 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 **Mandatory Data Rates**, check the check boxes 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**.

The available data rates change depending on the data rates set under **Supported Data Rate**.

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 dBm to 30 dBm, and the default is -10 dBm.

- **TPC 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 transmission power rates. The range is from -50 dBm to 80 dBm, and the default threshold is -70 dBm.

- **RX SOP Threshold (dBm)**: 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 Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 2.4-GHz band, the high threshold value is -79 dBm, the medium threshold value is -82 dBm, and the low threshold value is -85 dBm.

g) Under **Coverage Hole Detection**, configure the following:

Note	You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see Create a Model Config Design for RRM General Parameters. For more information about provisioning, see Provision Wireless Devices.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.

- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

h) Under **Client Limit**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note   A maximum client limit isn't supported on Cisco AireOS Wireless Controllers.

- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7, the maximum client limit is 200.

- If the wireless controller is running Cisco IOS XE Release 17.7 or later and earlier than Cisco IOS XE Release 17.9, the maximum client limit is 400.

- If the wireless controller is running Cisco IOS XE Release 17.9 or later, the maximum client limit is 500.

i) Under **802.11ax**, configure the following spatial reuse parameters:

Note   802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.

- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

  SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.

- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.

- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 8   Configure the following in the **5 GHz** tab:

a) 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, Catalyst Center disables the Admin status of the **5 GHz** RF profile.

• For Cisco AireOS Wireless Controller, if you disable the **2.4 GHz** toggle button and reprovision the wireless controller or AP, Catalyst Center creates the RF profile for the corresponding band and maps it to the AP group (instead of configuring it as **None**) and disables the Admin status of the corresponding radios on the APs.

• For Cisco AireOS Wireless Controller, when you disable the Admin status for the 5-GHz band on the RF profile, Catalyst 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, Catalyst 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 APs.

b) Under **Parent Profile**, click **High**, **Medium (Typical)**, **Low**, or **Custom**. (The available data rates and power configuration values change depending on the parent profile chosen. For example, if you choose **High**, it populates the configurations available in the device for 5 GHz. If you change any settings in the populated data rates and power configurations, the **Parent Profile** automatically changes to **Custom**.) A new RF profile is created only for select custom profiles.

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

c) From the **Channel Width** drop-down list, choose a channel bandwidth option: **20 MHz**, **40 MHz**, **80 MHz**, or **160 MHz**, or **Best**.

d) Check the **Zero Wait DFS** check box to allow APs with 5-GHz radio band to switch to a new channel without any waiting time.

Note Catalyst Center supports Zero Wait DFS for Cisco Wireless Controllers running Cisco IOS XE Release 17.9.1 and later.

e) Under **DCA Channel**, configure the following to manage the channel assignments:

Note For Cisco AireOS Wireless Controller, Catalyst 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.

• Check the **Select All** check box to select DCA channels **UNII-1 36-48**, **UNII-2 52-144**, and **UNII-3 149-173**. Alternatively, check the individual check boxes next to the channel numbers.

• If the individual channel numbers aren't already displayed, click **Show Advanced** to choose the channel numbers for each band.

• **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-3 149-173**: The channels available for UNII-3 band are **149**, **153**, **157**, **161**, **165**, **169**, and **173**. Check the **UNII-3 149-173** check box to include all channels, or check an individual check box.

f) 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**.

g) Under **Mandatory Data Rates**, check the check boxes 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**.

The available data rates change depending on the data rates set under **Supported Data Rate**.

h) 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 dBm to 30 dBm, and the default is -10 dBm.

- **TPC 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 transmission power rates. The range is from -50 dBm to 80 dBm, and the default threshold is -70 dBm.

- **RX SOP Threshold (dBm)**: 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 Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 5-GHz band, the high threshold value is -76 dBm, the medium threshold value is -78 dBm, and the low threshold value is -80 dBm.

i) Under **Coverage Hole Detection**, configure the following:

Note You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see Create a Model Config Design for RRM General Parameters. For more information about provisioning, see Provision Wireless Devices.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.

- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

j) Under **Client Limit**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note A maximum client limit isn't supported on Cisco AireOS Wireless Controllers.

- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7, the maximum client limit is 200.

- If the wireless controller is running Cisco IOS XE Release 17.7 or later and earlier than Cisco IOS XE Release 17.9, the maximum client limit is 400.

- If the wireless controller is running Cisco IOS XE Release 17.9 or later, the maximum client limit is 500.

k) Under **Flexible Radio Assignment (FRA)**, check the **Client Aware** check box to enable the Client Aware feature.

This feature monitors the dedicated 5-GHz radio. When the client load passes the threshold, it automatically changes the FRA from a monitor role into a 5-GHz role, effectively doubling the capacity of the cell on demand. Once the capacity crisis is over and Wi-Fi load returns to normal, the radios resume their previous roles.

Note You must enable FRA in **Design** > **Feature Templates** > **Wireless** > **RRM FRA Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM FRA parameters, see Create a Model Config Design for RRM FRA Parameters. For more information about provisioning, see Provision Wireless Devices.

If you enable the Client Aware feature, configure the following:

- In the **Client Select (%)** field, enter a value for client selection. The valid range is from 0 through 100 percent. The default value is 50 percent.

- In the **Client Reset (%)** field, enter a reset value for the client. The valid range is from 0 through 100 percent. The default value is 5 percent.

l) Under **802.11ax**, configure the following spatial reuse parameters:

Note 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.

- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.

- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.

- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 9 Configure the following in the **6 GHz** tab:

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

Note	• The 6-GHz radio is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
	• For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **6 GHz** toggle button, Catalyst Center disables the Admin status of the **6 GHz** RF profile.

b) Enable the **Enable PSC Enforcing** toggle button to allow Preferred Scanning Channel (PSC) enforcement.

PSC enforcement improves the connectivity of 6-GHz devices by prioritizing PSC-enabled channels.

Note	If you enable PSC enforcement, the check boxes next to the non-PSC channels are dimmed.

c) Under **DCA Channel**, configure the following 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.

    - **UNII-5 1-93**

    - **UNII-6 97-113**

    - **UNII-7 117-185**

    - **UNII-8 189-233**

- If the channel numbers aren't already displayed, click **Show Advanced** to select the channel numbers for each band.

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.

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 **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

e) Under **Mandatory Data Rates**, check the check boxes 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**.

The available data rates change depending on the data rates set under **Supported Data Rate**.

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

- **Standard Power Service**: For APs with the standard power capability, compliance with FCC regulations requires the activation of Automatic Frequency Coordination (AFC). AFC uses the AP location and height data to determine the optimal channel and transmission power, ensuring noninterference with the licensed incumbent users on the 6-GHz band. You can use the Standard Power Service feature on Catalyst Center to activate AFC. By default, this feature is disabled. To enable this feature, click the **Standard Power Service** toggle button.

    This feature is applicable only for Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.12.3 or later. When this feature is disabled, the 6-GHz dual-power mode APs are restricted to operate only in the low-power indoor mode, and the standard-power mode only APs have the radios disabled completely.

Note To ensure proper functioning of this feature, you must configure the AP height, AP height uncertainty, and external antenna cable length on the corresponding wireless controller. For the standard power-capable APs to operate on standard power, you must ensure that you select at least one supported DCA channel based on your country-specific regulations.

- **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 dBm to 30 dBm, and the default is -10 dBm.

- **TPC 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 transmission power rates. The range is from -50 dBm to 80 dBm, and the default threshold is -70 dBm.

- **RX SOP Threshold (dBm)**: 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 Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 6-GHz band, the high threshold value is -76 dBm, the medium threshold value is -78 dBm, and the low threshold value is -80 dBm.

g) Under **Coverage Hole Detection**, configure the following:

Note You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see Create a Model Config Design for RRM General Parameters. For more information about provisioning, see Provision Wireless Devices.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.

- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

h) Under **Client Limit**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note - If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7, the maximum client limit is 200.

- If the wireless controller is running Cisco IOS XE Release 17.7 or later and earlier than Cisco IOS XE Release 17.9, the maximum client limit is 400.

- If the wireless controller is running Cisco IOS XE Release 17.9 or later, the maximum client limit is 500.

i) Under **Flexible Radio Assignment (FRA)**, complete the following:

Note • You must enable FRA in **Design** > **Feature Templates** > **Wireless** > **RRM FRA Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM FRA parameters, see Create a Model Config Design for RRM FRA Parameters. For more information about provisioning, see Provision Wireless Devices.

• FRA is supported only on wireless controllers that run Cisco IOS XE Release 17.9.1 and later.

• In the **Client Reset Count** field, enter a reset count value for the client. The valid range is from 0 through 10. The default value is 1.

• In the **Client Utilization Threshold (%)** field, enter a utilization threshold value for the client. The valid range is from 0 through 100 percent. The default value is 5 percent.

j) Under **802.11ax**, configure the following multiple basic service set identifier (BSSID) and spatial reuse parameters:

• From the **6 GHz Discovery Frames** drop-down list, choose the required option from **None**, **Broadcast Probe Response**, and **FILS Discovery**.

6-GHz discovery frames are needed if the 6-GHz band is the only operational band. For more information about the 6-GHz discovery frames, click **Learn More**.

• In the **Broadcast Probe Response Interval (msec)** field, enter the broadcast probe response interval, in msec. The valid range is from 5 msec through 25 msec. The default value is 20 msec.

• Under **MULTI BSSID**, check the check boxes to enable the following parameters:

   • Downlink OFDMA

   • Uplink OFDMA

   • Downlink MU-MIMO

   • Uplink MU-MIMO

   • Target wake time

   • TWT Broadcast Support

Note You must enable multiple BSSID in **Design** > **Feature Templates** > **Wireless** > **Dot11ax Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for Dot11ax, see Create a Model Config Design for Dot11ax Configuration. For more information about provisioning, see Provision Wireless Devices.

• Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.

• In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

• Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.

- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.

- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 10   Click **Save**.

Step 11   (Optional) To mark a profile as the default RF profile, check the **Profile Name** check box and click **Mark Default**. In the **Warning** window, click **OK**.

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 or Delete a Basic Radio Frequency Profile

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

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **RF Profiles**.

Step 5   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 6   Check the check box next to the basic profile name that you want to edit.

Step 7   From the **Action** drop-down list, choose **Edit/View**.

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

Step 8   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 48.

Step 9   Click **Save**.

Step 10   To delete a basic RF profile, check the check box next to the basic RF profile name.

Step 11   From the **Action** drop-down list, choose **Delete** and then click **Yes**.

Step 12   To mark a basic RF profile as the default, check the check box next to a basic RF profile name.

Step 13   From the **Action** drop-down list, choose **Mark Default** and then click **Yes**.

What to do next

For Cisco AireOS Wireless Controllers, if you modify the DCA channels or data rates for an RF profile that is already provisioned on a wireless controller, Catalyst Center resets the corresponding radio.

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 profile 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.

Clone a Basic Radio Frequency Profile

You can create a copy of a basic RF profile by cloning it. Cloning allows you to reuse the configurations of an existing RF profile for a new RF profile. You can clone both the system and custom RF profiles.

Step 1	From the top-left corner, click the menu icon and choose **Design** > **Network Settings**
Step 2	Click the **Wireless** tab.
Step 3	From the left hierarchy tree, choose **Global**.
Step 4	Click **RF Profiles**.
Step 5	In the **Basic RF Profile** tab, check the check box next to the profile name that you want to clone.
Step 6	From the **Actions** drop-down list, choose **Create a Clone**.
Step 7	In the **Profile Name** field of the **Create Wireless Radio Frequency Profile** window, enter a unique name for the profile.
Step 8	Edit the RF profile configurations as necessary. For more information, see Create a Wireless Radio Frequency Profile, on page 48.
Step 9	Click **Save**.

Prerequisites for Configuring AI Radio Frequency Profiles

- You must enable Cisco AI Network Analytics under the system settings. For more information, see **Configure Cisco AI Network Analytics Data Collection** in the *Cisco Catalyst Center Administrator Guide*.

- You must enable AI-Enhanced RRM. From the top-left corner, click the menu icon and choose **System** > **Settings** > **External Services** > **Cisco AI Analytics**. In the **AI-ENHANCED RRM** area of the **Cisco AI Analytics** window, click the toggle button to enable the AI-Enhanced RRM.

- Cisco AI RF profiles are supported only on Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.7.1 or later.

Note Ensure that the **Group Mode** option for all the three bands (2.4 GHz, 5 GHz, and 6 GHz) is configured as **auto** or **leader** on the wireless controller.

- Cisco AI RF profiles are supported for 6-GHz radio only on wireless controllers that run Cisco IOS XE Release 17.9.1 and later.

- You must be a **Super Admin** or **Network Admin**.

Create an AI Radio Frequency Profile

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

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for Configuring AI Radio Frequency Profiles, on page 58.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **RF Profiles**.

Step 5   In the **Wireless Radio Frequency Profile** area, hover your cursor over **Add** and choose **AI RF Profile**.

Step 6   In the **Profile Name** field of the **Create AI Radio Frequency Profile** window, enter the RF profile name.

Step 7   In the **Radio Frequency Settings** area of **Basic Settings**, check the **2.4 GHz**, **5 GHz**, or **6 GHz** check box.

The RF bands are checked by default. If you uncheck a band, Catalyst Center disables the Admin status of the corresponding RF profile.

> **Note**   Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.9.1 and later support the AI RF profile for the **6 GHz** band.

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 time zone of the building. You must configure a time zone for the respective building under network settings.

Step 9   In the **Busy Hour Sensitivity** area, click the **Low**, **Medium**, or **High** radio button to define the threshold of the 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**, **5 GHz**, or **6 GHz** columns to enable or disable RF settings for the corresponding bands.

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 the 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 performance and interference.

Note	• When you disable the **2.4 GHz** band for FRA, it automatically disables the **5 GHz** band for FRA, and conversely.

• When you disable the **5 GHz** band for DCA, it disables the **2.4 GHz** band for FRA and the **5 GHz** band for FRA and DBS.

• You can individually enable the **2.4 GHz** band for DCA and TPC, and the **5 GHz** band for DCA, TPC, and DBS. For the **5 GHz** band, if DCA and DBS are disabled and you enable DBS, DCA is also enabled.

• You can enable or disable the **6 GHz** band together for DCA and DBS RF settings. You can individually enable the **6 GHz** band for TPC.

• FRA is not supported for the **6 GHz** band.

Step 11 In the **Advanced** area, 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) If the individual channel numbers are not already displayed, 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) In the **Supported Data Rate** area, configure the following:

• 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 boxes in the **Mandatory Data Rates** area.

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

• **TPC Power Threshold**: Is the cutoff signal level used by RRM to determine whether to reduce the power of an AP. Use the **TPC Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmission power rates. The range is from -50 dBm through 80 dBm, and the default threshold is -70 dBm.

• **RX SOP Threshold (dBm)**: 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 Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 2.4-GHz band, the high threshold value is -79 dBm, the medium threshold value is -82 dBm, and the low threshold value is -85 dBm.

h) Under **Coverage Hole Detection**, configure the following:

Note   You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see Create a Model Config Design for RRM General Parameters. For more information about provisioning, see Provision Wireless Devices.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.

- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

i) Under **CLIENT LIMIT**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note   - If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7.1, the maximum client limit is 200.

- If the wireless controller is running Cisco IOS XE Release 17.7.1 or later and earlier than Cisco IOS XE Release 17.9.1, the maximum client limit is 400.

- If the wireless controller is running Cisco IOS XE Release 17.9.1 or later, the maximum client limit is 500.

j) Under **802.11ax**, configure the following spatial reuse parameters:

Note   802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.

- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.

- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.

- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

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

a) Check the **Zero Wait DFS** check box to allow APs with 5-GHz radio to switch to a new channel without any waiting time.

Note	Catalyst Center supports Zero wait DFS for Cisco Wireless Controllers running Cisco IOS XE Release 17.9.1 and later.

b) 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 a color-coded representation of channels that are available in the Unlicensed National Information Infrastructure (UNII) radio bands for the available channel widths.

You can select **DBS Max Width** only when DBS is enabled.

When you disable the DBS, Catalyst Center allows you to select the static channel width.

c) Set the **DCA Channel** 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**.

d) Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.

e) Click **Show Advanced** to view and select the individual DCA channel numbers.

- Check the **UNII-1 36-48** check box to include all channels, or check an individual check box.

- Check the **UNII-2 52-144** check box to include all channels, or check an individual check box.

- 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.

f) 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 **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.

g) 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**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.

h) In the **Tx Power Configuration** area, complete the following:

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

- Use the **TPC 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 through 80 dBm and the default threshold is -70 dBm.

- **RX SOP Threshold (dBm)**: 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 Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 5-GHz band, the high threshold value is -76 dBm, the medium threshold value is -78 dBm, and the low threshold value is -80 dBm.

i) Under **Coverage Hole Detection**, configure the following:

  Note You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see Create a Model Config Design for RRM General Parameters. For more information about provisioning, see Provision Wireless Devices.

  - In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.

  - In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

  - In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

  - In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

j) Under **CLIENT LIMIT**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

  Note
  - If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7.1, the maximum client limit is 200.

  - If the wireless controller is running Cisco IOS XE Release 17.7.1 or later and earlier than Cisco IOS XE Release 17.9.1, the maximum client limit is 400.

  - If the wireless controller is running Cisco IOS XE Release 17.9.1 or later, the maximum client limit is 500.

k) Under **802.11ax**, configure the following spatial reuse parameters:

  Note 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

  - Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.

  - In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

  - Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

  SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.

- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.

- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 13 In the **Advanced** area, click the **6 GHz** toggle button.

a) Use the **DBS Width** slider to set the minimum and maximum 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 a color-coded representation of channels that are available in the UNII radio bands for the available channel widths.

You can select **DBS Width** only when DBS is enabled.

b) Enable the **Enable PSC Enforcing** toggle button to allow Preferred Scanning Channel (PSC) enforcement.

PSC enforcement improves the connectivity of the 6-GHz devices by prioritizing the PSC-enabled channels.

Note If you enable PSC enforcement, the check boxes next to the non-PSC channels are dimmed and the check boxes next to the PSC channels are checked by default. If necessary, you can uncheck the check box next to the required PSC channel.

c) Set the **DCA Channel** to manage the following channel assignments:

- **UNII-5 1-93**: The channels available for the UNII-5 band are **1**, **5**, **9**, **13**, **17**, **21**, **25**, **29**, **33**, **37**, **41**, **45**, **49**, **53**, **57**, **61**, **65**, **69**, **73**, **77**, **81**, **85**, **89**, and **93**.

- **UNII-6 97-113**: The channels available for the UNII-6 band are **97**, **101**, **105**, **109**, and **113**.

- **UNII-7 117-185**: The channels available for the UNII-7 band are **117**, **121**, **125**, **129**, **133**, **137**, **141**, **145**, **149**, **153**, **157**, **161**, **165**, **169**, **173**, **177**, **181**, and **185**.

- **UNII-8 189-233**: The channels available for the UNII-8 band are **189**, **193**, **197**, **201**, **205**, **209**, **213**, **217**, **221**, **225**, **229**, and **233**.

d) Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.

e) Click **Show Advanced** to select the remaining DCA channel numbers.

- Check the **UNII-5 1-93** check box to include all channels, or check an individual check box.

- Check the **UNII-7 117-185** check box to include all channels, or check an individual check box.

- Check the **UNII-8 189-233** 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.

f) 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 **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

g) In the **Tx Power Configuration** area, configure the following.

- **Standard Power Service**: For APs with the standard power capability, compliance with FCC regulations requires the activation of Automatic Frequency Coordination (AFC). AFC uses the AP location and height data to determine the optimal channel and transmission power, ensuring noninterference with the licensed incumbent users on the 6-GHz band. You can use the Standard Power Service feature on Catalyst Center to activate AFC. By default, this feature is disabled. To enable this feature, click the **Standard Power Service** toggle button.

  This feature is applicable only for Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.12.3 or later. When this feature is disabled, the 6-GHz dual-power mode APs are restricted to operate only in the low-power indoor mode, and the standard-power mode only APs have the radios disabled completely.

Note	To ensure proper functioning of this feature, you must configure the AP height, AP height uncertainty, and external antenna cable length on the corresponding wireless controller. For the standard power-capable APs to operate on standard power, you must ensure that you select at least one supported DCA channel based on your country-specific regulations.

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

- Use the **TPC 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 through 80 dBm and the default threshold is -70 dBm.

- **RX SOP Threshold (dBm)**: 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 Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 6-GHz band, the high threshold value is -76 dBm, the medium threshold value is -78 dBm, and the low threshold value is -80 dBm.

h) Under **Coverage Hole Detection**, configure the following:

Note	You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see Create a Model Config Design for RRM General Parameters. For more information about provisioning, see Provision Wireless Devices.

   - In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.

   - In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

   - In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.

   - In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

i) Under **CLIENT LIMIT**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note	• If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7.1, the maximum client limit is 200.
	• If the wireless controller is running Cisco IOS XE Release 17.7.1 or later and earlier than Cisco IOS XE Release 17.9.1, the maximum client limit is 400.
	• If the wireless controller is running Cisco IOS XE Release 17.9.1 or later, the maximum client limit is 500.

j) Under **802.11ax**, configure the following multiple basic service set identifier (BSSID) and spatial reuse parameters:

- From the **6 GHz Discovery Frames** drop-down list, choose the required option from **None**, **Broadcast Probe Response**, and **FILS Discovery**.

  6-GHz discovery frames are needed if the **6 GHz** radio is the only operational radio. For more information about the 6-GHz discovery frames, click **Learn More**.

- In the **Broadcast Probe Response Interval (msec)** field, enter the broadcast probe response interval, in msec. The valid range is from 5 msec through 25 msec. The default value is 20 msec.

- Under **MULTI BSSID**, check the check boxes to enable the following parameters:

  - Downlink OFDMA

  - Uplink OFDMA

  - Downlink MU-MIMO

  - Uplink MU-MIMO

  - Target wake time

  - TWT Broadcast Support

Note	You must enable multiple BSSID in **Design** > **Feature Templates** > **Wireless** > **Dot11ax Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for Dot11ax, see Create a Model Config Design for Dot11ax Configuration. For more information about provisioning, see Provision Wireless Devices.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.

- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

  SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.

- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.

- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 14   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 an AI Radio Frequency Profile

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

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for Configuring AI Radio Frequency Profiles, on page 58.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **RF Profiles**.

Step 5   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 6   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 7   Click **Edit/View**.

Step 8   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 59.

Step 9   Click **Save**.

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.

Delete an AI Radio Frequency Profile

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

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for Configuring AI Radio Frequency Profiles, on page 58.

Step 1	From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.
Step 2	Click the **Wireless** tab.
Step 3	From the left hierarchy tree, choose **Global**.
Step 4	Click **RF Profiles**.
Step 5	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 6	To delete an AI RF profile, check the check box next to the AI RF profile that you want to delete.
Step 7	Click **Delete** and then click **Yes**.

> **Note** Catalyst Center does not allow you to delete an AI RF Profile which is already assigned to a building.

What to do next

If you delete an RF profile that is already provisioned on a wireless controller and AP, you must reprovision the wireless controller. Reprovisioning the AP is not necessary. For more information about provisioning a wireless controller, see Provision a Cisco Catalyst 9800 Series Wireless Controller.

Clone an AI Radio Frequency Profile

You can create a copy of an AI RF profile by cloning it. Cloning allows you to reuse the configurations of an existing AI RF profile for a new AI RF profile.

Step 1	From the top-left corner, click the menu icon and choose **Design** > **Network Settings**
Step 2	Click the **Wireless** tab.
Step 3	From the left hierarchy tree, choose **Global**.
Step 4	Click **RF Profiles**.
Step 5	Click the **AI RF Profile** tab.
Step 6	Check the check box next to the profile name that you want to clone.
Step 7	Click **Create a Clone**.
Step 8	In the **Profile Name** field of the **Create AI Radio Frequency Profile** window, enter a unique name for the profile.
Step 9	Edit the RF profile configurations as necessary. For more information, see Create an AI Radio Frequency Profile, on page 59.
Step 10	Click **Save**.

Configure AI-Enhanced RRM

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

Before you begin

Ensure that the prerequisites are met. For more information, see .

Step 1   From the top-left corner, click the menu icon and choose **Workflows** > **Configure AI-Enhanced RRM**.

Step 2   In the **Configure AI-Enhanced RRM** window, click **Let's Do it** to go directly to the workflow.

Step 3   In the **Task Name** field of the **Get Started** window, enter a task name.

Step 4   In the **Select Deployment Type** window, select the deployment type from the available options. The options are **Enable Without Device Provisioning** and **Enable with Device Provisioning**.

Step 5   In the **Select Locations to Enable AI-Enhanced RRM** 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 **Search** 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**, **Impacted Location**, **Primary WLC**, and **Secondary WLC** of the selected sites.

- **Selected Locations**: A location that is being enabled for the AI RF profile.

- **Impacted Locations**: A location that is being partially managed by the same wireless controller of the selected location.

- **Primary WLC**: The primary wireless controller assigned to the location. Click **Assign** to assign a wireless controller. It's mandatory to assign the primary wireless controller.

- **Secondary WLC**: The secondary wireless controller assigned to the impacted location. It's optional to assign a secondary wireless controller. Click **Assign** to open the **Secondary Wireless Controller** dialog box. Select the deployment type, choose a wireless controller from the **Wireless Controller** table, and click **Confirm**.

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

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

Step 6   In the **Assign AI RF Profile and Verify Tags** window, the **Building** table lists AI RF profiles based on **Location**, **Floors**, and **Current RF Profiles**.

    a)   In the **Building** table, choose an AI-enabled RF profile from the drop-down list under **Select the AI RF profile** for the specific location.

    b)   Click the three dots under the Action column to create a new AI RF profile or clone the existing RF profile.

    c)   You can also create an AI RF profile from the **Create a new AI RF Profile to apply** link in the **Assign AI RF Profile and Verify Tags** window. For more information, see Create an AI Radio Frequency Profile, on page 59.

Step 7   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 8   In the **Summary** window, review the **Task Details**, **Select Deployment Type**, **Select Locations to Enable AI-Enhanced RRM** and **Assign AI RF Profile and Verify Tags**.

Step 9   In the **Schedule Task** window, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.

- **Later**: Schedule the date and time and define the time zone of the deployment.

- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see Visibility and Control of Wireless Device Configurations.

Step 10   Click **Deploy**.

Step 11   (Optional) In the **Download a backup of current RF settings** dialog box, you can download a backup CSV file that contains the selected buildings' current RF configuration details. When you're ready, click **Confirm** to continue.

Tip   If you disable AI-Enhanced RRM later, you can use this backup CSV file to update the RF profile configurations. For more information, see Unassign a Location from an Existing AI RF Profile, on page 73.

Step 12   On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.

- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.

- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see Network Provisioning Prechecks.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 13   If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a.   On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b.   On the **Preview Configuration** window, review the device configurations.

For more information, see Visibility and Control of Wireless Device Configurations.

c.   Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.

- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note   You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

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

Ensure that the prerequisites are met. For more information, see Prerequisites for Configuring AI Radio Frequency Profiles, on page 58.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **RF Profiles**.

Step 5 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 6 Click the three dots under the **Action** column for an AI RF profile.

Step 7 From the drop-down list, choose **Assign Location**.

The **Manage Location Assignment** window opens.

Step 8 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 opens.

Step 9 Review the confirmation and click **Confirm** to assign the chosen sites to the AI-enabled RF profile.

Step 10 In the **Schedule Task** window, depending on the Visibility and Control of Configurations settings, choose an available option:

• **Now**: Immediately deploy the configurations.

• **Later**: Schedule the date and time and define the time zone of the deployment.

• **Generate configuration preview**: Review the configurations before deploying them.

If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see Visibility and Control of Wireless Device Configurations.

Step 11   Click **Deploy**.

Step 12   (Optional) In the **Download a backup of current RF settings** dialog box, you can download a backup CSV file that contains the selected buildings' current RF configuration details. When you're ready, click **Confirm** to continue.

> **Tip**   If you disable AI-Enhanced RRM later, you can use this backup CSV file to update the RF profile configurations. For more information, see Unassign a Location from an Existing AI RF Profile, on page 73.

Step 13   On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.

- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.

- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see Network Provisioning Prechecks.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 14   If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a.   On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b.   On the **Preview Configuration** window, review the device configurations.

   For more information, see Visibility and Control of Wireless Device Configurations.

c.   Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.

- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

> **Note**   You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d.   In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e.   Click **Submit**.

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

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. From the top-left corner, 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

Ensure that the prerequisites are met. For more information, see Prerequisites for Configuring AI Radio Frequency Profiles, on page 58.

Step 1	From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.
Step 2	Click the **Wireless** tab.
Step 3	From the left hierarchy tree, choose **Global**.
Step 4	Click **RF Profiles**.
Step 5	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 6	Click the three dots under the **Action** column for an AI RF profile.
Step 7	From the drop-down list, choose **Unassign Location**. The **Unassign AI RF Profile** window opens.
Step 8	Check the check box next to a site to unassign an AI RF profile.
Step 9	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 10	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 11 Click **Upload a CSV with RF settings back** to upload a backup of the RF settings from your local machine.

Step 12 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 13 Review the **Confirm RF Settings for Selected Locations** window and click **Confirm**.

Step 14 In the **Schedule Task** window, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.

- **Later**: Schedule the date and time and define the time zone of the deployment.

- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see Visibility and Control of Wireless Device Configurations.

Step 15 Click **Unassign**.

Step 16 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.

- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.

- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see Network Provisioning Prechecks.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 17 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

  For more information, see Visibility and Control of Wireless Device Configurations.

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.

- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

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. From the top-left corner, 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

Ensure that the prerequisites are met. For more information, see Prerequisites for Configuring AI Radio Frequency Profiles, on page 58.

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   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **RF Profiles**.

Step 5   Check the check box next to the basic RF profile name that you want to upgrade to an AI RF profile.

Step 6   From the **Action** drop-down list, choose **Upgrade to AI**.

Step 7   In the confirmation window, click **Yes**.

Step 8   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 59.

Create an AP Authorization List

Catalyst Center allows you to configure a list of authorized APs. Catalyst Center supports the following types of AP authorization:

- Local authorization uses the AP MAC address, serial number, or both for authorization against the local database.

- AAA authorization uses a list of AAA servers for authorization.

You can choose the AP authorization list while provisioning the Cisco Wireless Controller. Cisco Wireless Controllers respond only to requests from the APs that are present in the AP authorization list.

Note
- If both MAC address and serial number are required for AP authorization, ensure that both are added to the AP authorization list. If one of these AP entries isn't available in the AP authorization list provisioned for a wireless controller, the corresponding AP can't join the network.

- For a mesh AP (MAP), you must add the MAC address for AP authorization.

- For Cisco AireOS Wireless Controllers, Catalyst Center supports only the MAC address for AP authorization. If you configure both MAC address and serial number, only the MAC address is used for Cisco AireOS Wireless Controllers.

- For Cisco Catalyst 9800 Series Wireless Controllers, Catalyst Center supports the configuration of AP authorization lists only on the wireless controllers running Cisco IOS Release 17.5 and later.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **Security Settings**.

Step 5   Click the **AP Authorization List** tab.

Step 6   In the **AP Authorization List** table, click **Add**.

Step 7   In the **List name** field of the **AP Authorization List** slide-in pane, enter a name for the AP authorization list.

Step 8   To configure local authorization, do the following:

   a) In the **Local Auth** tab, check the **Configure Local Authorization** check box.

   b) In the **Type** area, choose an authorization type:

      • To use the AP MAC address for authorization, click **Mac Address**.

      • To use the AP serial number for authorization, click **Serial Number**.

   c) To enter the AP MAC address or serial number data, do one of the following:

      • To add the MAC address or serial number individually to the authorization list, click **Add**. In the **AP Entry** field, enter the data.

      • To upload the CSV file with the data, click **Upload**. In the dialog box, do the following:

        1. Drag and drop your CSV file into the drag and drop area. Alternatively, click **Choose a file** and browse to select your CSV file stored locally.

          Note   If you don't have a CSV file, click **Download** to download a CSV file that you can edit and upload.

        2. Click **Save**.

   d) (Optional) To use both the MAC address and serial number for authorization:

      1. Click **Mac Address**, and enter the AP MAC address data (8.c, on page 77).

      2. Click **Serial Number**, and enter the AP serial number data (8.c, on page 77).

Step 9   To configure AAA authorization, do the following:

   a) In the **AAA Auth** tab, check the **Configure AAA Authorization** check box.

   b) Based on the AP authorization requirement for the AAA server, do one of the following:

      • If the AAA server uses only the MAC address for AP authorization, check the **Authorize AP against MAC Address** check box.

      • If the AAA server uses only the serial number for AP authorization, check the **Authorize AP against Serial Number** check box.

      • If the AAA server uses both the MAC address and serial number for AP authentication, check both the **Authorize AP against MAC Address** and **Authorize AP against Serial Number** check boxes.

   c) To add AP entries to the AP authorization list, do one of the following:

      • Click the plus icon (+) next to the required AP entry.

      • Click the AP entry and click **Add Selected**.

        Note   To choose multiple AP entries, press **Shift**, click the AP entries, and click **Add Selected**.

      • To add all the AP entries to the AP authorization list, click **Add All**.

      You can use the **Search** field to filter the AP entries.

Step 10   Click **Save**.

Edit or Delete an AP Authorization List

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **Security Settings**.

Step 5   Click the **AP Authorization List** tab.

Step 6   In the **AP Authorization List** table, check the check box next to the authorization list name that you want to edit or delete.

- To edit the AP authorization list, click **Edit**. In the **AP Authorization List** slide-in pane, edit the configuration as necessary, and click **Save**. For more information, see .
- To delete the AP authorization list, click **Delete**, and then click **Yes**.

Create an Anchor Group

You can create anchor groups with up to three Cisco Wireless Controllers and set the priority for the anchors. You can add the following devices as anchors:

- Cisco Wireless Controllers that are managed by Catalyst Center.

- Cisco Wireless Controllers that are not managed by Catalyst Center (external wireless controllers).

Note   You must add at least one anchor to an anchor group.

Priority order of the anchors determines the traffic sharing across the anchors:

- Equal sharing: When the priority order of all the anchors is the same (for example, 1, 1, and 1).

- Partial sharing: When the priority order of more than one anchor is the same (for example, 1, 1, and 2).

- Sequential sharing: When the priority order of the anchors is sequential (for example, 1, 2, and 3).

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **Anchor Groups**.

The **Anchor Groups** window opens.

Step 5   In the **Anchor Group** table, click **Add**.

Step 6   In the **Anchor Group Name** field of the **Anchor Group** slide-in pane, enter the anchor group name.

Step 7   To add a managed wireless controller as an anchor, click **Add Managed WLC** and do the following in the **Add Managed WLC** dialog box:

a) Check the check box next to the name of the devices that you want to add as anchors.

   To search for a device, in the **Search Table** search field, enter either the partial name or the full name of the device and press **Enter**.

b) Click **Add**.

Step 8   (Optional) To add an external wireless controller as an anchor, click **Add External WLC** and do the following in the **Add External WLC** dialog box:

a) In the **Device Name** field, enter the device name.
b) From the **Device Series** drop-down list, choose a device series.
c) In the **Peer IP Address** field, enter the peer IP address.
d) (Optional) In the **NAT IP Address** field, enter the Network Address Translation (NAT) IP address.
e) In the **MAC Address** field, enter the MAC address of the device.
f) In the **Mobility Group Name** field, enter the mobility group name.
g) (Optional) In the **Hash** field, enter the hash for the Cisco Catalyst 9800 Series Wireless Controller.

   Note   This field is available for only the Cisco Catalyst 9800-CL Wireless Controllers.

h) Click **Add**.

Step 9   (Optional) To add an existing external wireless controller as an anchor, click **Add Existing External WLC** and do the following in the **Add Existing External WLC** dialog box:

a) Check the check box next to the name of the devices that you want to add as anchors.

   To search for a device, in the **Search Table** search field, enter either the partial name or the full name of the device and press **Enter**.

b) Click **Add**.

Step 10   (Optional) To set the priority for an anchor, from the **Priority Order** drop-down list, choose the priority for the anchor wireless controller.

Step 11   Click **Save**.

Edit or Delete an Anchor Group

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **Anchor Groups**.

Step 5   In the **Anchor Group** table, check the check box next to the anchor group that you want to edit or delete.

   • To edit the anchor group, click **Edit**. In the **Anchor Group** slide-in pane, configure the anchors and click **Save**. For more information, see .

• To delete the anchor group, click **Delete** and then click **Yes**.

AP Profiles

AP profiles consolidate the AP authentication settings for Plug and Play (PnP), Cisco Advanced Wireless Intrusion Prevention System (aWIPS), rogue management, and mesh networks. AP profiles allow you to manage and provision APs.

Catalyst Center provides a default AP profile for Cisco IOS XE devices and Cisco AireOS devices. You can edit the default AP profiles, but you can't delete them. Site tags and AP groups generated by Catalyst Center use the default AP profiles.

If your authentication method is EAP-Transport Level Security (EAP-TLS), which uses certificate-based authentication, you cannot use a subordinate CA certificate. With EAP-TLS authentication for AP profiles, you can only use a root CA certificate.

> ✎ **Note** When you upgrade to Release 2.3.7.x from an earlier version, by default, Catalyst Center doesn't push the default AP profile to the wireless controller. To update the default AP profile on the wireless controller, you must explicitly save it on the **AP Profiles** window. For more information, see Edit or Delete an AP Profile, on page 89.
>
> When you save the default AP profile, if there's a difference between the current wireless controller configuration and the AP profile configuration saved on Catalyst Center, Catalyst Center pushes the default AP profile to the wireless controller during subsequent reprovisioning.
>
> After saving the default AP profile, there's no option to prevent Catalyst Center from pushing the default AP profile to the wireless controller during reprovisioning.

You can also create custom AP profiles for Cisco IOS XE and Cisco AireOS devices. To assign an AP profile to a site, associate it with a wireless network profile.

Create an AP Profile for Cisco IOS XE Devices

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **AP Profiles**.

Step 5 In the **AP Profile** table, hover your cursor over **Add** and choose **AP Profile for IOS-XE**.

Step 6 In the **Create Access Point Profile** window, enter a name for the AP profile.

Step 7 (Optional) Enter a description for the AP profile.

Step 8 If this AP profile is for remote teleworker APs or Cisco OfficeExtend APs, check the **Remote Teleworker** check box.

You can enable or disable the **Remote Teleworker** check box only while creating the AP profile. You can't update this option for existing AP profiles.

Note   Remote teleworker-enabled AP profiles don't support the following settings:

- aWIPS application

- Rogue detection

- Mesh

- Power

Step 9   Configure the required settings in the followings tabs:

  a) **Management**: For more information, see Configure Management Settings for an AP Profile for Cisco IOS XE Devices, on page 81.

  b) **Security**: For more information, see Configure Security Settings for an AP Profile for Cisco IOS XE Devices, on page 82.

  c) **Mesh**: For more information, see Configure Mesh Settings for an AP Profile for Cisco IOS XE Devices, on page 83.

  d) **Power**: For more information, see Configure Power Settings for an AP Profile for Cisco IOS XE Devices, on page 84.

  e) **Additional**: For more information, see Configure Additional Settings for an AP Profile for Cisco IOS XE Devices, on page 85.

Step 10   Click **Save**.

Configure Management Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the following for an AP profile for Cisco IOS XE devices:

- Authentication settings to onboard APs securely during the PnP claim process. Based on the authentication settings configured at the global-level or site-level hierarchy in Catalyst Center, PnP pushes the 802.1x (Dot1x) supplicant and certificates when claiming an AP. The AP uses the 802.1x supplicant for authenticating with Cisco ISE.

- Authentication settings for day-*n* authentication of APs.

- Credentials for console access, SSH, and Telnet.

- Enabling Cisco Discovery Protocol (CDP) to make an AP discoverable to its neighboring devices.

Step 1   In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Management** tab.

Step 2   In the **Access Points Authentication** area, choose an authentication method.

Note   This authentication method is used during the AP PnP claim and day-*n* authentication. Changing the authentication method impacts the service of the APs onboarded through the PnP claim process. If you change the authentication method, perform a factory reset for the APs onboarded through PnP claim process. If an AP joins with a different Extensible Authentication Protocol (EAP) method, the EAP method changes based on the authentication method that you choose.

The following authentication methods are available:

- **NO-AUTH**: Default authentication method.

- **EAP-TLS**: EAP-Transport Level Security (EAP-TLS) uses certificate-based authentication.

- **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. EAP-PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol.

  If you choose **EAP-PEAP**, enter a username and password. Catalyst Center generates a certificate and applies it during the PnP claim process.

- **EAP-FAST**: EAP-Flexible Authentication through Secure Tunneling (EAP-FAST) 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 choose **EAP-FAST**, enter a username and password. Catalyst Center generates a certificate and applies it during the PnP claim process.

Step 3 In the **SSH and Telnet** area, configure the following:

a) (Optional) Click the **SSH** toggle button to configure the credentials for SSH.

b) (Optional) Click the **Telnet** toggle button to configure the credentials for Telnet.

c) In the **Username** field, enter the name used to authenticate the device.

  The username can't contain spaces or angle brackets (< >).

  Note   If you disable SSH and Telnet, the **Username** field is optional.

d) In the **Password** field, enter the password used to authenticate the device.

  Note   If you disable SSH and Telnet, the **Password** field is optional.

e) In the **Enable Password** field, enter the password to enable a higher privilege level in the CLI.

  Note   If you disable SSH and Telnet, the **Enable Password** field is optional.

Step 4 In the **Cisco Discovery Protocol (CDP) State** area, click the **CDP State** toggle button to enable or disable CDP.

What to do next

Configure the other necessary settings for the AP profile. For more information, see .

Configure Security Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the following for an AP profile for Cisco IOS XE devices:

- Cisco Advanced Wireless Intrusion Prevention System (aWIPS) and forensic capture to detect intrusion threats and mitigate them. Catalyst Center supports aWIPS for devices running Cisco IOS XE Release 17.3.1 or later.

- Rogue detection to detect the APs that are installed on the network without explicit authorization from a system administrator. Catalyst Center supports rogue detection for devices running Cisco IOS XE Release 17.4 or later.

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Security** tab.

Step 2 In the **aWIPS and Forensic Capture Enablement** area, configure the following:

a) Click the **aWIPS** toggle button to enable or disable aWIPS.

b) Click the **Forensic Capture Enablement** toggle button to enable or disable forensic capture.

Note You must enable the **aWIPS** toggle button to use the **Forensic Capture Enablement** toggle button.

Step 3 In the **Rogue Detection** area, configure following:

a) Click the **Rogue Detection** toggle button to enable or disable rogue detection.

b) In the **Minimum RSSI** field, enter the valid RSSI value. The valid range is from -128 to -70 dBm. The default value is -90 dBm.

c) In the **Transient Interval** field, enter a valid transient time interval in seconds. The valid transient interval ranges from 120 to 1800 seconds. The default value is 0.

d) In the **Report Interval** field, enter a valid report time interval in seconds. The valid report interval ranges from 10 to 300 seconds. The default value is 10 seconds.

Step 4 In the **Rogue Containment** area, click the **PMF Denial** toggle button to enable the containment for rogue AP doing Protected Management Frame (PMF).

Note **PMF Denial** is supported from IOS-XE version 17.12 and above.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP Profile for Cisco IOS XE Devices, on page 80.

Configure Mesh Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the mesh settings for an AP profile for Cisco IOS XE devices.

Before you begin

Ensure that you add the MAC address of the mesh access point (MAP) to the AP authorization list. For more information, see Create an AP Authorization List, on page 76.

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Mesh** tab.

Step 2 Click the **Mesh** toggle button.

Note If you disable the **Mesh** toggle button, the existing custom mesh settings are deleted, and the AP profile is associated with the default mesh profile on the device.

Step 3 (Optional) In the **Range - Root AP to Mesh AP (in feet)** field, enter the maximum range (in feet) from the root access points (RAP) to the MAPs in the network. The valid range is from 150 feet through 132000 feet.

Step 4 (Optional) To allow wireless client association over the backhaul radio, check the **Backhaul Client Access** check box.

Generally, the backhaul radio is a 5-GHz radio for most of the MAPs. The backhaul radio can carry both backhaul traffic and client traffic.

If you disable the **Backhaul Client Access** check box, Catalyst Center sends only backhaul traffic over the backhaul radio, and client association is only over the secondary radio or radios.

Step 5 (Optional) In the **RAP Downlink Backhaul** area, choose the required option.

If your country prohibits the use of **5 GHz**, choose **2.4 GHz**. Even if your country allows the use of **5 GHz**, consider using **2.4 GHz** because 2.4-GHz radio can cover larger mesh or bridge distances.

Note
- For a mesh AP, when you change the mesh role to RAP and provision the AP, the AP reboots. RAP downlink backhaul mesh settings are effective only after the reboot.

- When you change the RAP configuration from **5 GHz** to **2.4 GHz**, Catalyst Center propagates the update 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.

Step 6 (Optional) In the **Backhaul Data Rates** area, 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 AP. Backhaul creates a wireless connection between the APs. 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 7 (Optional) In the **Bridge Group Name** field in the **Bridge Group** area, enter a name of up to 10 characters for the bridge group.

A bridge group name controls the association of MAPs. By grouping radios, two networks on the same channel, but in different bridge group names can't communicate with one another. This setting is also useful if you have more than one RAP in your network in the same sector (area).

If you don't enter a bridge group name, Catalyst Center uses the **Default** bridge group name for the mesh profile.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP Profile for Cisco IOS XE Devices, on page 80.

Configure Power Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the following for an AP profile for Cisco IOS XE devices:

- AP power profile: If an AP doesn't receive the required power, it functions in a derated state based on the settings in the AP power profile. For more information, see Create an AP Power Profile, on page 89.

Note The power settings are applicable only for the Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later.

- Calendar power profile: You can create calendar power profiles for APs that are in power save mode. You can map multiple AP power profiles to different calendar schedules as required. Based on the configured schedule, Catalyst Center runs all the rules defined in the AP power profiles simultaneously.

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Power** tab.

Step 2 In the **AP Power Profile** area, from the **Select Value** drop-down list, choose a power profile.

(To create a power profile, click **Create New** and configure the parameters. For more information, see Create an AP Power Profile, on page 89.)

Step 3 In the **Calendar Power Profile** area, do the following:

a) To add a calendar power profile, click **Add**. In the **Add Calendar Power Profile** slide-in pane, do the following:

  1. From the **Select Power Profile** drop-down list, choose a power profile.

    To create a power profile, click **Create New** and configure the parameters. For more information, see Create an AP Power Profile, on page 89.

  2. Choose the recurrence frequency for applying the power profile rules to the APs:

    - **Daily**: Applies the power profile rules to APs daily.

    - **Weekly**: Applies the power profile rules to APs every week on the selected days. Click the required day to select it.

    - **Monthly**: Applies the power profile rules to APs every month on the selected dates. Click the required date to select it.

  3. Specify the start time and end time for the power profile rules.

  4. Click **Save**.

b) (Optional) To edit a power profile rule, check the check box next to the corresponding power profile name and click **Edit**. In the **Edit Power Profile** slide-in pane, edit the required parameters and click **Save**.

c) (Optional) To delete a power profile, check the check box next to the corresponding power profile name, click **Delete**, and then click **Yes**.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP Profile for Cisco IOS XE Devices, on page 80.

Configure Additional Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the following for an AP profile for Cisco IOS XE devices:

- Country code: Set the country code for the Rest of World (ROW) domain APs that don't have a country code configured already.

Note	The country code setting doesn't impact the APs that already have a country code configured.

- Time zone: Choose the time zone for the APs.

- Client limit: Specify the maximum number of allowed clients.

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Additional** tab.

Step 2 In the **Country Code** area, from the **Select Value** drop-down list, choose a country for ROW APs that don't have a country code configured.

Step 3 In the **Time Zone** area, choose one of the following options:

- **Not Configured**: APs operate in the UTC time zone.
- **Controller**: APs operate in the Cisco Wireless Controller time zone.
- **Delta from Controller**: APs operate in the offset time from the wireless controller time zone. Configure the following offset values:

  - **HH**: Enter the hour value. The valid range is from -12 through 14.

  - **MM**: Enter the minute value. The valid range is from 0 through 59.

Step 4 In the **Client Limit** area, enter a value for the maximum client limit. The valid range is from 0 through 1200.

What to do next

After configuring all the necessary settings for the AP profile, click **Save**. For more information, see Create an AP Profile for Cisco IOS XE Devices, on page 80.

Create an AP Profile for Cisco AireOS Devices

For Cisco AireOS devices, AP profiles group the AP-level parameters and configurations. AP profiles can be mapped to custom AP groups. When APs are provisioned, all APs under the corresponding AP group are configured with the settings available in the AP profile.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **AP Profiles**.

Step 5 In the **AP Profile** table, hover your cursor over **Add** and choose **AP Profile for AireOS**.

Step 6 In the **Create Access Point Profile** window, enter a name for the AP profile.

Step 7 (Optional) Enter a description for the AP profile.

Step 8 If this AP profile is for remote teleworker APs or Cisco OfficeExtend APs, check the **Remote Teleworker** check box.

You can enable or disable the **Remote Teleworker** check box only while creating the AP profile. You can't update this option for existing AP profiles.

Note Remote teleworker-enabled AP profiles don't support the following settings:

- Rogue detection

- Mesh

Step 9 Configure the required settings in the followings tabs:

a) **Management**: For more information, see Configure Management Settings for an AP Profile for Cisco AireOS Devices, on page 87.

b) **Security**: For more information, see Configure Security Settings for an AP Profile for Cisco AireOS Devices, on page 88.

c) **Mesh**: For more information, see Configure Mesh Settings for an AP Profile for Cisco AireOS Devices, on page 88.

Step 10 Click **Save**.

Configure Management Settings for an AP Profile for Cisco AireOS Devices

Use this procedure to configure the following for an AP profile for Cisco AireOS devices:

- Credentials for console access, SSH, and Telnet.

- Enable Cisco Discovery Protocol (CDP) to make the AP discoverable to its neighboring devices.

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for AireOS**), click the **Management** tab.

Step 2 In the **SSH and Telnet** area, configure the following:

a) (Optional) Click the **SSH** toggle button to configure the credentials for SSH.

b) (Optional) Click the **Telnet** toggle button to configure the credentials for Telnet.

c) In the **Username** field, enter the name used to authenticate the device.

Username can't contain spaces or angle brackets (< >).

Note If you disable SSH and Telnet, the **Username** field is optional.

d) In the **Password** field, enter the password used to authenticate the device.

Note If you disable SSH and Telnet, the **Password** field is optional.

e) In the **Enable Password** field, enter the password to enable a higher privilege level in the CLI.

Note If you disable SSH and Telnet, the **Enable Password** field is optional.

Step 3 In the **Cisco Discovery Protocol (CDP) State** area, click the **CDP State** toggle button to enable or disable CDP.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP Profile for Cisco AireOS Devices, on page 86.

Configure Security Settings for an AP Profile for Cisco AireOS Devices

Use this procedure to configure rogue detection for an AP profile for Cisco AireOS devices. Rogue detection allows you to detect the APs that are installed on the network without explicit authorization from a system administrator.

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for AireOS**), click the **Security** tab.

Step 2 In the **Rogue Detection** area, click the **Rogue Detection** toggle button to enable or disable rogue detection.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP Profile for Cisco AireOS Devices, on page 86.

Configure Mesh Settings for an AP Profile for Cisco AireOS Devices

Use this procedure to configure the mesh settings for an AP profile for Cisco AireOS devices.

Before you begin

Ensure that you add the MAC address of the MAP to the AP authorization list. For more information, see Create an AP Authorization List, on page 76.

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for AireOS**), click the **Mesh** tab.

Step 2 Click the **Mesh** toggle button.

Step 3 (Optional) In the **RAP Downlink Backhaul** area, click the radio button next to the required option.

If your country prohibits the use of **5 GHz**, choose **2.4 GHz**. Even if your country allows the use of **5 GHz**, consider using **2.4 GHz** because 2.4-GHz radio can cover larger mesh or bridge distances.

Note
- For a mesh AP, when you change the mesh role to RAP and provision the AP, the AP reboots. RAP downlink backhaul mesh settings are effective only after the reboot.
- When you change the RAP configuration from **5 GHz** to **2.4 GHz**, Catalyst Center propagates the update 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.

Step 4 (Optional) In the **Bridge Group Name** field in the **Bridge Group** area, enter a name of up to 10 characters for the bridge group.

A bridge group name controls the association of MAPs. By grouping radios, two networks on the same channel, but in different bridge group names, can't communicate with one another. This setting is also useful if you have more than one RAP in your network in the same sector (area).

If you don't enter a bridge group name, Catalyst Center uses the **Default** bridge group name for the mesh profile.

What to do next

After configuring all the necessary settings for the AP profile, click **Save**. For more information, see Create an AP Profile for Cisco AireOS Devices, on page 86.

Edit or Delete an AP Profile

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **AP Profiles**.

Step 5 In the **AP Profile** table, check the check box next to the AP profile that you want to edit or delete.

- To edit the AP profile, click **Edit**. In the **Edit Access Point Profile** slide-in pane, edit the configuration as necessary, and click **Save**. For more information, see Create an AP Profile for Cisco AireOS Devices, on page 86 and Create an AP Profile for Cisco IOS XE Devices, on page 80.
- To delete the AP profile, click **Delete**, and then click **Yes**.

Create an AP Power Profile

You can create AP power profiles for Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later. Assign an AP power profile to APs by associating it to an AP profile. You can define multiple rules for an AP power profile and specify the sequences of rules.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **Power Profile**.

Step 5 In the **AP Power Profile** table, click **Add**.

Step 6 In the **Power Profile Name** field of the **Create Power Profile** slide-in pane, enter a name for the AP power profile.

Step 7 (Optional) In the **Description** field, enter a description for the AP power profile.

Step 8 Click **Add** to create a rule for the AP power profile.

Step 9 In the **Rule** dialog box, configure the following:

a) From the **Interface** drop-down list, choose a type of interface.

b) From the **Interface ID** drop-down list, choose an interface ID.

Note If only one interface ID is available, Catalyst Center automatically selects the available interface ID.

c) From the **Parameter** drop-down list, choose a parameter.

Note	If only one parameter is available, Catalyst Center automatically selects the available parameter.

d) From the **Parameter Value** drop-down list, choose a parameter value.

Note	If only one parameter value is available, Catalyst Center automatically selects the available parameter value.

e) Click **Add**.

Step 10 (Optional) To create another rule for the AP power profile, repeat Step 8, on page 89 and Step 9, on page 89.

Step 11 (Optional) To update the sequence of a rule in the **Rules** table, click the corresponding ⠿ icon, and drag and drop the rule to the required position.

Step 12 Click **Save**.

What to do next

Associate the AP power profile with an AP profile. For more information, see Create an AP Profile for Cisco IOS XE Devices, on page 80.

Edit or Delete an AP Power Profile

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **Power Profile**.

Step 5 In the **AP Power Profile** table, check the check box next to the AP power profile that you want to edit or delete.

- To edit the AP power profile, click **Edit**. In the **Edit Power Profile** slide-in pane, edit the description, rules, and sequence as necessary, and click **Save**. For more information, see Create an AP Power Profile, on page 89.
- To delete the AP power profile, click **Delete**, and then click **Yes**.

Provision a Cisco Sensor SSID for Nonfabric Deployment

- The Catalyst Center sensor uses the Cisco sensor provisioning Service Set Identifier (SSID) to communicate with the Plug and Play (PnP) server and obtain day-zero 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 Catalyst Center.

- The following platforms support the Cisco sensor provisioning SSID:

  - Cisco AireOS Wireless 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 Series Wireless Controllers for Cloud

• Cisco Catalyst 9800 Series Wireless Controller

• Cisco AireOS Wireless Controller

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

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   Click **SSIDs**.

Step 4   From the **SSID** table, hover over ⊕Add ∨ and choose **Enterprise**.

The **Wireless SSID** workflow opens.

Step 5   In the **Basic Settings** window, click the **Sensor** field and then click **Next**.

Note   The parameters for the SSID are automatically populated and cannot be edited.

Step 6   In the **Associate SSID to Profile** window, from the left pane, select a profile and do the following:

a)   Under **Fabric**, select **Yes**.
b)   Click **Associate Profile**.
c)   Click **Next**.

Note   If you don't have a profile, click **Add Profile** and configure the profile settings.

Step 7   In the **Summary** window, review the configuration settings.

Step 8   Click **Save**.

Step 9   From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

Step 10   Check the check box next to a device and from the **Actions** drop-down list, 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** is displayed at the bottom-right corner.

Step 14   (Optional) After deploying the configuration on the devices, the **Task Progress** bar displays the progress of the ongoing provisioning task under **Activities** > **Tasks** (which you can view by clicking the task name).

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 Catalyst Center.

Step 1 From the top-left corner, click the menu icon and choose **Assurance** > **Settings** > **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:

a) Check the check box of the backhaul configuration.

b) Hover your cursor over the **Actions** drop-down list and choose **Edit**.

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

a) Check the check box of the backhaul configuration.

b) Hover your cursor over the **Actions** drop-down list and choose **Delete**.

Create an Antenna Radio Profile

Catalyst Center supports the C-ANT9104 antenna, which integrates with the Cisco Catalyst 9130AXE Unified Access Point to provide dual 5-GHz 4x4 radios with high gain, steerable, and switchable functions. With Catalyst Center, you can select the beam steering (direction) for the antennae. The following modes are available:

• Wide beam

• Narrow beam

• Narrow beam with 10 degrees of tilt

• Narrow beam with 20 degrees of tilt

You can configure wide and narrow beamwidth states for installations where high user density, precise pattern control, and long-range performance in the 5-GHz band are required.

The beam steering configuration is available for antenna combinations ABCD (left antennae) and EFGH (right antennae). The antenna pattern names are set based on the selected beam. You can visualize the heatmaps on Catalyst Center floor maps.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 Click **Antenna Radio Profiles**.

Step 5 In the **Antenna Radio Profile** table, click **Add**.

Step 6 Configure wide and narrow beam steering for the antennae in the **Antenna Radio Profile** slide-in pane:

• In the **Radio Profile Name** field, enter a unique name for the radio profile.

• From the **Beam Steer Mode** drop-down list, choose a beam steering mode.

Step 7   Click **Save**.

The new antenna radio profile is displayed in the **Antenna Radio Profile** table.

Edit or Delete an Antenna Radio Profile

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose **Global**.

Step 4   Click **Antenna Radio Profiles**.

Step 5   In the **Antenna Radio Profile** table, check the check box next to the antenna radio profile name that you want to edit or delete.

- To edit the antenna radio profile, click **Edit**. In the **Antenna Radio Profile** slide-in pane, edit the configuration as necessary, and click **Save**. For more information, see Create an Antenna Radio Profile, on page 93.
- To delete the antenna radio profile, click **Delete** and then click **Yes**.

About Cisco Connected Mobile Experiences Integration

Catalyst Center supports the integration of on-premises Cisco 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 Catalyst 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 large enterprise, you can assign CMX at the floor level.

Note   CMX should be anonymized for security purposes.

Create Cisco CMX Settings

Before you begin

Make sure that CMX is configured with a valid SSL/TLS certificate. See the CMX 10.5 SSL certificate installation procedure.

Step 1   From the top-left corner, click the menu icon and choose **System** > **Settings**.

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

The **Cisco Spaces/CMX Servers** window opens.

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.

- **Username**: Enter the CMX web GUI username.

   Note   To assign a CMX server to a site, building, or floor, you must have Write permission on **Network Hierarchy**. For more information, see the "Catalyst Center User Role and Permissions" section in the *Cisco Catalyst Center Administrator Guide*.

- **Password**: Enter the password credentials.

   Note   Make sure that CMX is reachable.

Step 5   Click **Add**.

The connection status is shown in three stages as follows:

- **Initiating Connection**: Verifies connectivity to the server.

- **Establishing Trust**: Establishes trust to the CMX server. The CMX server must have a valid SSL/TLS certificate configured to establish trust. If the certificate is not yet stored in Catalyst Center Trusted Certificates, you will be prompted to **Accept** the certificate to continue.

- **Connecting CMX Server**: Validates the user credentials provided.

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   From the left hierarchy tree, choose either **Global** or the required area, building, or floor.

Step 9   Click **Cisco Spaces/CMX Servers**.

Step 10   In the **Cisco Spaces/CMX Servers** section, from the **Location Settings** drop-down list, choose the CMX server.

Step 11   Click **Save**.

The **Create CMX Settings** window opens.

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, Catalyst Center starts querying the CMX for the client location and displays the location on the floor map.

Step 12   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 13   If the CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** window, hover your cursor over the ellipsis ●●● next to the building or floor on which you made the changes in the left hierarchy tree, and then choose **Sync: Cisco Spaces/CMX Servers** to push the changes manually.

Step 14 To edit the CMX server details or delete a CMX server, do the following:

a) From the top-left corner, click the menu icon and choose **System** > **Settings**.

b) From the **External Services** section, click **Cisco 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 Connection Failure

• Check if you have uploaded the CMX certificate to **System** > **Settings** > **Trusted Certificates**.

• After upgrading to Catalyst Center, edit the CMX connection details to reestablish the connection by reviewing and accepting the CMX SSL/TLS certificate.

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 Catalyst 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 Catalyst 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 Catalyst 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 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 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.

Catalyst Center integrates with Cisco Spaces to provide you with the exact location of wireless clients, rogue APs, and interferers on Catalyst Center floor maps. Depending on your requirements, you can create Cisco Spaces settings either at the global level or at the site, building, or floor level.

When you assign Cisco Spaces at the global level or at the site, building, or floor level, Catalyst Center automatically sends the floor map configuration to Cisco Spaces. Similarly, any time you save a change to a floor map, Catalyst Center automatically synchronizes the floor map configuration with Cisco Spaces. Synchronization occurs serially; one floor map doesn't start to synchronize until the previously configured floor map synchronization is completed. So, if multiple floors are configured in close succession, it can take a long time to complete.

You can also trigger a manual synchronization of floor maps to Cisco Spaces. However, we recommend that you use discretion when using this option. When a manual synchronization is triggered, the Catalyst Center

GUI hangs until the synchronization has completed and Catalyst Center returns a response to indicate the synchronization success or failure. Additionally, if an automatic synchronization is already in progress when a manual synchronization is triggered, the manual synchronization won't start until the automatic synchronization is done. While waiting for the automatic synchronization to end and during the manual synchronization itself, the Catalyst Center GUI hangs. In these cases, depending on the number of floor maps contained in the site, the Catalyst Center GUI could hang for a long period.

Therefore, you should use the manual synchronization option only in the unlikely event that the automatic map synchronization to Cisco Spaces fails due to a network issue or a temporary service outage. The manual synchronization option should not be used on a consistent basis to update floor map changes with to Cisco Spaces.

To integrate Cisco Spaces with Catalyst Center, see the "Catalyst Center Integration" section in the *Cisco Spaces Configuration Guide*.

Assign Cisco Spaces to Sites

To monitor sites using Cisco Spaces, you need to assign Cisco Spaces to the site that you want to monitor.

Before you begin

Integrate Cisco Spaces with Catalyst Center. For details, see the *Cisco Spaces Configuration Guide*.

Step 1   From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2   Click the **Wireless** tab.

Step 3   From the left hierarchy tree, choose either **Global** or the area, building, or floor to which you want to assign Cisco Spaces.

Step 4   Click **Cisco Spaces/CMX Servers**.

Step 5   In the **Cisco Spaces/CMX Servers** window, from the **Location Services** drop-down list, select a site.

Step 6   Click **Save**.

Catalyst Center deploys the site information to Cisco Spaces automatically.

Monitor Sites Using Cisco Spaces

You can monitor sites using Cisco Spaces.

Before you begin

• Integrate Cisco Spaces with Catalyst Center. For details, see the *Cisco Spaces Configuration Guide*.

• Assign Cisco Spaces to the site that you want to monitor.

Step 1   In the Catalyst Center GUI, click the menu icon and choose **Design** > **Network Hierarchy**.

Step 2   From the left hierarchy tree, choose either **Global** or the area, building, or floor that you want Cisco Spaces to monitor.

Step 3   To confirm that Cisco Spaces is operational, verify that the Cisco Spaces/CMX status icon displays on the floor that you want to monitor, as shown in the following figure.
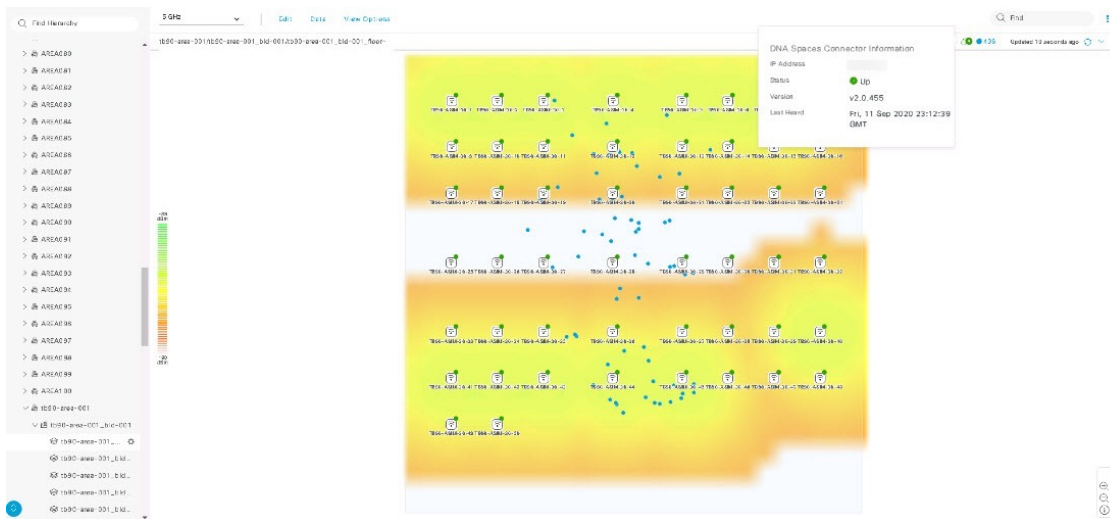
Configure a FlexConnect VLAN

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 From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose the required site:

- **Global**: Configures the VLAN at the global level for all sites.

- Area, building, or floor: Configures the VLAN at the chosen level only.

Step 4 Click **FlexConnect Settings**.

Child sites inherit the FlexConnect settings from the parent site. Inherited settings are displayed with an inherit icon next to the setting; hover your cursor over the icon to see the origin of the setting. You can use the **Delete** option to delete a setting and the **Inherit** option to inherit settings from the parent site, if it hasn't been inherited.

Step 5 In the **Native VLAN ID** field, enter a value for the VLAN ID. The valid range is from 1 through 4094.

Step 6 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 number of VLAN mappings that you can define for a FlexConnect deployment is 16. However, for Cisco Catalyst 9800 Series Wireless Controllers, this number includes default WLAN VLANs and VLANs pushed by AAA.

Step 7   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 23 and Create SSIDs for a Guest Wireless Network, on page 34.

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 a secure and scalable wireless LAN.

Note   All APs are configured and shipped as MAPs. To use an AP as a RAP, you must reconfigure 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.
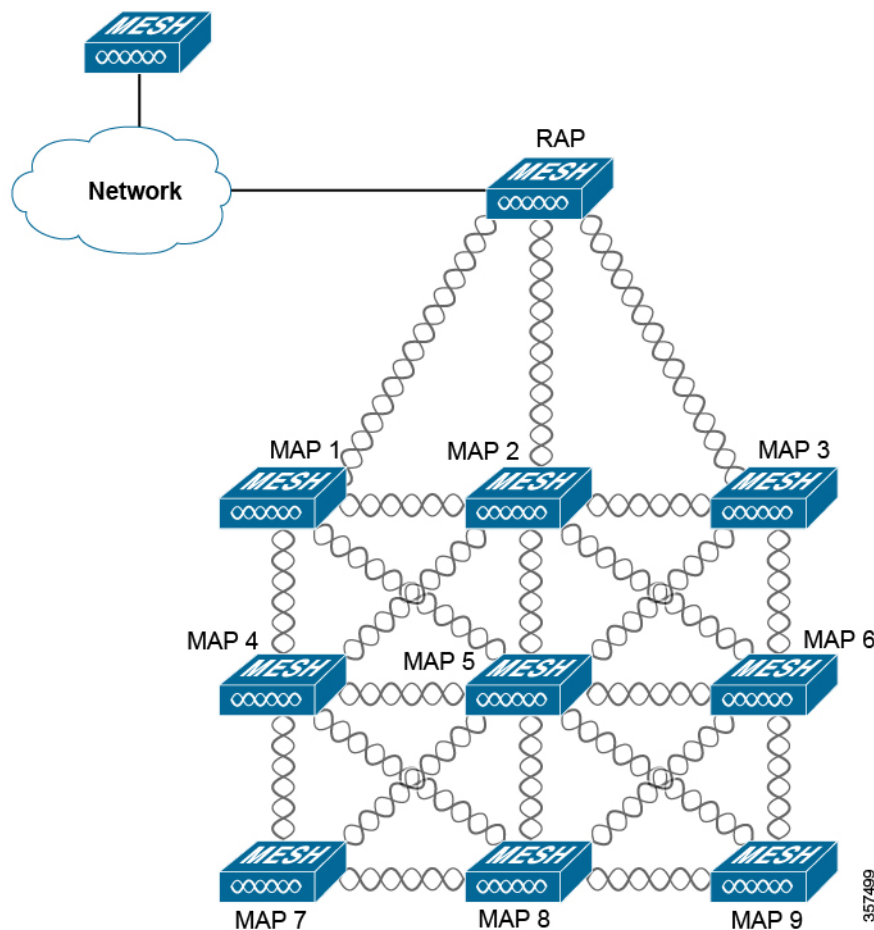
Both MAPs and RAPs can provide WLAN client access. However, typically, the location of RAPs is often not suitable for providing client access.

Some buildings have onsite controllers to terminate Control and Provisioning of Wireless Access Point (CAPWAP) sessions from the MAPs, but it's not a mandatory requirement because CAPWAP sessions can be backhauled to a wireless controller over a WAN.

In a Cisco wireless backhaul network, traffic can be bridged between MAPs and RAPs. This traffic can come 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 must configure a list of authorized APs in the wireless controller. Wireless controllers respond only to requests from the MAPs that are present in its authorization list.

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

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

These settings are configured for the global site in the **Create AP Profile** window. For more information, see Configure Mesh Settings for an AP Profile for Cisco IOS XE Devices, on page 83 and Configure Mesh Settings for an AP Profile for Cisco AireOS Devices, on page 88.

AP Configuration

If you have existing APs that you want to use in the 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 APs.

After an AP is configured for Bridge or Flex+Bridge mode, the **AP 360** window shows the mesh configuration. At this point, you must provision the APs with the new configuration. For more information, see Provision a Cisco AP—Day 1 AP Provisioning.

> **Note** For Cisco Catalyst 9800 Series Wireless Controllers, during bulk mesh AP provisioning across floors, we recommend that you don't update the following configurations simultaneously on already provisioned APs:
>
> - Mesh role on the AP and mesh configuration (**Bridge Group Name**, **Range - Root AP to Mesh AP (in feet)**, **Backhaul Client Access**) on the AP profile
> - Mesh role on the AP and AP profile or flex profile mapping with the site tag
>
> If you simultaneously update these configurations during bulk mesh AP provisioning, you must do one of the following:
>
> - Reprovision the Cisco Catalyst 9800 Series Wireless Controller. APs reboot after reprovisioning the wireless controller. After the reboot is complete, you can reprovision the APs with the required mesh role change.
> - Reprovision one of the APs that has the updated mesh configuration. The other APs with the updated mesh configuration also reboot. After the reboot is complete, you can reprovision the APs with the required mesh role change.

Configure a Certificate Revocation Check

Use the following steps to configure a certificate revocation check for the controller certificate.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Security and Trust**.

Step 2 From the left hierarchy tree, choose a site, building, or floor.

Step 3 In the **Revocation Check** drop-down list, **Revocation - Check: CRL None** is selected by default.

Step 4 To skip the revocation check, choose **Revocation - Check: None** and click **Save**.