

# Provision Wireless Devices


- Wireless device provisioning overview, on page 1
- About wireless devices and country codes, on page 1
- Role-based access control, on page 3
- Prerequisites for provisioning a Cisco AireOS Controller, on page 3
- Provision a Cisco AireOS Controller, on page 4
- Provision Cisco APs on day 1, on page 11
- Enable ICMP ping on APs in FlexConnect mode, on page 15
- Day-zero workflow for Cisco AireOS Mobility Express APs, on page 16
- Configure and provision a Cisco Catalyst 9800 Series Wireless Controller, on page 18
- Configure and provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches, on page 48
- Renew AP LSC for a wireless device, on page 55
- Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 56
- Inter-Release Controller Mobility introduction, on page 350
- Prerequisites for provisioning a Meraki device, on page 353
- Provision a Meraki device, on page 353
- Provision remote teleworker devices, on page 355


## Wireless device provisioning overview

These sections provide information about how to provision various Cisco wireless devices.

## About wireless devices and country codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation within that regulatory domain (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Catalyst Center provisions controllers with country codes according to the site they are assigned. In the case of controllers, they can be assigned to more than one site. So, they can be assigned more than one country

code. During provisioning, Catalyst Center assigns sites to the controller along with the sites' country codes. For example, a controller that manages both India and US sites is assigned the IN and US country codes.

When access points are provisioned, they are assigned to a floor. If the access point is a ROW AP, Catalyst Center gets the country code for the site and assigns it to the AP. Any additional APs on the same floor are assigned the same country code.

During AP provisioning with an RF profile selected, out of all the DCA Channels configured on the RF profile, only the supported channels as per the country code are considered for Dynamic Channel Assignment (DCA). You can see the list of unsupported DCA channels in the AP preprovision summary step of the AP provision workflow on Catalyst Center.

The country code information is displayed on the **Device 360** window for controllers and access points.

For a complete list of country codes supported per product, see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.

# Configure regulatory activation for wireless controllers

Ensure APs associated with a wireless controller obtain a valid country code so their radios become operational.

Regulatory activation is required when APs are unable to obtain a country code through standard geolocation or proximity methods. If a country code is not available, the AP radios are not operational.Catalyst Center uses the regulatory activation file to resolve the country code on these APs.

You can configure regulatory activation for Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches in nonfabric deployments.

Use this procedure to configure regulatory activation for wireless controllers to resolve the country code on associated APs that have not been able to obtain a country code.

**Before you begin**

- Obtain the regulatory activation file, in JSON format, from the Meraki dashboard.
- Ensure that the wireless controller is running Cisco IOS XE Release 17.18.1 or later.
- Ensure that the wireless controller is reachable in the inventory.

**Procedure**

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Select the required wireless controller.

**Step 3** From the **Actions** drop-down list, choose **Provision** > **Regulatory Activation**.

**Step 4** In the **Regulatory Activation** slide-in pane, configure the regulatory activation file using one of these options.

| If you want to... | Then... |
|---|---|
| upload a new file | **a.** Use one of these options:<br>• Drag and drop the file into the drag and drop area.<br>• Click **Choose a file**, browse to the location of the file, and click **Open**.<br>**b.** Click **Upload File**. |
| use an existing file that was uploaded earlier | click **Use existing file**. |

**Step 5** Under **Uploaded AP Summary**, review the summary of APs and country codes extracted from the uploaded file.

**Step 6** Click **Deploy**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

# Role-based access control

Role-based access control in Catalyst Center allows you to define the capabilities and the permissions that a user has access to. Before provisioning wireless devices, ensure you have access to the sites and devices where you want to provision, along with the necessary permissions to perform provisioning.

For more information, see User profile roles and permissions.

# Prerequisites for provisioning a Cisco AireOS Controller

- Make sure that you have defined the global network settings before provisioning a Cisco Wireless Controller, including:
  - Network servers, such as AAA, DHCP, and DNS.

    For more information, see Configure global network servers.
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS.

    For more information, see Add global CLI credentials, Add global SNMPv2c credentials, Add global SNMPv3 credentials, and Add global HTTPS credentials.
  - IP address pools.

    For more information, see Configure IP address pools.

- Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles.

**Note** When you upgrade from an earlier release:

- For WPA3-Enterprise SSIDs, Catalyst Center enables the Dot1x-SHA256 authentication key management settings for the SSIDs.
- For WPA2-WPA3-Enterprise SSIDs, Catalyst Center enables both Dot1x and Dot1x-SHA256 authentication key management settings for the SSIDs.

This configuration might change the intended configuration for the Cisco AireOS Wireless Controllers and wireless controllers running Cisco IOS XE Release 17.6 or earlier. You can update the **Auth Key Management** settings for the SSIDs before reprovisioning the wireless controllers.

For more information, see Configure global wireless settings.

- Make sure that you have the wireless controller in your inventory. If not, use the **Discovery** feature to discover the controller.
- Make sure that the wireless controller is added to a site. For more information, see Assign an unprovisioned device to a site.
- You cannot reuse any pre-existing VLANs on devices. Provisioning fails if Catalyst Center pushes the same VLAN that already exists on the device.
- You cannot make any configuration changes to the wireless controller that is being managed by the Catalyst Center manually. You must perform all configurations from the Catalyst Center GUI.

# Provision a Cisco AireOS Controller

### Before you begin

Ensure that the prerequisite is met. For more information, see Prerequisites for provisioning a Cisco AireOS Controller, on page 3.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window display with the discovered devices listed.

**Step 2** Expand the **Global** site in the left pane, and select the site, building, or floor that you're interested in.

The available devices in the chosen site display in the **Inventory** window.

**Step 3** In the **Devices** table, click the **Search** field. In the **Quick Filters** tab, do these steps:

a) For **Device Family**, click **Wireless Controllers** to get the list of wireless controllers that are discovered.

b) For **Reachability**, click **Reachable** to get the list of wireless controllers that are discovered and reachable.
c) Click **Apply**.

**Step 4** Check the check box next to the device name that you want to provision.

**Step 5** From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window displays.

**Step 6** Click **Choose a site** to assign a site for the wireless controller.

**Step 7** In the **Add Sites** window, check the check box next to the site name to associate the wireless controller, and click **Save**.

**Step 8** Click **Apply**.

**Step 9** Click **Next**.

The **Configuration** window displays.

**Step 10** Select a role for the wireless controller: **Active Main WLC** or **Guest Anchor WLC**.

**Step 11** Click **Select Primary Managed AP Locations** to select the managed AP location for the wireless controller.

**Step 12** In the **Managed AP Location** window, check the check box next to the site name. You can either select a parent site or the individual sites. If you select a parent site, the children under that parent site are automatically selected.

**Note** Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that site. One wireless controller can manage only one site.

**Step 13** Click **Save**.

**Step 14** (Optional) Check the **AP Authorization List** check box to choose the authorization list for AP authorization, and do these tasks:

**Note** This check box is displayed only if an AP authorization list is available. For more information about the AP authorization list, see Create an AP authorization list.

- From the **AP Authorization List Name** drop-down list, choose an AP authorization list. Based on the content of the AP authorization list, Catalyst Center displays a message indicating the corresponding primary authorization type and failback mechanism.
- (Optional) To view the entries for the selected AP authorization list, click **View Entries**.
- If the wireless controller manages both mesh and nonmesh APs, Catalyst Center displays the **Authorize Only Mesh Access Points** and **Authorize All Access Points** check boxes.

  To enable authorization for only mesh APs, check the **Authorize Only Mesh Access Points** check box.

  To enable authorization for all APs, check the **Authorize All Access Points** check box.

**Step 15** Under **Interface and VLAN Configuration**, click **+ Add** and configure the interface and VLAN details for an active main wireless controller.

Interface and VLAN configuration is applicable for nonfabric wireless controller provisioning only.

The **Configure Interface and VLAN** window displays.

**Step 16** From the **Interface Name** drop-down list, choose the interface name.

**Note** An info icon ( ⓘ ) is displayed next to the additional interfaces. For more information about additional interfaces, see Configure additional interfaces for a network profile.

**Step 17** In the **VLAN ID** field, enter a value for the VLAN.

**Step 18** In the **Interface IP Address** field, enter a value for the interface IP address.

**Step 19** In the **Interface Net Mask (in bits)** field, enter the subnet mask for the interface.

**Step 20** In the **Gateway IP Address** field, enter the gateway IP address.

**Step 21** From the **LAG/Port Number** drop-down list, choose the link aggregation or the port number.

**Step 22** Click **OK**.

**Step 23** (Optional) For a guest anchor wireless controller, change the VLAN ID configuration by changing the **VLAN ID** under **Assign Guest SSIDs to DMZ site**.

**Step 24** Click **Next**.

The **Feature Templates** window displays.

**Step 25** In the **Devices** pane, you can either search for a feature template by entering its name in the **Find** field, or expand the device and select a feature template.

The selected feature template displays in the right pane.

**Step 26** Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the feature template.

You can't edit all the configurations at this step.

**Step 27** After making the necessary changes, click **Apply**.

**Step 28** Click **Next**.

The **Advanced Configuration** window displays, which is where you can enter the values for predefined template variables.

**Step 29** Search for the device or the template in the **Devices** panel.

**Step 30** Enter a value for the predefined template variable in the **wlanid** field.

**Step 31** Click **Next**.

**Step 32** In the **Summary** step, review the device details, and click **Next** to provision the device.

**Step 33** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Note**

- When you provision the wireless controller, Catalyst Center pushes the configuration to the wireless controller and configures it based on the network intent. During the reprovisioning, if there are any out-of-band configurations on the wireless controller that are a part of the network intent or conflicting with the configurations being pushed by Catalyst Center, Catalyst Center overwrites the out-of-band configurations on the wireless controller with the network intent configuration.

  For all the configurations that are supported through the network intent on Catalyst Center, we recommend that you use them instead of out-of-band configurations.

- 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).

**Step 34** On the **Tasks** window, monitor the task deployment.

**Step 35** Provision the secondary controller.

**Step 36** The **Status** column in the **Device Inventory** window shows `SUCCESS` after a successful deployment.

After provisioning, if you want to make any changes, click **Design**, change the site profile, and provision the wireless controller again.

**Step 37** After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

**Step 38** In the **Device Inventory** window, click **See Details** in the **Provision Status** column to get more information about the network intent or to view a list of actions that you need to take.

**Step 39** Click **See Details** under **Device Provisioning**.

**Step 40** Click **View Details** under **Deployment of network intent**, and click the device name.

**Step 41** Expand the **Configuration Summary** area to view the operation details, feature name, and the management capability.

The configuration summary also displays any errors that occurred while provisioning the device.

**Step 42** Expand the **Provision Summary** area to view details of the exact configuration that is sent to the device.

# Configure Cisco Wireless Controller high availability

Cisco Wireless Controller high availability (HA) can be configured through Catalyst Center. Currently, both the formation and breaking of wireless controller HA is supported; switchover options are not supported.

## Prerequisites for configuring Cisco Wireless Controller high availability

- The Discovery and Inventory features of wireless controller 1 and wireless controller 2 must be successful. The devices must be managed.
- The service ports and the management ports of wireless controller 1 and wireless controller 2 must be configured.
- The redundancy ports of wireless controller 1 and wireless controller 2 must be physically connected.
- The management address of wireless controller 1 and wireless controller 2 must be in the same subnet. The redundancy management address of wireless controller 1 and wireless controller 2 must also be in the same subnet.

- Manually configure this boot variables on the wireless controller:

```
config t
boot system bootflash::<device_iosxe_image_filename>
config-register 0x2102

show boot.  (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102
```

## Configure Cisco Wireless Controller HA

### Procedure

**Step 1** From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

**Step 2** Check the check box next to the wireless controller name that you want to configure as the primary controller.

**Step 3** From the **Actions** drop-down list, choose **Provision** > **Configure WLC HA**.

The **High Availability** slide-in pane displays.

**Note** A warning is displayed at the top of the pane if the wireless controller that you selected isn't assigned to a site. Catalyst Center doesn't push the telemetry configuration to the wireless controller until it's assigned to a site.

By default, the chosen wireless controller becomes the primary controller and the **Primary WLC** field is disabled.

**Step 4** Enter the **Redundancy Management IP** and the **Peer Redundancy Management IP** address in the respective text boxes.

The IP addresses used for redundancy management IP and peer redundancy management IP should be configured in the same subnet as the management interface of the wireless controller. Ensure that these IP addresses are unused IP addresses within that subnet range.

**Step 5** From the **Select Secondary WLC** drop-down list, choose the secondary controller.

**Note** When you choose the secondary controller, based on the wireless management interface IP subnet of the primary controller, the redundancy management IP is auto populated, and an **i** icon displays at the top of the **High Availability** window, along with this message:

Ensure that the Redundancy Management IP and Peer Redundancy Management IP aren’t assigned to any other network entities. If the IPs are in use, change the IP accordingly and configure.

**Step 6** Click **Configure HA**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

**Step 9** When the task is deployed, the HA configuration is initiated in the background using the CLI commands. First, the primary wireless controller is configured. On success, the secondary wireless controller is configured. After the configuration is completed, both wireless controllers reboot. This process may take up to 2.5 minutes to complete.

**Step 10** To verify the HA configuration:

a) On the **Provision** > **Inventory** window, click the device that you configured as an HA device.
A dialog box with high-level device information opens.

b) In the dialog box, click **View Details**.

c) Click the **Wireless Info** tab.

The **Redundancy Summary** tab displays the **Sync Status** as **In Progress**. When Catalyst Center finds that HA pairing succeeded, the **Sync Status** changes to **Complete**.

This process is triggered by the inventory poller or manual resynchronization. By now, the secondary wireless controller (wireless controller 2) is deleted from Catalyst Center. This flow indicates a successful HA configuration on the wireless controller.

## What happens during or after the high availability process is complete

1. Cisco wireless controller 1 and wireless controller 2 are configured with redundancy management, redundancy units, and SSO. The wireless controllers reboot in order to negotiate their role as active or standby. Configuration is synced from active to standby.
2. On the **Show Redundancy Summary** window, you can see these configurations:
   - SSO is enabled.
   - The wireless controller is active.
   - The wireless controller is in hot standby.
3. The management port of the active wireless controller is shared by both the controllers and will be pointing to the active controller. The user interface, Telnet, and SSH on the standby wireless controller will not work. You can use the console and service port interface to control the standby wireless controller.

## Commands to configure and verify high availability

Catalyst Center sends commands to configure Cisco Wireless Controller HA.

Catalyst Center sends the commands to wireless controller 1, including:

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Catalyst Center sends the commands to wireless controller 2, including:

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

Enter these commands to verify the HA configuration from the wireless controller:

- To check HA-related details: **config redundancy mode sso**
- To check the configured interfaces: **show redundancy summary**

# Disable high availability configured device in the existing deployment

The Catalyst Center Disable HA feature is supported on Cisco Catalyst 9800 Series Wireless Controllers and Cisco AireOS Wireless Controllers.

### Before you begin

Ensure that the HA device in the existing deployment is configured outside of Catalyst Center.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window is displayed with the discovered devices listed.

**Step 2** Check the check box next to the name of the wireless controller that has the HA feature that you want to disable.

**Step 3** From the **Actions** drop-down list, choose **Provision** > **Configure WLC HA**.

The **High Availability** slide-in pane display.

**High Availability** slide-in pane shows the **Redundancy Summary** of selected wireless controller configured from outside Catalyst Center.

**Step 4** Click **Disable HA**.

**Step 5** In the **Warning** dialog box, click **OK**.

**Step 6** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 7** On the **Tasks** window, monitor the task deployment.

**Step 8** After the task deploys, a success message displays at the bottom of the window indicating that the HA feature has been successfully disabled for the selected wireless controller.

# Provision Cisco APs on day 1

Use the procedure to provision APs.

### Before you begin

- Make sure that you have Cisco APs in your inventory. If not, use the Discovery feature to discover APs. For more information, see Discover Your Network.
- Make sure that you enable the required licenses for the APs on the **License Manager** window. For more information, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
- If you add new AP zones or SSIDs, you must reprovision the wireless controller. For more information, see Provision a Cisco AireOS Controller, on page 4 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 40.
- If you update the AP zone configurations, you must reprovision the wireless controller. For more information, see Provision a Cisco AireOS Controller, on page 4 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 40.
- If you're using N+1 HA and modify any nonflex SSIDs that are already provisioned on the primary and secondary controllers to flex SSIDs (or conversely), make sure that the states of WLANs are consistent across both the primary and secondary controllers on the corresponding site.

  For example, *SSID1* is configured on a network profile as flex SSID, provisioned on both the primary and secondary controllers, and later modified as nonflex SSID. If you reprovision only the primary controller without reprovisioning the secondary controller, *SSID1* becomes nonflex SSID on the primary controller but remains flex SSID on the secondary controller. If you provision an AP on a site shared by both the primary and secondary controllers, the provisioning fails. To ensure consistency, you must reprovision the secondary controller. When you reprovision the secondary controller, *SSID1* changes to nonflex SSID on the secondary controller too and both controllers have the same state for *SSID1* before provisioning the AP.
- For ROW APs, we recommend that you create an AP profile with the necessary country code and configure custom site tags. For more information, see Configure additional settings for an AP profile for Cisco IOS XE devices and Add AP groups, flex groups, site tags, and policy tags to a network profile.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

**Step 2** Check the check box next to the APs that you want to provision.

You can choose up to 500 APs simultaneously.

**Step 3** From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

**Step 4** If you chose APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue with device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box and choose different APs. |

**Step 5** In the **Assign Site** step, configure the required parameters.

a) Click **Choose a floor** and assign an AP to the site.
b) In the **Choose a floor** slide-in pane, click the floor where the AP resides and click **Save**.
c) Click **Next**.

**Note** Catalyst Center doesn't configure this site as the AP location during AP provision. You can configure the AP location using the **Configure Access Points** workflow. For more information, see Configure APs.

**Step 6** In the **Configuration** step, configure the required parameters.

a) Click **Advanced Configuration** to configure antenna radio profiles on antenna slots.

**Note** Advanced configuration is supported on Cisco Catalyst 9130AXE Unified Access Points with Cisco Catalyst 9800 Series Wireless Controller software release 17.6 or later. Global tri-radio mode is enabled on the wireless controller and configured during AP provisioning.

For information about antenna radio profile, see Create an antenna radio profile.

b) Configure the beam selection value for AP radio slots from the **Slot 1** and **Slot 2** drop-down lists.
c) Click **Save**.
d) From the **AP Zone Name** drop-down list, choose an AP zone.

**Note** This drop-down list is enabled only when AP zones are added to the network profile for the site.

If you choose an AP zone, the RF profile is inherited from the AP zone configuration.

e) From the **RF Profile** drop-down list, use the default settings or choose a different value from the list.

The default RF profile is the custom profile that you marked as default under the **Design** > **Network Settings** > **Wireless** > **RF Profiles** > **Basic RF Profile** tab.

**Note** This drop-down list is disabled if you choose an AP zone from the **AP Zone** drop-down list.

f) In the **Mesh Role** drop-down list, choose **Root** or **Mesh**.

For information about wireless mesh networks, see About wireless mesh networks.

g) Click **Next**.

**Step 7** In the **Summary** step, review the device details, and click **Next** to provision the AP.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

**Step 10** You're prompted with a message that the creation or modification of an AP group is in progress and then a message that APs will reboot after provisioning. Click **OK**.

The **Last Sync Status** column in the **Inventory** window shows `SUCCESS` for a successful deployment.

# Migrate APs from a Wireless Controller to another Wireless Controller

Use this procedure to migrate APs from one wireless controller to another wireless controller with the same floors in the network hierarchy.

### Before you begin

- Ensure that the old wireless controller (for example, *WC1*) is provisioned with the required sites (for example, *Building-1* with *Floor-1*, *Floor-2*, and *Floor-3)* as the primary-managed AP location.
- Ensure that the APs that need to be migrated are provisioned on the floors managed by the old wireless controller (for example, *Building-1*/*Floor-1*, *Building-1*/*Floor-2*, *Building-1*/*Floor-3* managed by *WC1*).

### Procedure

**Step 1** Add a new building and floor to the network hierarchy (for example, *Building-New* with *Floor-New*). For more information, see Add, edit, and delete a building and Add, edit, and delete a floor.

**Step 2** Create a wireless network profile and assign it to the newly added floor (*Floor-New*). For more information, see Create network profiles for wireless.

**Step 3** Reprovision the old wireless controller with the newly added floor (*Floor-New*) as the primary-managed AP location and remove the old sites (*Floor-1*, *Floor-2*, and *Floor-3*). For more information, see Provision a Cisco AireOS Controller, on page 4 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 40.

**Step 4** Provision the new wireless controller (for example, *WC2*) with the old sites (*Floor-1*, *Floor-2*, and *Floor-3*) as the primary-managed AP locations. For more information, see Provision a Cisco AireOS Controller, on page 4 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 40.

**Step 5** Use the **Configure Access Points** workflow to change the primary wireless controller name and IP address. In the **Configure AP Parameters** window of this workflow, do these steps:

a) Check the **High Availability** check box.
b) From the **Select Primary Controller Name** drop-down list, choose the new wireless controller (*WC2*).
c) In the **Primary Controller IP Address** field, enter the IP address of the new wireless controller (IP address of *WC2*).

For more information, see Configure APs.

**Step 6** Do these steps to ensure that the APs have joined the new wireless controller (*WC2*):

a) From the main menu, choose **Provision** > **Inventory**.
b) Click the **Access Points** device family button at the top of the **Inventory** window.
c) Hover your cursor over the **Focus** drop-down list, and choose **Inventory**.
d) Under the **Associated WLC IP** column, check the IP address of the corresponding wireless controller for the APs.

If this column isn't displayed, click the gear icon at the top-right corner of the window and customize the table settings to display the column. For more information, see Display information about your inventory.

**Note** If the AP is flapping and assigned with the AUTO_INV_EVENT_SYNC_DISABLED or INV_EVENT_SYNC_DISABLED tag, automatic synchronization of events on the AP is disabled. After the underlying cause of the AP flapping is resolved, we recommend that you perform a manual synchronization to display the most current AP details. Alternatively, wait for the next scheduled synchronization to update the AP information.

**Step 7** Reprovision the APs to deploy the latest configuration. For more information, see Provision Cisco APs on day 1, on page 11.

# Reset APs

Using the Factory Reset feature, you can clear the configurations on the APs and reset them to the default configuration. After the AP configurations are cleared, the APs reboot.

**Important** Resetting an AP disrupts the network connectivity for all the associated clients.

### Before you begin

Ensure that the APs are reachable.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Inventory**.
The **Inventory** window displays the list of discovered devices.

**Step 2** In the **Devices** table, click the **Access Points** device family button to display the list of available APs.

**Step 3** Check the check box next to the APs that you want to reset.

You can select up to 100 APs for factory reset.

**Step 4** From the **Actions** drop-down list, choose **Provision** > **Factory Reset**.
The **Factory Reset** slide-in pane opens.

**Step 5** Under **Factory Reset**, choose one of these options:

- **Clear all configuration**: Clears all the configurations on the AP and resets it to the default configuration.
- **Clear all configuration except static IP**: Clears all the configurations on the AP, except the static IP configuration.

**Step 6** Under **Schedule Task**, do these steps:

a) Choose one of these options:

- **Now**: Immediately reset the APs.
- **Later**: Schedule the AP reset for a later date or time.

b) (Optional) In the **Task Name** field, update the task name.

c) If you chose **Later**, do these tasks:

- Under **Start Date/Time**, specify a start date and time for the task.
- From the **Time Zone** drop-down list, choose a time zone for the task.

**Step 7** To view the APs selected for reset, expand the **Selected Devices** drop-down list.

**Step 8** Click **Apply**.

To view the status of AP reset, go to the **Activities** > **Tasks** window and open the relevant work item.

# Enable ICMP ping on APs in FlexConnect mode

You can enable Internet Control Message Protocol (ICMP) ping on APs that are in FlexConnect mode and in an unreachable state. Catalyst Center uses the ICMP to ping FlexConnect APs that are in unreachable state every 5 minutes to enhance reachability and then updates the reachability status in the **Inventory** window.

### Procedure

**Step 1** From the main menu, choose **System** > **Settings** > **Device Settings** > **ICMP Ping**.

**Step 2** Check the **Enable ICMP ping for unreachable access points in FlexConnect mode** check box to enable the ICMP ping.

**Step 3** Click **Save**.

This success message displays: `ICMP Ping status updated successfully`.

Catalyst Center starts pinging FlexConnect APs that are disassociated from Cisco Wireless Controllers but are reachable. You can view the reachability status in the **Inventory** window.

**Step 4** To view the reachability status, choose **Provision** > **Inventory**.

**Step 5** The **Reachability** column shows **Ping Reachable** when the device is reachable by the ICMP ping.

# Day-zero workflow for Cisco AireOS Mobility Express APs

### Before you begin

The Cisco Mobility Express wireless network solution comprises at least one 802.11ac Wave 2 Cisco Aironet Series access point with an in-built, software-based wireless controller managing other APs in the network. The AP acting as the wireless controller is referred to as the *primary AP*. The other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as *subordinate APs*.

- Design your network hierarchy with sites, buildings, floors, and so on. For more information, see Create, edit, and delete a site, Add, edit, and delete a building, and Add, edit, and delete a floor.
- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS at the global level. The credentials that are defined at the global level are inherited by the sites. For more information, see Add global CLI credentials, Add global SNMPv2c credentials, and Add global SNMPv3 credentials.
- Create WLANs, interfaces, and RF profiles.
- Configure the DHCP server with Option #43 or Option #60. This is the IP address of the Catalyst Center Plug and Play server. Using this IP address, the APs contact the PnP server and download the configuration.
- Make sure that you have Mobility Express APs in the inventory. If not, discover them using the Discovery feature. For more information, see Discover your network using CDP, Discover your network using an IP address range or CIDR, and About Inventory.
- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

### Procedure

**Step 1** The Cisco Mobility Express contacts the DHCP server and connects to the Catalyst Center Plug and Play server.

**Step 2** The DHCP server allocates the IP address with Option #43, which is the IP address of the Catalyst Center Plug and Play server.

**Step 3** The Mobility Express AP starts the PnP agent and contacts the PnP server.

**Note** If you have a set of Mobility Express APs in the network, they go through an internal protocol. The protocol selects one Mobility Express AP, which will be configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.

**Step 4** Find the unclaimed AP in the **Provision** > **Network Devices** > **Plug and Play** tab.

The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.

You must wait for the **Onboarding Status** to become **Initialized**.

**Step 5** To claim the AP, check the check box next to the AP device name.

**Step 6** Choose **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window displays.

**Step 7** In the **Site Assignment** window, choose a site from the **Site** drop-down list.

Claiming the selected AP to this particular site also applies the associated configurations.

**Step 8** Click **Next**.

**Step 9** To configure a device, click the device name in the **Configuration** window.

**Step 10** In the **Configuration for device name** window, assign the static IP details for the device:

- **Management IP**
- **Subnet Mask**
- **Gateway**

**Step 11** Click **Save**.

**Step 12** Click **Next**.

The **Summary** window is displayed.

**Step 13** Click **Claim** in the **Summary** window.

After the Mobility Express AP is claimed, the configured IP address is assigned to the Mobility Express AP.

The claimed device, which is an AP, and the wireless controller are now available under **Provision** > **Device Inventory** > **Inventory**.

**Step 14** (Optional) Add devices in bulk from a CSV file.

For more information, see Add devices in bulk.

When you bulk import Mobility Express APs through a CSV file, all the Mobility Express APs appear on the **Devices** > **Plug and Play** window. Based on the VRRP protocol, only one Mobility Express AP among the imported ME APs becomes the primary AP. The remaining APs become subordinate APs. After claiming the primary AP, you don't need to claim the subordinate APs. Catalyst Center does not clear the subordinate APs from the **Plug and Play** window. You must delete those subordinate APs manually from the **Devices** > **Plug and Play** window.

**Step 15** To provision the Cisco Wireless Controller, see Provision a Cisco AireOS Controller, on page 4.

# Configure and provision a Cisco Catalyst 9800 Series Wireless Controller

## Cisco Catalyst 9800 Series Wireless Controller overview

The Cisco Catalyst 9800 Series Wireless Controller is the next generation of wireless controllers built for intent-based networking. The Cisco Catalyst 9800 Series Wireless Controller is Cisco IOS XE based and integrates the RF excellence from Aironet with the intent-based networking capabilities of Cisco IOS XE to create the best-in-class wireless experience for your organization.

The Cisco Catalyst 9800 Series Wireless Controller is built on a modular operating system and uses open, programmable APIs that enable automation of day-zero and day-*n* network operations.

The Cisco Catalyst 9800 Series Wireless Controller is available in multiple form factors:

- Catalyst 9800-40 Wireless Controller.
- Catalyst 9800-80 Wireless Controller.
- Catalyst 9800-CL Cloud Wireless Controller: Deployable on private cloud (ESXi, KVM, Cisco ENCS, and Hyper-V) and manageable by Catalyst Center.
- Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches, Catalyst 9400 Series Switches, and Catalyst 9500H Series Switches.
- Cisco Catalyst 9800-L Wireless Controller: Provides seamless software updates for small- to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network.

This table lists the supported virtual and hardware platforms for the Cisco Catalyst 9800 Series Wireless Controller:

| Platform | Description |
|---|---|
| Cisco Catalyst 9800-80 Wireless Controller | Supports up to 6000 access points and 64,000 clients.<br>Supports up to 80 Gbps throughput and occupies a 2-rack unit space.<br>Modular wireless controller with up to 100-GE uplinks and seamless software updates. |
| Cisco Catalyst 9800-40 Wireless Controller | A fixed wireless controller with seamless software updates for mid-sized organizations and campus deployments.<br>Supports up to 2000 access points and 32,000 clients.<br>Supports up to 40 Gbps throughput and occupies a 1-rack unit space.<br>Provides four 1-GE or 10-GE uplink ports. |

| Platform | Description |
|---|---|
| Cisco Catalyst 9800-CL Cloud Wireless Controller | Cisco Catalyst 9800-CL Cloud Wireless Controller can be deployed in a private cloud or a public cloud as Infrastructure as a Service (IaaS).<br>Cisco Catalyst 9800-CL Cloud Wireless Controller is the next generation of enterprise-class virtual wireless controllers built for high availability and security.<br>A virtual form factor of Cisco Catalyst 9800-CL Cloud Wireless Controller for private cloud supports ESXi, KVM, Cisco ENCS, and Hyper-V hypervisors. |
| Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches | Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches bring the wired and wireless infrastructure together with consistent policy and management.<br>This deployment model supports only Cisco SD-Access, which is a highly secure solution for small campuses and distributed branches. The embedded controller supports access points (APs) only in Fabric mode. |
| Cisco Catalyst 9800-L Wireless Controller | Cisco Catalyst 9800-L Wireless Controller provides seamless software updates for small to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network.<br>• Cisco Catalyst 9800-L Copper Series Wireless Controller (9800-L-C RJ45)<br>• Cisco Catalyst 9800-L Fiber Series Wireless Controller 9800-L-F SFP) |

This table lists the host environments supported by the Cisco Catalyst 9800 Series Wireless Controller:

| Host Environment | Software Version |
|---|---|
| VMware ESXi | • VMware ESXi vSphere 6.0<br>• VMware ESXi vSphere 6.5[1]<br>• VMware ESXi vCenter 6.0<br>• VMware ESXi VCenter 6.5 |
| KVM | • Linux KVM based on Red Hat Enterprise Linux 7.1 and 7.2<br>• Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS |
| NFVIS | Cisco ENCS 3.8.1 and 3.9.1 |

[1] Installing the .ova file of C9800-CL using ESXi vSphere does not work. This is not limited to the C9800 ova but affects other products. Cisco and VMware are actively working to fix the issue. Contact your Cisco account representative to see if the problem is fixed. There are issues specific to VMware 6.5 and C9800-CL OVA file deployment in which deployment fails with the warning "A required disk image was missing" and the error "Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files." To install C9800-CL on VMware ESXi 6.5, do one of these tasks: 1) Install the .iso file of C9800-CL using the ESXi embedded GUI (ESXI 6.5 client version 1.29.0 is tested and required). 2) Install the .ova file of C9800-CL using the OVF tool.

This table lists the Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) versions supported in Catalyst Center:

**Note** Cisco Enterprise NFVIS devices support the N-1 to N upgrade path only. For example, upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 3.12.x only is supported. Upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 4.1.x is not supported.

| Cisco Enterprise NFVIS version | Enterprise network compute system device platform | Notes |
|---|---|---|
| 4.1.2<br>4.1.1<br>3.12.3<br>3.11.3<br>3.11.2<br>3.11.1 | ENCS 5400<br>UCS-E<br>UCS-C | Catalyst Center supports these NFVIS upgrade paths: NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2.<br>Cisco Enterprise NFVIS 3.12.1 is not supported on any versions of Catalyst Center.<br>Upgrade to Cisco Enterprise NFVIS 3.12.1 from Cisco Enterprise NFVIS 3.11.x using Catalyst Center is not supported.<br>Upgrade to Cisco Enterprise NFVIS 3.12.2 from Cisco Enterprise NFVIS 3.12.1 using Catalyst Center is not supported.<br>Upgrade to Cisco Enterprise NFVIS 3.12.2 from 3.11.2 is supported using Catalyst Center.<br>Cisco Enterprise NFVIS 3.12.2 is supported on Catalyst Center. |
| 3.12.2<br>3.11.3<br>3.11.2<br>3.11.1 | ENCS 5100 | Cisco 5100 ENCS does not support Cisco Enterprise NFVIS 3.10.x. |

# Configure a Cisco Catalyst 9800 Series Wireless Controller in Catalyst Center

1. Install Catalyst Center.

   For more information, see the Cisco Catalyst Center Installation Guide.

2. For information on software image upgrade, see Software image upgrade support for Cisco Catalyst 9800 Series Wireless Controller, on page 24.

3. Log in to the Catalyst Center GUI and verify that the applications you need are in the **Running** state.

   From the main menu, choose **System Settings** > **Software Updates** > **Installed Apps**.

4. Integrate Cisco Identity Services Engine with Catalyst Center. After integration, any devices that Catalyst Center discovers along with relevant configurations and data are pushed to Cisco ISE.

5. Discover the Cisco Catalyst 9800 Series Wireless Controller.

   You must enable NETCONF and set the port to 830 to discover the Cisco Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

For more information, see Discover your network using CDP or Discover your network using an IP address range or CIDR.

You must add the wireless management IP address manually.

**Note** On the Cisco Catalyst 9800 Series Wireless Controller, you must configure a static IP address for the wireless management interface to prevent provisioning failure.

While performing discovery using the Cisco Discovery Protocol (CDP) or an IP address range in the **Discovery** window, choose **Use Loopback** from the **Preferred Management IP** drop-down list to specify the device's loopback interface IP address.

6. Make sure that the discovered devices appear in the **Device Inventory** window and are in the **Managed** state.

   For more information, see About Inventory and Display information about your inventory.

   You must wait for the devices to move to a **Managed** state.

7. To verify the Assurance connection with the Cisco Catalyst 9800 Series Wireless Controller, use these commands:

   - **#show crypto pki trustpoints | sec DNAC-CA**

     ```
     Trustpoint DNAC-CA
         Subject Name:
         cn=kube-ca
               Serial Number (hex): 00E***************
         Certificate configured.
     ```

   - **#show crypto pki trustpoints | sec sdn-network**

     ```
     Trustpoint sdn-network-infra-iwan:
         Subject Name:
         cn=sdn-network-infra-ca
             Serial Number (hex): 378***************
         Certificate configured.
     ```

   - **#show telemetry ietf subscription all**

     ```
     Telemetry subscription brief

       ID               Type        State       Filter type
       ------------------------------------------------------
       1011             Configured  Valid       tdl-uri
       1012             Configured  Valid       tdl-uri
       1013             Configured  Valid       tdl-uri
     ```

   - **#show telemetry internal connection**

     ```
     Telemetry connection

     Address Port Transport State Profile
     ------------------------------------------------------------
     IP address 25103 tls-native Active sdn-network-infra-iwan
     ```

   - **#show network-assurance summary**

```
Network-Assurance                       : True
Server Url                              : https://10.***.***.***
ICap Server Port Number                 : 3***
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

8. Configure a TACACS server while configuring authentication and policy servers.

   Configuring TACACS is not mandatory if you have configured the username locally on the Cisco Catalyst 9800 Series Wireless Controller.

9. Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

   You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Catalyst Center.

   To import and upload an existing network hierarchy, see Import your site hierarchy to Catalyst Center.

   To create a new network hierarchy, see Create, edit, and delete a site and Add, edit, and delete a building.

10. Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

    For more information, see Work with APs on a floor map.

11. Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network. You can add a TACACS server while adding a AAA server.

    For more information, see Network settings overview, Configure global network servers, and Add AAA server.

12. Create a wireless radio frequency profile with the parent profile as custom.

    For more information, see Create a wireless radio frequency profile.

13. Create IP address pools at the global level.

    Catalyst Center uses IP address pools to automate the configuration and deployment of SD-Access networks.

    To create an IP address pool, see Configure IP address pools.

    You must reserve an IP address pool for the building that you are provisioning. For more information, see Reserve IP Address Pools.

14. Create enterprise and guest wireless networks. Define the global wireless settings once; Catalyst Center then pushes the configurations to various devices across geographical locations.

    Designing a wireless network is a two-step process. First, you must create SSIDs, and then associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

**Note** When you upgrade from an earlier release:

- For WPA3-Enterprise SSIDs, Catalyst Center enables the Dot1x-SHA256 authentication key management settings for the SSIDs.
- For WPA2-WPA3-Enterprise SSIDs, Catalyst Center enables both Dot1x and Dot1x-SHA256 authentication key management settings for the SSIDs.

This configuration might change the intended configuration for the Cisco AireOS Wireless Controllers and wireless controllers running Cisco IOS XE Release 17.6 or earlier. You can update the **Auth Key Management** settings for the SSIDs before reprovisioning the wireless controllers.

For more information, see Create SSIDs for an enterprise wireless network and Create SSIDs for a guest wireless network. For information about other wireless settings, see Configure global wireless settings.

15. Configure the backhaul settings. For more information, see Manage backhaul settings.
16. In the **Policy** window for the Cisco Catalyst 9800 Series Wireless Controller, do this configuration:
    - Create a virtual network. The virtual network segments your physical network into multiple logical networks.
    - Create a group-based access control policy and add a contract. For more information, see Create group-based access control policy.
17. Configure high availability.

    For more information, see Configure high availability for the Cisco Catalyst 9800 Series Wireless Controller, on page 25.
18. Provision the Cisco Catalyst 9800 Series Wireless Controller with the configurations added during the design phase.

    For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 40.
19. Configure and deploy application policies on the Cisco Catalyst 9800 Series Wireless Controller.

    For more information, see Create an application policy, Deploy an application policy, and Edit an application policy.

**Note** You must provision Cisco Catalyst 9800 Series Wireless Controller devices before deploying an application policy.

For Cisco Catalyst 9800 Series Wireless Controller devices, two different policies with different business relevance for two different SSIDs do not work. The last deployed policy always takes precedence when you are setting up relevance.

For Cisco Catalyst 9800 Series Wireless Controller devices, changing the default business relevance for an application does not work in FlexConnect mode.

You can apply an application policy only on a nonfabric SSID.

# Software image upgrade support for Cisco Catalyst 9800 Series Wireless Controller

### Before you begin

- Discover the Cisco Catalyst 9800 Series Wireless Controller.

  Enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller. NETCONF enables wireless services on the controller and provides a mechanism to install, manipulate, and delete the configuration of network devices.

  For more information, see Discover your network using CDP, or Discover your network using an IP address range or CIDR.

- Make sure that the devices appear in the device inventory and are in the **Managed** state.

  For more information, see About Inventory and Display information about your inventory.

### Procedure

**Step 1** From the main menu, choose **Design** > **Image Repository**.

The **Inventory** window displays with the discovered devices listed.

**Step 2** Import the Cisco Catalyst 9800 Series Wireless Controller software image from your local computer or from a URL.

For more information, see Import a software image.

**Step 3** Assign the software image to a device family.

For more information, see Manage software image assignment for a device family.

**Step 4** You can mark a software image as Golden by clicking the star for a device family or a particular device role.

For more information, see Mark a software image as standard.

**Step 5** Provision the software image.

From the main menu, choose **Provision** > **Device** > **Inventory**.

**Step 6** In the **Inventory** window, check the check box next to the Cisco Catalyst 9800 Series Wireless Controller whose image you want to upgrade.

**Step 7** From the **Actions** drop-down list, choose **Software Image** > **Image Update**.

For more information, see Provision a software image.

# Configure high availability for the Cisco Catalyst 9800 Series Wireless Controller

### Before you begin

Configuring high availability (HA) on the Cisco Catalyst 9800 Series Wireless Controller involves these prerequisites:

- Both the Cisco Catalyst 9800 Series Wireless Controllers are running the same software version and have the active software image on the primary wireless controller.
- The service ports and management ports of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured.
- The redundancy ports of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are physically connected.
- Preconfigurations such as interface configurations, route addition, ssh line configurations, and NETCONF-YANG configurations are completed on the Catalyst 9800 Series Wireless Controller appliance.
- The management interface of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are in the same subnet.
- The discovery and inventory of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 devices are successful from Catalyst Center.
- The devices are reachable and in the **Managed** state.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

**Step 2** To view devices available in a particular site, expand the **Global** site in the left pane, and choose the site, building, or floor that you're interested in.

All the devices available in that chosen site display in the **Inventory** window.

**Step 3** In the **Devices** table, click the **Search** field. In the **Quick Filters** tab, do these steps:

**a.** For **Device Family**, click **Wireless Controllers** to get the list of wireless controllers that are discovered.

**b.** For **Reachability**, click **Reachable** to get the list of wireless controllers that are discovered and reachable.

**c.** Click **Apply**.

**Step 4** In the **Inventory** window, check the check box next to the required Cisco Catalyst 9800 Series Wireless Controller name to configure it as a primary controller.

**Step 5** Hover your cursor over **Actions** and choose **Provision** > **Configure WLC HA**.

The **High Availability** slide-in pane displays.

**Note** A warning displays at the top of the pane if the selected controller isn't assigned to a site. Catalyst Center doesn't push its telemetry configuration to the controller until it's assigned to a site.

By default, the selected Catalyst 9800 Series Wireless Controller becomes the primary controller and the **Primary C9800** field is disabled.

**Step 6** For Cisco Catalyst 9800-CL Wireless Controllers, from the **Select Primary Interface** and **Select Secondary Interface** drop-down lists, choose the interface that is used for HA connectivity.

The HA interface serves these purposes:

- Enables communication between the controller pair before the IOSd boots up.
- Provides transport for IPC across the controller pair.
- Enables redundancy across control messages exchanged between the controller pair. The control messages can be HA role resolution, keepalives, notifications, HA statistics, and so on.

**Step 7** From the **Select Secondary C9800** drop-down list, choose the secondary controller to create an HA pair.

**Note** When you choose the secondary controller, based on the wireless management interface IP subnet of the primary controller, the redundancy management IP is auto populated, and an **i** icon displays at the top of the **High Availability** window, along with this message:

Ensure that the Redundancy Management IP and Peer Redundancy Management IP aren’t assigned to any other network entities. If the IPs are in use, change the IPs accordingly and configure.

**Step 8** Enter the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses in the respective fields.

**Note**
- The IP addresses used for the redundancy management IP and peer redundancy management IP should be configured in the same subnet as the management interface of the Cisco Catalyst 9800 Series Wireless Controller. Ensure that these IP addresses are unused IP addresses within the subnet range.
- Catalyst Center only pushes the management IP address of the Cisco Catalyst 9800 Series Wireless Controller to the Cisco ISE network access device list. Whereas the standby controller uses the redundancy management IP address to initiate AAA requests. So, you must add the redundancy management IP addresses to the AAA servers for a seamless client authentication and standby monitoring.

**Step 9** From the **Netmask** drop-down list, choose the netmask address.

**Step 10** Click **Configure HA**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Note** The **Preview Configuration** window displays the configurations for the primary wireless controller and secondary wireless controller.

**Step 12** On the **Tasks** window, monitor the task deployment.

When the task is deployed, the HA configuration is initiated in the background using the CLI commands. First, the primary controller is configured. On success, the secondary controller is configured. Both the devices reboot once the HA is enabled. This process may take up to 2.5 minutes to complete.

**Step 13** To verify the HA configuration:

a) On the **Provision** > **Inventory** window, click the device that you configured as an HA device.
A dialog box with high-level device information opens.
b) In the dialog box, click **View Details**.
c) Click the **Wireless Info** tab.

The **Redundancy Summary** tab displays the **Sync Status** as **HA Pairing is in Progress**. When Catalyst Center finds that the HA pairing is successful, the **Sync Status** becomes **Complete**.

This process is triggered by the inventory poller or manual resynchronization. By now, the secondary controller (Catalyst 9800 Series Wireless Controller 2) is deleted from Catalyst Center. This flow indicates successful HA configuration in the Catalyst 9800 Series Wireless Controller.

**Step 14** To manually resynchronize the controller:

a) On the **Provision** > **Inventory** window, check the check box next to the controller that you want to synchronize manually.
b) From the **Actions** drop-down list, choose **Inventory** > **Resync Device**.

### What to do next

These actions occur after the HA process completes:

- Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured with redundancy management, redundancy units, and Single sign-on (SSO). The devices reboot to negotiate their role as an active controller or a standby controller. The configuration is synchronized from active to standby.

**Note** If you've configured a AAA server or Cisco ISE server for client and endpoint authentication in Catalyst Center then in a HA setup, the CTS credentials for active and standby controllers are synchronized and hence, during a HA switchover, Catalyst Center doesn't update the CTS credentials for the wireless controllers on Cisco ISE.

- On the **Show Redundancy Summary** window, you can see these configurations:
  - SSO is enabled.

- The Catalyst 9800 Series Wireless Controller 1 is in the active state.
- The Catalyst 9800 Series Wireless Controller 2 is in the standby state.

## Information about high availability

High availability (HA) allows you to reduce the downtime of wireless networks that occurs because of the failover of controllers. You can configure HA on Cisco Catalyst 9800 Series Wireless Controller through Catalyst Center.

## Commands to configure high availability on Cisco Catalyst 9800 Series Wireless Controllers

**Procedure**

**Step 1** Use these commands to configure HA on the primary controller for Cisco Catalyst 9800 Series Wireless Controller:

- Run the **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure an HA chassis interface:

  ```
  chassis ha-interface GigabitEthernet 3 local-ip 192.0.2.2 255.255.255.0
  remote-ip 192.0.2.3
  ```

- Run the **reload** command to reload devices for the changes to become effective.

**Step 2** Use these commands to configure HA on the secondary controller for Catalyst 9800 Series Wireless Controller:

- Run the **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure an HA chassis interface:

  ```
  chassis ha-interface GigabitEthernet 2 local-ip 192.0.2.3 255.255.255.0
  remote-ip 192.0.2.2
  ```

**Step 3** Run the **chassis clear** command to clear or delete all the HA-related parameters, such as the local IP, remote IP, HA interface, mask, timeout, and priority.

**Note** Reload the devices for changes to take effect by running the **reload** command.

**Step 4** Use these commands to configure HA on the primary controller for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the **chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure an HA chassis interface:

  ```
  chassis ha-interface local-ip 192.0.2.2 255.255.255.0 remote-ip 192.0.2.3
  ```

- Run the **reload** command to reload devices for the changes to become effective.

**Step 5** Use these commands to configure HA on the secondary controller for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the **chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure an HA chassis interface:

```
chassis ha-interface local-ip 192.0.2.3 255.255.255.0 remote-ip 192.0.2.2
```

**Step 6** Run the **chassis clear** command to clear or delete all the HA-related parameters, such as the local IP, remote IP, HA interface, mask, timeout, and priority.

**Note** Reload the devices for changes to take effect by running the **reload** command.

## Commands to verify Cisco Catalyst 9800 Series Wireless Controllers high availability

Use these commands to verify the high availability configurations from Cisco Catalyst 9800 Series Wireless Controller:

- Run the **config redundancy mode sso** command to check the HA-related details.
- Run the **show chassis** command to view chassis configurations about the HA pair, including the MAC address, role, switch priority, and current state of each controller device in the redundant HA pair.
- Run the **show ip interface brief** command to view the actual operating redundancy mode running on the device, and not the configured mode as set by the platform.
- Run the **show redundancy states** command to view the redundancy states of the active and standby controllers.
- Run the **show redundancy summary** command to check the configured interfaces.
- Run the **show romvar** command to verify high availability configuration details.

# N+1 high availability

## Overview of N+1 high availability

Catalyst Center supports N+1 high availability (HA) on Cisco AireOS wireless controllers and Cisco Catalyst 9800 Series Wireless Controllers.

Cisco AireOS wireless controllers have a dedicated stock-keeping unit (SKU) for their N+1 controllers. Cisco Catalyst 9800 Series Wireless Controllers don't have a dedicated SKU; the same model and same PID must be used for HA. For example, a Cisco Catalyst 9800-80 must be paired with another 9800-80.

The N+1 HA architecture provides redundancy for controllers across geographically separated data centers with low-cost deployments.

N+1 HA allows Cisco Wireless Controllers to be used as backup controllers for multiple primary controllers. These wireless controllers are independent of each other and do not share configuration or IP addresses on any of their interfaces. When a primary wireless controller resumes operation, the APs fall back automatically from the backup wireless controller to the primary wireless controller if the AP fallback option is enabled.

Catalyst Center supports primary and secondary controller configurations for N+1 HA.

N+1 HA is configured at the AP level, not at the global level. Configurations are pushed directly to the AP.

APs with higher priority on the primary controller always connect first to the backup controller, even if they have to push out the lower priority APs.

The N+1 HA configuration has these limitations:

- Auto provisioning of a secondary controller is not supported because of the VLAN ID configuration.
- You must reprovision the secondary controller manually with the latest design configuration if you made any changes to the primary controller.
- Catalyst Center does not support fault tolerance.
- Access Point Stateful Switch Over (AP SSO) functionality is not supported for N+1 HA. The AP Control and Provisioning of Wireless Access Points (CAPWAP) state machine is restarted when the primary controller fails.

## Prerequisites for configuring N+1 high availability from Catalyst Center

- Discover primary and the secondary controller by running the Discovery feature.

  For more information, see Discover your network using CDP, or Discover your network using an IP address range or CIDR.

- Make sure that the wireless controllers are reachable and in the Managed state.

  For more information, see About Inventory and Display information about your inventory.

- Verify the network connectivity between devices. If the primary controller goes down, the AP should be able to join the secondary controller through the N+1 configuration.
- Create two buildings to manage the primary and secondary locations for both devices. For example, create two buildings, *Building A* and *Building B*, where Building A is the primary managed location for controller-1 and also the secondary managed location for controller-2, and Building B is configured only as a primary managed location for controller-2.

  For more information, see Create, edit, and delete a site and Add, edit, and delete a building.

- Add and position APs on a floor map to get a coverage heatmap visualization during the design phase.

  For more information, see Work with APs on a floor map.

- Create two SSIDs and associate them as the backhaul SSIDs.

  For more information, see Create SSIDs for an enterprise wireless network and Create SSIDs for a guest wireless network.

## Configure N+1 high availability from Catalyst Center

This procedure shows how to configure N+1 high availability (HA) on Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

**Step 2** Check the check box next to the desired controller to provision it as a primary controller.

**Step 3** From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window displays.

**Step 4** Click **Choose a site** to assign a primary-managed AP location for the primary controller.

**Step 5** In the **Choose a site** window, select a site and click **Save**.

**Step 6** Click **Next**.

The **Configuration** window displays, which shows the primary-managed AP location for the primary device.

**Step 7** Add or update the managed AP locations for the primary controller by clicking **Select Primary Managed AP Locations**.

**Step 8** In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.

You can either select a parent site or the individual sites.

**Step 9** Configure the interface and VLAN details.

**Step 10** Under the **Configure Interface and VLAN** area, configure the IP address and subnet mask details, and click **Next**.

**Step 11** In the **Advanced Configuration** window, configure the values for the predefined template variables, and click **Next**.

**Step 12** In the **Summary** window, verify the managed AP locations for the primary controller and other configuration details, and click **Next**.

**Step 13** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 14** On the **Tasks** window, monitor the task deployment.

**Step 15** To provision the secondary controller, in the **Inventory** window, check the check box next to the desired controller to provision it as a secondary controller.

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

The **Assign Site** window displays.

**Step 17** Click **Choose a site** to assign the managed AP location for the secondary controller.

The managed AP location for the secondary controller should be the same as the managed AP location of the primary controller.

**Step 18** In the **Choose a site** window, check the check box next to the site name to associate the secondary controller, and click **Save**.

**Step 19** Click **Next**.

The **Configuration** window displays, which shows the primary AP managed and secondary-managed AP locations for the secondary device.

**Step 20** Add or update the managed AP locations for the secondary controller by clicking **Select Secondary Managed AP Locations**.

**Step 21** In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.

You can either select a parent site or the individual sites.

**Step 22** Configure the interface and VLAN details for the secondary controller.

**Step 23** Under the **Configure Interface and VLAN** area, configure the IP address and subnet mask details for the secondary controller, and click **Next**.

**Step 24** In the **Advanced Configuration** window, configure the values for the predefined template variables, and click **Next**.

**Step 25** In the **Summary** window, verify the managed AP locations for the secondary controller and other configuration details, and click **Next**.

**Step 26** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 27** On the **Tasks** window, monitor the task deployment.

**Step 28** To verify the managed locations of the primary and secondary controllers, click the device name of the controllers that you provisioned on the **Provision** > **Inventory** window.

**Step 29** In the dialog box, click **View Device Details**.

**Step 30** In the device details window, click the **Wireless Info** tab to view the primary and secondary managed location details.

**Step 31** Provision the AP for the primary controller. For more information, see Provision Cisco APs on day 1, on page 11.

# Mobility configuration overview

The mobility configuration in Catalyst Center allows you to group a set of Cisco Wireless Controllers into a mobility group for a seamless roaming experience of wireless clients.

By creating a mobility group, you can enable multiple wireless controllers in a network to dynamically share information and forward traffic when inter-controller or inter-subnet roaming occurs. Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different wireless controllers within the same wireless network.

Catalyst Center allows you to create mobility groups between various platforms, such as Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.

The mobility configuration has these guidelines and limitations:

- You cannot select multiple controllers for configuring mobility on the **Provision** window.
- You cannot create mobility groups with the group name as default. This resets the mobility and RF group names as default and deletes all the peers.
- You cannot configure a mobility group name on the anchor controller.

- You must reboot the wireless controller manually if there is a change to the virtual IP address when configuring mobility groups on Cisco AireOS Controllers.
- Wireless controllers with the same mobility group name are automatically grouped into a single mobility group and added as peers to each other.
- When configuring mobility groups on Cisco AireOS Controllers, if the wireless controllers do not have the IP address 192.0.2.1, Catalyst Center pushes the virtual IP address 192.0.2.1 to all the wireless controllers.
- Do not explicitly add guest anchor controllers to the mobility group. The provisioned guest anchor controllers do not appear in the drop-down list while adding peers in the mobility configuration window.
- If you provision a wireless controller as a guest anchor, ensure that it is not added to the mobility group.

## Mobility configuration workflow

Here is the workflow that you can follow to configure mobility on Cisco Wireless Controller:

- To configure mobility, you must provision a wireless controller with the mobility group name, RF group name, and mobility peers.
- The configuration that is applied during the wireless controller provisioning is automatically replicated to all the mobility peers configured in that group.
- Resynchronize the wireless controllers to get the latest tunnel status.

## Mobility configuration use cases

These use cases explain the steps to configure mobility between controllers.

### Use case 1

This use case assumes that wireless controller 1, wireless controller 2, and wireless controller 3 are newly added to Catalyst Center with the mobility group name, "Default." These wireless controllers aren't yet provisioned.

1. Provision wireless controller 1 by configuring the mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.
2. Provision wireless controller 2.

   In the **Provision** window, the mobility configuration is automatically populated for wireless controller 2 with the group name and peers.
3. Provision wireless controller 3.
4. After provisioning all the wireless controllers, resynchronize the wireless controllers to receive the latest tunnel status.

### Use case 2

This use case assumes that wireless controller 1, wireless controller 2, and wireless controller 3 have already been added to Catalyst Center with different mobility group names. These wireless controllers are provisioned.

1. Provision wireless controller 1 by configuring the mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.
2. The mobility configuration is automatically replicated across other peers, such as wireless controller 2 and wireless controller 3.
   - After the successful provisioning of wireless controller 1, wireless controller 2 and wireless controller 3 are added as peers on the wireless controller 1.
   - On wireless controller 2, wireless controller 1 and wireless controller 3 are added as peers.
   - On wireless controller 3, wireless controller 1 and wireless controller 2 are added as peers.

## Configure mobility group

### Procedure

**Step 1** From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays, which lists all the discovered devices.

**Step 2** Check the check box next to the Cisco Catalyst 9800 Series Wireless Controller name for which you want to configure mobility.

**Step 3** From the **Actions** drop-down list, choose **Provision** > **Configure WLC Mobility**.

The **Configure Mobility Group** slide-in pane displays.

For more information, see Mobility configuration overview, on page 32.

**Step 4** From the **Mobility Group Name** drop-down list, you can either add a new mobility group by clicking +, or choose from the existing mobility groups.

Information about the existing mobility peers is loaded from the intent available in Catalyst Center.

**Note** If you choose the default mobility group from the drop-down list, you cannot add mobility peers.

**Step 5** In the **RF Group Name** field, enter a name for the RF group.

**Step 6** To enable Datagram Transport Layer Security (DTLS) data encryption, click the **Data Link Encryption** button on.

**Step 7** To enable or disable Cipher configuration for mobility, use the **DTLS High Cipher Only** toggle button.

Cipher configuration is applicable for Cisco Catalyst 9800 Series Wireless Controller Release 17.5 or later. You must manually reboot the device for changes to take effect.

**Step 8** To manually reboot the device after making changes in the DTLS cipher configuration to take effect after provision, enable the **Restart for DTLS Ciphers to take effect** toggle button.

**Step 9** Under **Mobility Peers**, click **Add** to configure a mobility peer. You can add a maximum of 24 peer devices to a mobility group.

**Step 10** In the **Add Mobility Peer** slide-in pane, do this configuration:

a) Choose one of these types of mobility peers:

- To include mobility peers that are managed by Catalyst Center, click **Managed WLC**.
- To include mobility peers that are not managed by Catalyst Center, click **External WLC**.

b) If you choose **Managed WLC**, from the **Device Name** drop-down list, choose the controller.

After the device is provisioned, Catalyst Center creates a mobility group in the device, assigns the RF group, and configures all ends of peers. The mobility group configuration is deployed automatically to all the selected peer devices.

c) If you choose **External WLC**, do this configuration:

- In the **Device Name** field, enter the device name.
- (Optional) From the **Device Series** drop-down list, choose the device series.
- In the **Private IPv4/IPv6 Address** field, enter the private IPv4 or IPv6 address.
- (Optional) In the **Public IPv4/IPv6 Address** field, enter the public IPv4 or IPv6 address.
- In the **MAC Address** field, enter the MAC address of the device.
- In the **Mobility Group Name** field, enter the mobility group name.
- (Optional) In the **Hash** field, enter the hash for the Cisco Catalyst 9800 Series Wireless Controller.

**Note** This field is available only for Cisco Catalyst 9800-CL Wireless Controller.

d) Click **Save**.

**Step 11** Click **Configure Mobility**.

**Step 12** (Optional) You can reset the mobility group name and the RF group name using one of these methods:

- In the **Configure Mobility Group** slide-in pane, choose **default** from the **Mobility Group Name** drop-down list.
- In the **Configure Mobility Group** slide-in pane, click **Reset Mobility**.

This step automatically sets the **RF Group Name** to **default** and removes all peers. After you provision, the mobility on the device is set and the device is removed from all other peers.

**Step 13** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 14** On the **Tasks** window, monitor the task deployment.

# Configure AP Impersonation

Catalyst Center allows you to enable or disable AP Impersonation. AP Impersonation is a global setting that provides a quick and effective means to detect and report phishing incidents. AP Impersonation is supported for Catalyst 9800 Controllers.

### Procedure

**Step 1** From the main menu, choose **Design** > **Network Settings**.

**Step 2** Click **Wireless** > **Security Settings**.

**Step 3** In the left hierarchy tree, **Global** is selected by default. Expand the Global site and select the desired site, building, or floor.

**Note** The sites, buildings, and floors inherit the settings from the global level.

**Step 4** Click the **AP Impersonation** tab.

**Step 5** Check the **Enable AP Impersonation** check box to enable AP Impersonation.

**Step 6** Select the type: **Auth IE** or **Infra MFP**.

**Note** **Infra MFP** type is selected by default.

**Step 7** Click **Save**.

**Step 8** (Optional) To disable the AP Impersonation, uncheck the **Enable AP Impersonation** check box.

# About DTLS Ciphersuites

Ciphersuites are a set of encryption and integrity algorithms designed to protect radio communication on your wireless LAN.

You can configure multiple DTLS (Data Datagram Transport Layer Security) Ciphersuites on Cisco Catalyst 9800 Series Wireless Controller, Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches, and Cisco Embedded Wireless Controller on Catalyst Access Points platforms running Release 17.5 or later.

## Configure Multiple DTLS Ciphersuites

You can configure DTLS Ciphersuites either at the global level or site level.

### Before you begin

- Make sure that the Device Controllability feature is enabled on the **System** > **Settings** > **Device Settings** > **Device Controllability** window.

- Discover Cisco Catalyst 9800 Series Wireless Controllers in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.

### Procedure

**Step 1** From the main menu, choose **Design** > **Network Settings** > **Wireless**.

**Step 2** From the left hierarchy tree, select **Global** to configure all sites with the same DTLS Ciphersuite configuration.

From the left hierarchy tree, select a site to configure DTLS Ciphersuites at the site level. The DTLS Ciphersuite configuration will be pushed to the controller available on that particular site.

**Step 3** Click **Security Settings**.

**Step 4** Click the **Configure DTLS Ciphersuites** tab.

**Step 5** Uncheck the **Skip DTLS Ciphersuite Config** check box to configure Ciphersuites as part of Device Controllability.

**Step 6** Configure either default Ciphersuites or custom Ciphersuites.

By default, the **Default** Ciphersuite is selected.

The Default Ciphersuite box shows the list of default Ciphersuites and these Ciphersuites are configured as default on the device. You cannot change the priority of these default ciphersuites.

**Step 7** To configure custom Ciphersuites, click the **Custom** button.

Custom Ciphersuite overrides the default Ciphersuites with priority.

**Step 8** From the **Version** drop-down list, choose the DTLS version.

Based on the DTLS version, Catalyst Center shows the available Ciphersuites.

**Step 9** Click the blue toggle button next to the Ciphersuite if you do not want to apply any of the Ciphersuites.

**Step 10** To change the priority of Ciphersuites, drag each Ciphersuite.

**Step 11** Click **Save**.

The message `DTLS Ciphersuite Config Saved successfully` is displayed.

**Step 12** To apply the Ciphersuite configuration, you must provision the device.

For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 40.

# About N+1 Rolling AP Upgrade

The Rolling AP Upgrade feature is supported on the Cisco Catalyst 9800 Series Wireless Controller in an N+1 HA setup. This feature helps you upgrade software images on the APs associated with the Cisco Catalyst 9800 Series Wireless Controller in your wireless LAN network. To achieve the zero downtime, it is possible to upgrade APs in a staggered way using the N+1 Rolling AP Upgrade feature.

The primary controller identifies the candidate APs through the radio resource management neighbor AP map. The upgrade process starts with the software image downloading to the primary controller while the image is predownloaded to the candidate APs. After the candidate APs have been upgraded and rebooted,

they join the secondary controller in a staggered manner. After all the APs have joined the secondary controller, the primary controller reboots. The APs rejoin the primary controller in a staggered manner after it is rebooted.

Here are the prerequisites for configuring the Rolling AP Upgrade feature:

- An N+1 HA setup with two wireless controllers, one as the primary controller and the other one as the secondary.
- The primary and the N+1 controllers have the same configuration and manage the same location in the network.
- The N+1 controller is already running the Golden image so that Rolling AP Upgrade works with zero downtime.

  Golden images are standardized images for network devices and Catalyst Center automatically downloads the images from cisco.com. Image standardization helps in device security and optimal device performance.
- The N+1 controller is reachable and in **Managed** state in Catalyst Center.
- Both the controllers are part of the same mobility group, and a mobility tunnel is established between the primary and N+1 controller. The upgrade information between the primary and N+1 controllers are exchanged through the mobility tunnel.



**Note** If you have a cyclic N+1 HA deployment, where *wireless controller 1* is N+1 for *wireless controller 2* and *wireless controller 2* is N+1 for *wireless controller 1*, you cannot run Rolling AP Upgrade on both devices. Instead, one controller must go through a normal upgrade. You can run Rolling AP Upgrade on the other controller after the first controller is upgraded without the rolling AP upgrade.

## Workflow to Configure a Rolling AP Upgrade

This procedure shows how to configure a Rolling AP Upgrade on Cisco Catalyst 9800 Series Wireless Controllers.



**Note** N+1 Rolling AP Upgrade is supported on fabric and nonfabric deployments.

### Procedure

**Step 1** Install Catalyst Center.

For more information, see the *Cisco Catalyst Center Installation Guide*.

**Step 2** Log in to the Catalyst Center GUI and verify that the applications you need are in the **Running** state.

From the main menu, choose **System** > **Software Updates** > **Installed Apps**.

**Step 3** Discover the wireless controller using the Discovery feature.

You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete the configurations on network devices.

For more information, see Discover your network using CDP or Discover your network using an IP address range or CIDR.

**Step 4** Make sure that the discovered devices appear in the **Device Inventory** window and are in the **Managed** state.

For more information, see About Inventory and Display information about your inventory.

You must wait for devices to move to a **Managed** state.

**Step 5** Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Catalyst Center.

To import and upload an existing network hierarchy, see Import your site hierarchy to Catalyst Center.

To create a new network hierarchy, see Create, edit, and delete a site and Add, edit, and delete a building.

**Step 6** Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

For more information, see Work with APs on a floor map.

**Step 7** Provision the primary controller with the primary managed AP location, Rolling AP Upgrade enabled, and mobility group configured with the secondary controller as its peer.

To do this, choose **Provision** > **Network Devices** > **Inventory**, and check the check box next to the primary controller name.

**Step 8** Configure the N+1 controller as the mobility peer in the Mobility Group configuration.

For more information, see Mobility configuration overview, on page 32.

**Step 9** Provision the N+1 HA controller by configuring the primary controller's primary managed AP location as the N+1 controller's secondary managed AP location. This configures the secondary controller as the N+1 controller.

For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 40.

**Step 10** Provision the APs that are associated with the primary controller.

**Step 11** Import the software images to the repository.

For more information, see Import a software image.

**Step 12** Assign the software image to a device family.

For more information, see Manage software image assignment for a device family.

**Step 13** Mark the software image as Golden by clicking the star for a device family or a device role.

For more information, see Mark a software image as standard.

**Step 14** Before upgrading the image, make sure that the image readiness checks are successful for both devices.

Also make sure that the status of the **N+1 Device Check** and the **Mobility Tunnel Check** has a green tick mark.

- To do the image update readiness check, choose **Provision** > **Network Devices** > **Software Images**.
- From the **Focus** drop-down list, choose **Software Images**. Select the device whose image you want to upgrade.
- If the prechecks are successful for a device, the **Status** link in the **Image Precheck Status** column has a green tick mark. If any of the upgrade readiness prechecks fail for a device, the Image Precheck Status link has a red

mark, and you cannot update the OS image for that device. Click the **Status** link and correct any errors before proceeding.

**Step 15** Initiate the upgrade on primary controller.

**Step 16** On the **Software Images** window, check the check box next to the primary controller.

**Step 17** From the **Actions** drop-down list, choose **Software Image** > **Update Image**.

For more information, see Provision a software image.

**Step 18** To monitor the progress of the image upgrade, click **In Progress** in the **Software Image** column.

The **Device Status** window displays this information:

- **Distribution Operation**: Provides information about the image distribution process. The image gets copied from Catalyst Center to the primary device. The activate operation starts after the distribution process is complete.
- **Activate Operation**: Provides the activate operation details. The Rolling AP Upgrade starts during this process.
- **Rolling AP Upgrade Operation**: Provides a summary of the Rolling AP Upgrade, such as whether the Rolling AP Upgrade task is complete, the number of APs pending, the number of rebooting APs, and the number of APs that have joined the N+1 controller.

  Click **View AP Status** to view details about the primary controller, N+1 controller, device names, current status, and iterations.

# Provision a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to provision a Cisco Catalyst 9800 Series Wireless Controller.

### Before you begin

Ensure that you have completed the steps in Configure a Cisco Catalyst 9800 Series Wireless Controller in Catalyst Center, on page 20.

To share the wireless controller across multiple fabric sites, ensure that you have completed the requirements. For more information, refer to Shared wireless controllers for multiple fabric sites.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Inventory**.

**Step 2** In the **Devices** table, check the check box next to the wireless controller name that you want to provision.

**Step 3** From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

**Step 4** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, click the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, refer to "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue with device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box and select a different wireless controller. |

**Step 5** In the **Assign Site** window, assign a site to the wireless controller.

a) Click **Choose a Site**.

b) In the **Choose a site** slide-in pane, click the site name that you want to assign to the wireless controller, and click **Save**.

c) Click **Next**.

**Step 6** In the **Configuration** window, select a role for the Cisco Catalyst 9800 Series Wireless Controller: **Active Main WLC** or **Anchor**.

**Step 7** Select the managed AP location.

- Click **Select Primary Managed AP Locations** to select the managed AP location for the primary controller.
- Click **Select Secondary Managed AP Locations** to select the managed AP location for the secondary controller.

**Step 8** Select either a parent site or individual sites for the managed AP locations, and click **Save**.

If you select a parent site, all the children under the parent site are also chosen. You can uncheck the check box to deselect a child site.

**Note** The inheritance of managed AP locations allows you to automatically select a site along with the buildings and floors under that particular site. One site is managed by only one wireless controller.

**Step 9** (Optional) Check the **AP Authorization List** check box to select the authorization list for AP authorization, and then configure the AP authorization settings.

**Note** This check box is displayed only if an AP authorization list is available. For more information about the AP authorization list, refer to Create an AP authorization list.

- From the **AP Authorization List Name** drop-down list, select an AP authorization list. Based on the content of the AP authorization list, Catalyst Center displays a message indicating the corresponding primary authorization type and failback mechanism.

- (Optional) To view the entries for the selected AP authorization list, click **View Entries**.
- If the wireless controller manages both mesh and nonmesh APs, Catalyst Center displays the **Authorize Only Mesh Access Points** and **Authorize All Access Points** check boxes.

  To enable authorization for only mesh APs, check the **Authorize Only Mesh Access Points** check box.

  To enable authorization for all APs, check the **Authorize All Access Points** check box.

**Step 10** For an active main wireless controller, configure the interface and VLAN details.

**Step 11** (Optional) In the **Configure VLAN** area, configure VLAN settings.

You can configure up to eight IPv6 addresses and one IPv4 address for a dynamic interface. To configure dynamic interfaces, refer to Configure additional interfaces for a network profile.

**Note** For the FlexConnect SSIDs, VLANs aren't automatically created on the Cisco Catalyst 9800 Series Wireless Controllers during provisioning. The interface and VLANs mapped to the wireless network profile are created on the Flex profile during AP provisioning.

Select the required VLAN and click **Edit**. In the **Configure VLAN** slide-in pane, complete these configurations:

a) (Optional) In the **IPv4** tab, enter data in these fields:

- **Interface IP Address**: Enter the IPv4 address for the interface.
- **Gateway IP Address**: Enter the gateway IPv4 address for the interface.
- **Subnet Mask (in bits)**: Enter the subnet mask details for the interface.

b) (Optional) In the **IPv6** tab, click **Add IPv6 Address** and complete these configurations:

- Enter the IPv6 address for the interface.
- From the **Prefix Length** drop-down list, choose a prefix length.

**Step 12** (Optional) Check the **Skip AP Provision** check box to skip configuring the AP-related commands while provisioning the wireless controller.

For more information, refer to Skip AP provision during Cisco Catalyst 9800 Series Wireless Controller provisioning.

**Note** When you reprovision the wireless controller, Catalyst Center skips configuring AP-related commands if the AP intent configuration does not change. You can use this check box to skip AP-related configurations when there are changes to the intent configuration.

For more information about the detected AP configuration changes, refer to Skip AP provision during Cisco Catalyst 9800 Series Wireless Controller provisioning.

**Step 13** (Optional) Check the **Rolling AP Upgrade** check box to enable the Rolling AP Upgrade feature in an N+1 HA setup.

(Optional) If you check this check box, from the **AP Reboot %** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions.

For more information, refer to Workflow to Configure a Rolling AP Upgrade, on page 38.

**Note** If configured, the same AP reboot percentage value applies to both the Rolling AP Upgrade and staggered AP LSC renewal processes. For example, if you set the AP reboot percentage to 25%, only 25% of APs will reboot at a time during both Rolling AP Upgrade and staggered AP LSC renewal.

**Step 14** (Optional) Check the **AP LSC Certificate Renewal** check box to renew the Locally Significant Certificate (LSC) for the associated APs before its expiry.

By default, the wireless controller renews the AP LSCs daily at 12:00 AM in a staggered manner.

If you check this check box, complete these configurations:

- From the **Renewal Profile** drop-down list, select an AP LSC renewal profile.

  To create an AP LSC renewal profile, refer to Create an AP LSC renewal profile.

- (Optional) If you select an AP LSC renewal profile for staggered renewal, from the **AP Reboot %** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.

**Note** If configured, the same AP reboot percentage value applies to both the Rolling AP Upgrade and staggered AP LSC renewal processes. For example, if you set the AP reboot percentage to 25%, only 25% of APs will reboot at a time during both Rolling AP Upgrade and staggered AP LSC renewal.

**Step 15** (Optional) To make the wireless controller eligible for sharing with multiple fabric sites, check the **Share With Fabric Sites** check box, then choose the fabric sites where the wireless controller can be shared.

If sharing is already enabled on the wireless controller, click **Edit** to manage the remote fabric sites.

**Note** This feature is in beta.

In the **Edit Fabric Sites** slide-in pane, complete these configurations:

a) In **Step 1 of 2: Select Fabric Sites**, select the fabric sites where you want to share the wireless controller.

   Catalyst Center lists the sites that are configured as the primary or secondary managed AP locations for this wireless controller.

b) Check the **Split Network Profiles for new shared Fabric Sites** to create site-specific network profile copy.

c) Click **Next**.

d) **Step 2 of 2: Resolve Network Profile Conflicts** lists the network profile conflicts for newly added fabric sites. For each conflict, review the current network profile, proposed **New Network Profile Name**, and **SSID and Policy Profile Mapping**. Edit the proposed names as needed, and click **Apply**.

   Catalyst Center does not clone the custom policy tags, CLI templates, and feature templates associated with the profile during this step. Configure them manually after Catalyst Center creates the site-specific network profile copy.

e) After resolving all conflicts, click **Save**.

**Note**

- If the managed AP locations change after site selection, Catalyst Center displays a warning message. Review the site selection before provisioning.
- This step makes the wireless controller eligible for sharing with multiple fabric sites. To share the wireless controller, add it to each remote fabric site. For more information, refer to Configure a shared wireless controller for multiple fabric sites.

**Step 16** Click **Next**.

**Step 17** In the **Devices** pane of the **Feature Templates** window, select a feature template.

You can either search for a feature template by entering its name in the **Find** field, or expand the device and select a feature template. The chosen feature template is displayed in the right pane.

**Step 18** Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the feature template.

You can't edit all the configurations in this step.

**Step 19** After making the necessary changes, click **Apply**.

**Step 20** Click **Next**.

**Step 21** In the **Devices** pane of the **Advanced Configuration** window, search for the device or template.

**Step 22** In the **wlanid** field, enter a value for the predefined template variable, and click **Next**.

**Step 23** In the **Summary** window, review the configuration settings, and click **Next**.

**Step 24** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 25** On the **Tasks** window, monitor the task deployment.

**Note** When you provision the wireless controller, Catalyst Center pushes the configuration to the wireless controller and configures it based on the network intent.

During the reprovisioning, if there are any out-of-band configurations on the wireless controller that are a part of the network intent or conflicting with the configurations being pushed by Catalyst Center, Catalyst Center overwrites the out-of-band configurations on the wireless controller with the network intent configuration.

The selective AP group Resource Facing Service (RFS) translate feature optimizes reprovisioning for AP-related configurations (such as AP tag mapping, RF tags, and flex or RF profiles). Out-of-band changes to AP-related configurations are not automatically corrected during reprovisioning unless a compliance report explicitly flags them. To correct the AP-related out-of-band configurations to match your network intent, perform a wireless controller resynchronization and compliance run. For example, if you manually update the static AP tag mapping:

- With resynchronization and compliance run, the manual change is corrected to match the intent configuration.
- Without resynchronization and compliance run, the manual change is not corrected and only the new intent changes are applied.

To disable the selective AP group RFS translate feature, contact Cisco Technical Assistance Center (TAC).

For all the configurations that are supported through the network intent on Catalyst Center, we recommend that you use them instead of out-of-band configurations.

**Step 26** Verify the configurations that are pushed from Catalyst Center to the device using the show commands on the wireless controller.

- **#show wlan summary**
- **#show run | sec line**
- **#show running-configuration**

**Step 27** After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

**Step 28** In the **Inventory** window, from the **Focus** drop-down list, select **Provision**.

**Step 29** Under the **Provisioning Status** column, click the **See Details** link of a corresponding device to view information about network intent or a list of actions.

**Step 30** In the device slide-in pane, click **See Details** under **Device Provisioning**.

**Step 31** Click **View Details** under **Deployment of network intent**, and click the device name.

**Step 32** Click and expand the device name.

**Step 33** Expand the **Configuration Summary** area to view the operation details, feature name, and management capability.

The configuration summary also displays any error (with failure reasons) that occurred while provisioning the device.

**Step 34** Expand the **Provision Summary** area to view details of the configuration that is sent to the device.

**Step 35** Provision the AP.

# Day-zero workflow for Cisco Embedded Wireless Controller on Catalyst Access Points

The Cisco Embedded Wireless Controller on Catalyst Access Points (EWC-APs) is the next-generation Wi-Fi solution, which combines the Cisco Catalyst 9800 Series Wireless Controller with Cisco Catalyst 9100 Series Access Points, creating the best-in-class wireless experience for the evolving and growing organization.

### Before you begin

- Design your network hierarchy with sites, buildings, floors, and so on.

  For more information, see Create, edit, and delete a site and Add, edit, and delete a building.

- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS for the site where you want to claim the device.

  For more information, see Add global CLI credentials, Add global SNMPv2c credentials, and Add global SNMPv3 credentials.

- Create wireless SSIDs, wireless interfaces, and wireless Radio Frequency profiles.

  For more information, see Create SSIDs for an enterprise wireless network, Create SSIDs for a guest wireless network, Create a wireless interface, and Create a wireless radio frequency profile.

**Note** For Cisco Embedded Wireless Controller on Catalyst Access Points, only Flex-based SSID creation is supported.

- Configure the DHCP server with Option #43 on the switch where the Cisco Embedded Wireless Controller on Catalyst Access Points is connected. This IP address is IP address of the Catalyst Center Plug and Play (PnP) server. Using this IP address, the APs contact the PnP server, but remain in the **Unclaimed** state.
- Make sure that you have the Cisco Embedded Wireless Controller on Catalyst Access Points in the inventory. If not, discover them using the Discovery feature. For more information, see Discover your network using CDP, Discover your network using an IP address range or CIDR, and About Inventory.
- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

The Cisco Embedded Wireless Controller on Catalyst Access Points is available in multiple form factors:

- Cisco Embedded Wireless Controller on Catalyst 9115AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9117AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9120AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9130AX Access Points

### Procedure

**Step 1** The Cisco Embedded Wireless Controller on Catalyst Access Points contacts the DHCP server.

In response, the DHCP server provides the IP address along with Option #43, which contains the IP address of the Cisco Plug and Play server.

**Step 2** Based on Option #43, the Cisco Embedded Wireless Controller on Catalyst Access Points turns on the Plug and Play agent and contacts the Catalyst Center Plug and Play server.



**Note** If you have a set of Cisco Embedded Wireless Controller on Catalyst Access Points in the network, they go through an internal protocol. The protocol selects one Cisco Embedded Wireless Controller on Catalyst Access Points, which is configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.

**Step 3** Find the unclaimed Cisco Embedded Wireless Controller on Catalyst Access Points in the **Provision** > **Plug and Play** tab.

The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.

You must wait for the onboarding status to become **Initialized** under the **Onboarding State** column.

**Step 4** To claim the Cisco Embedded Wireless Controller on Catalyst Access Points, check the check box next to the AP device name.

**Step 5** Choose **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window displays.

**Step 6** In the **Assign Site** window, choose a site from the **Site** drop-down list.

Claiming the selected AP to this particular site also applies the associated configurations.

**Step 7** Click **Next**.

**Step 8** In the **Assign Configuration** window, to configure a device, click the corresponding **Assign** option.

**Step 9** In the **Configuration for device name** slide-in pane, do these tasks:

- In the **Wireless Management IP** field, enter the wireless management IP address.

  The IP address must not be the same as the IP address that the AP uses for contacting the PnP server.

- In the **Subnet Mask** field, enter the subnet mask.
- In the **Gateway** field, enter the gateway IP address.

**Step 10** Click **Save**.

**Step 11** Click **Next**.

The **Summary** window displays.

**Step 12** Click **Claim**.

After the Cisco Embedded Wireless Controller on Catalyst Access Points claim is successful, the configured wireless management address, subnet mask, and gateway are assigned to the Cisco Embedded Wireless Controller.

The claimed device is now listed on the **Provision** > **Inventory** window and moved to the **Managed** state. The device is automatically provisioned. After the provisioning is complete, you can view the device on the **Provisioned** tab of the **Provision** > **Plug and Play** window.

# Configure and provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches

## Supported hardware platforms

| Device role | Platforms |
|---|---|
| Embedded Wireless Controller | Cisco Catalyst 9300 Series Switches<br>Cisco Catalyst 9400 Series Switches<br>Cisco Catalyst 9500H Series Switches |
| Fabric Edge | Cisco Catalyst 9300 Series Switches<br>Cisco C9350 Series Smart Switches<br>Cisco Catalyst 9400 Series Switches<br>Cisco Catalyst 9500H Series Switches<br>Cisco Catalyst 3600 Series Switches<br>Cisco Catalyst 3850 Series Switches |
| APs | Cisco 802.11ac Wave 2 APs:<br>• Cisco Aironet 1810 Series OfficeExtend Access Points<br>• Cisco Aironet 1810W Series Access Points<br>• Cisco Aironet 1815i Access Point<br>• Cisco Aironet 1815w Access Point<br>• Cisco Aironet 1815m Access Point<br>• Cisco 1830 Aironet Series Access Points<br>• Cisco Aironet 1850 Series Access Points<br>• Cisco Aironet 2800 Series Access Points<br>• Cisco Aironet 3800 Series Access Points<br>• Cisco Aironet 4800 Series Access Points<br>Cisco 802.11ac Wave 1 APs<br>• Cisco Aironet 1700 Series Access Points |

| Device role | Platforms |
|---|---|
| | • Cisco Aironet 2700 Series Access Points<br>• Cisco Aironet 3700 Series Access Points<br><br>Cisco Catalyst 9105 Series Wi-Fi 6 Access Points<br>Cisco Catalyst 9115 Series Wi-Fi 6 Access Points<br>Cisco Catalyst 9117 Series Wi-Fi 6 Access Points<br>Cisco Catalyst 9120 Series Wi-Fi 6 Access Points<br>Cisco Catalyst 9124 Series Wi-Fi 6 Access Points<br>Cisco Catalyst 9130 Series Wi-Fi 6 Access Points<br>Cisco Catalyst 9136 Series Wi-Fi 6 Access Points<br>Cisco Catalyst Wireless 9136I Wi-Fi 6 Access Point<br>Cisco Catalyst Wireless 9163E Wi-Fi 6 Access Point<br>Cisco Catalyst Wireless 9166D Wi-Fi 6 Access Point<br>Cisco Catalyst Wireless 9166I Wi-Fi 6 Access Point<br>Cisco Catalyst Wireless 9162I Wi-Fi 6 Access Point<br>Cisco Catalyst Wireless 9164I Wi-Fi 6 Access Point<br>Cisco Catalyst Wireless 9167 Series Wi-Fi 6 Access Point<br>Cisco Wireless 9171I Series Wi-Fi 7 Access Points<br>Cisco Wireless 9172H Series Wi-Fi 7 Access Points<br>Cisco Wireless 9172I Series Wi-Fi 7 Access Points<br>Cisco Catalyst Wireless 9176 Series Wi-Fi 6 Access Point<br>Cisco Catalyst 9176D1 Series Wi-Fi 7 Access Points<br>Cisco Catalyst 9176I Series Wi-Fi 7 Access Points<br>Cisco Wireless 9177D Series Wi-Fi 7 Access Points<br>Cisco Wireless 9177E Series Wi-Fi 7 Access Points<br>Cisco Wireless 9177I Series Wi-Fi 7 Access Points<br>Cisco Catalyst Wireless 9178 Series Wi-Fi 6 Access Point<br>Cisco Catalyst 9178I Series Wi-Fi 7 Access Points |

# Preconfiguration

On Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches, make sure that these commands are present if the switch is already configured with **aaa new-model**:

```
aaa new-model
aaa authentication login default local
```

```
aaa authorization exec default local
aaa session-id common
```

This is required for NETCONF configuration. These configurations are not required if you are using automated underlay for provisioning.

# Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches

1. Install Catalyst Center.

   For more information, see the Cisco Catalyst Center Installation Guide.

2. Log in to the Catalyst Center GUI and verify that the applications you need are in the **Running** state.

   From the main menu, choose **System** > **Software Updates** > **Installed Apps**.

3. Integrate Cisco Identity Services Engine with Catalyst Center. After Cisco ISE is registered with Catalyst Center, any device that Catalyst Center discovers, along with relevant configurations and other data, is pushed to Cisco ISE.

4. Discover Cisco Catalyst 9000 Series Switches and the edge switches.

   You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.

   Do not enable NETCONF to discover the edge switches.

   For more information, see Discover your network using CDP and Discover your network using an IP address range or CIDR.

   Change the **Preferred Management IP** to **Use Loopback**.

5. Make sure that the devices appear in the device inventory and are in **Managed** state.

   For more information, see About Inventory and Display information about your inventory.

   Ensure that the devices are in the **Managed** state.

6. Design your network hierarchy, which represents your network's geographical location. You can create sites, buildings, and floors so that later you can easily identify where to apply the design settings or configurations.

   You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Catalyst Center.

   To import and upload an existing network hierarchy, see the Import your site hierarchy to Catalyst Center.

   To create a new network hierarchy, see the Create, edit, and delete a site and Add, edit, and delete a building.

7. For a nonfabric network, add and position APs on a floor map to get heatmap visualization during the design phase.

   For a fabric network, you cannot place APs on a floor map during the design time. The APs are onboarded after adding devices to a fabric network.

   For more information, see Work with APs on a floor map.

8. Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network.

   You can configure up to six AAA servers on the **Wireless** window during the SSID creation.

   For more information, see Network settings overview, Configure global network servers, and Add AAA server.

9. Configure device credentials, such as CLI, SNMP, and HTTPs.

   For more information, see Configure global device credentials, Add global CLI credentials, Add global SNMPv2c credentials, Add global SNMPv3 credentials, and Add global HTTPS credentials.

10. Configure IP address pools at the global level.

    To configure an IP address pool, see Configure IP address pools.

    To reserve an IP address pool for the building that you are provisioning, see Reserve IP Address Pools.

11. Create enterprise and guest wireless networks. Define the global wireless settings once, and then Catalyst Center pushes the configurations to various devices across geographical locations.

    Designing a wireless network is a two-step process. First, you must create SSIDs on the **Wireless** window. Then, associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

    For more information, see Create SSIDs for an enterprise wireless network and Create SSIDs for a guest wireless network.

12. Configure the backhaul settings.

13. On the **Policy** window, do this configuration:

    - Create a virtual network. The virtual network segments your physical network into multiple logical networks.
    - Create a group-based access control policy, and add a contract. For more information, see Create group-based access control policy.

14. Provision Cisco Catalyst 9000 Series Switches and the edge node switches with the configurations added during the design phase.

    - Create a fabric site.
    - Add devices to the fabric network by creating a CP+Border+Edge or CP+Border.
    - Enable embedded wireless capabilities on the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.
    - Onboard APs in the fabric site.

    For more information, see Provision SD-Access LISP Fabric Network.

    After the devices are deployed successfully, the deploy status changes from **Configuring** to **Success**.

# Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches

### Before you begin

Before provisioning a Cisco Catalyst 9800 Embedded Wireless Controller on Catalyst 9000 Series Switches, ensure that you have completed the steps in Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches, on page 50.

This procedure explains how to provision embedded wireless on Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, and Cisco Catalyst 9500H Series Switches.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window display with the discovered devices listed.

**Step 2** Check the check box next to the Catalyst 9000 Series Switch device and the edge switch that you want to associate to a site.

**Step 3** From the **Actions** drop-down list, choose **Provision** > **Assign Device to Site**. Assign the devices to a site. For more information, see Assign an unprovisioned device to a site.
The next step is to provision the Catalyst 9000 Series Switch and the edge node with the configurations that were added during the design phase.

**Step 4** In the **Provision** > **Inventory** window, check the check box next to the device name that you want to provision.

a) From the **Actions** drop-down list, choose **Provision** > **Provision Device**.
b) Click **Next**.
c) In the **Summary** window, review the configuration, and click **Next**.
d) Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

e) On the **Tasks** window, monitor the task deployment.

**Step 5** To provision the edge switch, check the check box next to the edge switch that you want to provision.

a) From the **Actions** drop-down list, choose **Provision**.
b) Click **Next**.
c) In the **Summary** window, verify the configurations, and click **Deploy**.

After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

**Step 6** To add devices to a fabric site, click the menu icon and choose **Provision** > **Fabric Sites**.

**Step 7** Create a fabric site. For more information, see Add a fabric site.

**Step 8** Add an IP transit network.

**Step 9** Add devices and associate virtual networks to a fabric site.

**Step 10** Add the Cisco Catalyst 9000 Series Switch as a control plane, a border node, and an edge node or a control plane and a border node.

a) Click the device and choose **Add as CP+Border+Edge** or **Add as CP+Border**.
b) Click the edge node and choose **Add to Fabric**.
c) Click **Save**.

**Step 11** To enable embedded wireless on the device, click the device that is added as a **Edge**, **CP+Border+Edge** or **CP+Border**, and click the **Embedded Wireless LAN Controller** toggle button.

a) If you haven't installed the wireless package on Cisco Catalyst 9000 Series Switches before enabling the wireless capability, Catalyst Center displays a warning message indicating that the embedded wireless controller software image is necessary for enabling the capability. In the warning dialog box, click **OK** to install the image manually.
b) On the **Download Image** window, click **Choose File** to navigate to a software image stored locally, or **Enter image URL** to specify an HTTP or FTP source from which to import the software image.
c) Click **Import**.

The progress of the image import is displayed. To exit the window, and view the progress of the import and schedule the installation later, click **Close**.

d) After the image import is complete, under **Schedule Image Installation** on the **Download Image** window, choose one of these options:

- **Now**: Immediately install the image.
- **Later**: Schedule the image installation for a later date or time.

e) In the **Task Name** field, update the task name, if required.
f) If you chose **Later**, do these tasks:

- Under **Start Date/Time**, specify a start date and time for the image installation.
- To use the default site time zone for the image installation, check the **Site Settings** check box. To select a time zone, uncheck the **Site Settings** check box and choose a time zone from the drop-down list.

g) Click **Apply**.

To view the status of image installation, go to the **Activities** > **Tasks** window and open the relevant work item.

h) After the embedded wireless controller software image is distributed and activated on the switch, resynchronize the device using the **Provision** > **Inventory** > **Resync** option.

**Step 12** On the **Manage Scope** window, do these tasks:

- Under the **Primary** tab, check the check box next to the required site name.
- Under the **Secondary** tab, check the check box next to the required site name.

You can select either a parent site or individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect an individual site.

You can also use the **Search Hierarchy** search field or the filter icon to find a site.

**Step 13** Click **Next**.

**Step 14** On the **Advanced** window, configure the required settings.

- To enable the Rolling AP Upgrade feature, check the **Rolling AP Upgrade** check box.

(Optional) If you check this check box, from the **AP Reboot Percentage** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.

- To renew the Locally Significant Certificate (LSC) for the associated APs before its expiry, check the **AP LSC Certificate Renewal** check box.

  If you check this check box, complete these configurations:

  - From the **Renewal Profile** drop-down list, select an AP LSC renewal profile.

    To create an AP LSC renewal profile, see Create an AP LSC renewal profile.

  - (Optional) If you select an AP LSC renewal profile for staggered renewal, from the **AP Reboot %** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.

**Note** If configured, the same AP reboot percentage value applies to both the Rolling AP Upgrade and staggered AP LSC renewal processes. For example, if you set the AP reboot percentage to 25%, only 25% of APs will reboot at a time during both Rolling AP Upgrade and staggered AP LSC renewal.

**Step 15** Click **Next**.

**Step 16** On the **Summary** window, review the configuration settings, and click **Save**.

**Step 17** On the **Modify Fabric** step, click **Now** to commit the changes, and click **Apply** to apply the configurations.
The next step is to onboard APs in a fabric site.

**Step 18** In the Catalyst Center GUI, click the menu icon and choose **Provision** > **Fabric Sites**.

A list of fabric sites displays.

**Step 19** Select the fabric site that was created, and click the **Host Onboarding** tab to enable IP pool for APs.

**Step 20** Select the authentication template that is applied for devices in the fabric site. Then, click **Save**.

**Step 21** Under **Virtual Networks**, click **INFRA_VN** to associate one or more IP pools with the selected virtual network.

**Step 22** Under **Virtual Network**, click the guest virtual networks to associate IP pools for the selected guest virtual network.

**Step 23** Check the **IP Pool Name** check box that was created for APs during the design phase.

**Step 24** Click **Update** to save the setting.

The AP gets the IP address from the specified pool, which is associated with the AP VLAN and registers with the wireless controller through one of the discovery methods.

**Step 25** Specify wireless SSIDs within the network that hosts can access. Under the **Wireless SSID** section, select the guest or enterprise SSIDs and assign address pools, and click **Save**.

**Step 26** Manually trigger resynchronization by choosing **Inventory** > **Resync** to see the APs on Catalyst Center for embedded wireless.
The discovered APs are now displayed under **Inventory** in the **Provision** window and the **Status** is displayed as **Not Provisioned**.

**Step 27** Provision the AP.

For more information, see Provision Cisco APs on day 1, on page 11.

**Step 28** Configure and deploy application policies. For more information, see Create an application policy, Deploy an application policy, and Edit an application policy.

Provision the Catalyst 9300 Series Switches and Cisco Catalyst 9500H Series Switches before deploying an application policy.

Two different policies with different business relevance for two different SSIDs don't work. The last deployed policy takes precedence when you're setting up the relevance.

Changing the default business relevance for an application doesn't work in FlexConnect mode.

You can apply an application policy only on a nonfabric SSID.

# Renew AP LSC for a wireless device

**Before you begin**

Ensure that the device is running Cisco IOS XE Release 17.1.7.1 or later.

Use this procedure to renew the AP Locally Significant Certificate (LSC) for a wireless device before it expires.

You can renew the AP LSCs for these devices:

- Cisco Catalyst 9800 Series Wireless Controllers
- Wireless-capability-enabled switches

You can renew the certificates for APs that are due for renewal based on the due time, site tags, or manual selection.

## Procedure

**Step 1** Navigate to the device in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global**, and choose an area, building, or floor.
c) Select the device to renew the AP LSCs.

**Step 2** From the **Actions** drop-down list, choose **Provision** > **Renew AP LSC Certificate**.

**Step 3** In the **Renew Access Point Certificate** window, complete these configurations:

a) Select an option for renewing the AP LSCs.

*Table 1: AP selection options*

| Option | Description |
|---|---|
| **All APs due for certificate renewal** | Renews the certificates for all APs that are due for renewal based on the number of days before expiry.<br>In the **Due Time** field, enter the number of days before AP LSC expiry. The valid range is 0 to 60 days. |

| Option | Description |
|---|---|
| **APs configured with selected site tags and due for certificate renewal** | Renews the certificates for all APs that are due for renewal based on the site tags.<br>• From the **Site tags** drop-down list, select one or more site tags.<br>• In the **Due Time** field, enter the number of days before AP LSC expiry. The valid range is 0 to 60 days. |
| **Manually select APs** | Renews the certificates for all APs that are due for renewal based on your selection.<br>In the table, select the required APs.<br>**Note**<br>You can search for APs using the search field for each column in the table. In the search field, manually enter a value, and press **Enter**.<br>The search results display the corresponding APs with value highlighted throughout the column. |

b) Click **Submit**.

**Step 4** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 5** On the **Tasks** window, monitor the task deployment.

# Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Catalyst Center allows you to customize individual features or parameters on Cisco Catalyst 9800 Series Wireless Controllers using the Per-Device Configuration feature. Using Per-Device Configuration, you can create, edit, clone, and delete the device-level configurations for a wireless controller.

You can use these configurations to onboard new wireless controllers to Catalyst Center and manage their configurations. You can also manage the APs associated with these wireless controllers.

### Default status

By default, the Per-Device Configuration feature is disabled on Catalyst Center. To enable the configurations, see Enable Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 58.

### Limitations

- Per-Device Configuration isn't supported for
  - wireless controllers that were previously added to Catalyst Center and are using intent-based wireless network configurations with site-based network profiles (for these wireless controllers, Per-Device Configuration is available in read-only mode), and
  - SD-Access wireless configurations.
- For AI-Enhanced RRM configurations, Per-Device Configuration is supported for only the Assurance use case with the **Enable Without Device Provisioning** deployment type.

# Prerequisites for Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

- Ensure that the wireless controller is running Cisco IOS XE Release 17.12 or later.
- Add the wireless controller to Catalyst Center.
  - You can add a single device manually and add multiple devices using discovery or by importing a CSV file on the **Inventory** window. For more information, see Add devices to the Catalyst Center Inventory.
  - You can migrate the devices from Cisco Prime Infrastructure using the Prime Data Migration Tool (PDMT). For more information, see *Cisco Prime Infrastructure to Cisco Catalyst Center Prime Data Migration Guide*.
- Ensure that the devices are displayed on the **Inventory** window and are in the **Managed** state.

  For more information, see About Inventory and Display information about your inventory.
- Design your network hierarchy by adding areas, buildings, and floors. This structure makes it easier to identify sites for applying configurations later.

  You can either
  - create a network hierarchy (see Create, edit, and delete a site and Add, edit, and delete a building), or
  - import an existing network hierarchy into Catalyst Center if you have it on Cisco Prime Infrastructure (see Import your site hierarchy to Catalyst Center).
- Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

  For more information, see Work with APs on a floor map.
- Ensure that the country codes are configured.

  For more information, see About wireless devices and country codes, on page 1.

# Enable Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to enable the Per-Device Configuration feature for a Cisco Catalyst 9800 Series Wireless Controller.

**Note** If the wireless controller is managed using intent-based wireless network configurations with site-based network profiles, Per-Device Configuration can be used in read-only mode for the wireless controllers.

### Before you begin

Ensure that the prerequisites are met. See Prerequisites for Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 57.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** From the top-right corner of the device details window, click **Enable Per-Device Configuration**.

**Step 4** In the **Per-device configuration** dialog box, view the details and click **Enable**.

### What to do next

Ensure that the wireless controller is resynchronized before performing other operations. For more information on manually resynchronizing the wireless controller, see Resynchronize device information.

# Configure per-device features for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure and provision individual features using Per-Device Configuration for a wireless controller.

**Note** If you make any configuration changes outside of Catalyst Center (for example, through CLI or WebUI), these changes are detected and imported during the next inventory synchronization. This process may lead to conflicts. To maintain consistency and ensure predictable network behavior, we recommend that you use Catalyst Center for all supported configuration changes.

### Before you begin

Ensure that

- the prerequisites are met (see Prerequisites for Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 57) and
- Per-Device Configuration is enabled on the wireless controller (see Enable Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 58).

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** (Optional) From the top-right corner of the device details window, click **Manage APs** to modify the AP configuration for the APs associated with the wireless controller.

For more information, see Manage APs associated with a Cisco Catalyst 9800 Series Wireless Controller, on page 60.

**Step 4** In the **Configuration** tab, configure and provision the required features for the wireless controller.

- **SSID**: See SSID configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 66.
- **RF**: See RF configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 97.
- **AP**: See AP configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 111.
- **Tag Mapping**: See Tag mapping configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 144.
- **Security**: See Security configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 151.
- **Global Wireless**: See Global wireless configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 217.
- **Services**: See Service configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 288.
- **Layer 2**: See Layer 2 configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 311.
- **Network Settings**: See Network settings for a Cisco Catalyst 9800 Series Wireless Controller, on page 324.
- **Layer 3**: See Layer 3 configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 343.
- **Administration**: See Administrative configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 345.

To search for a configuration, in the left pane of the device details window, click the **Search Features** field, and enter the name of the configuration.

**Note** The available configurations and their options can vary based on the Cisco IOS XE release running on the wireless controller.

## Manage APs associated with a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to manage the APs associated with a wireless controller through Per-Device Configuration. You can configure the tags (site tag, policy tag, and RF tag) and tag-mapping profiles for APs associated with a wireless controller.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** From the top-right corner of the device details window, click **Manage APs**.

**Step 4** (Optional) In the **Access Points** slide-in pane, edit the AP configuration set under **Operational Access Points**.

**a.** Check the check box next to the required AP names.

**b.** Click **Edit AP Configuration Set**.

The **Edit AP Configuration Set** slide-in pane opens.

**c.** From the **Policy Tag** drop-down list, choose a policy tag.

**d.** From the **Site Tag** drop-down list, choose a site tag.

**e.** From the **RF Tag** drop-down list, choose an RF tag.

**f.** Complete Step 7, on page 61 through Step 9, on page 61 to provision the configuration.

**Step 5** (Optional) Assign APs to a site.

**a.** Check the check box next to the required AP names.

**b.** Click **Assign AP to Site**.

The **Assign AP to Site** slide-in pane opens.

**c.** Choose the required site.

**Note** You can either search for a site by entering its name in the **Search** field or expand **Global** to choose the site.

**d.** Click **Assign**.

**Step 6** (Optional) Click **Configure AP and Radio Parameters** to configure the AP and radio parameters.

For more information, see Configure APs.

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Customize table settings for Per-Device Configuration

Use this procedure to customize the Per-Device Configuration table settings for a feature if the device details window displays a table.

**Note** This procedure isn't applicable if the window doesn't display a table for the feature, such as **Airtime Fairness**.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, click the required settings.

**Step 4** In the corresponding configuration table, click the gear icon at the top-right corner.
The **Table Settings** slide-in pane opens.

**Step 5** Click **Table Appearance** to adjust the table density and table striping.
a) Under **Table Density**, choose an option: **Default** or **Compact**
b) To apply table striping, click the toggle button under **Table Striping**.
c) Click **Apply**.

**Step 6** (Optional) To reset the table settings, click **Reset All Settings**.

## Edit a Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to edit the Per-Device Configuration for a feature if the device details window displays a table.



**Note** This procedure isn't applicable if the window doesn't display a table for the feature, such as **Airtime Fairness**.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, click the required per-device feature.

**Step 4** Check the check box next to the configuration that you want to edit.

**Step 5** Hover your cursor over **Actions** and click **Edit**.

**Step 6** In the slide-in pane, edit the required configurations.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Clone a Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to clone the Per-Device Configuration for a feature if the device details window displays a table.

**Note** This procedure isn't applicable if the window doesn't display a table for the feature, such as **Airtime Fairness**.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, click the required per-device feature.

**Step 4** Check the check box next to the configuration that you want to clone.

**Step 5** Hover your cursor over **Actions** and click **Clone**.

**Step 6** In the slide-in pane, complete the required configurations.

**Step 7** (Optional) Edit the other necessary configurations.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Clone a Per-Device Configuration from another Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to clone the Per-Device Configuration from another Cisco Catalyst 9800 Series Wireless Controller for these features:

- WLAN profile
- Policy profile
- AP join profile
- RF profile
- Flex profile
- Site tag

If you clone a configuration from a wireless controller running a different Cisco IOS XE Release, some options might be unavailable or incorrect. Catalyst Center chooses a default that applies to your wireless controller in these cases. Verify the values before proceeding.

**Note** If the wireless controller from which you are cloning the configurations is encrypted with a master key, you must configure a password (clear text or encrypted) during the cloning process for WLAN profiles and AP join profiles to enable successful provisioning.

### Before you begin

Ensure that the wireless controller that you want to clone is already added to Catalyst Center and is in the Managed state.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, click the corresponding per-device feature.

**Step 4** Click **Clone from another WLC**.

**Step 5** In the slide-in pane, complete these steps:
a) From the drop-down list, choose the wireless controller from which you want to clone the configuration.

The list of configurations associated with the chosen wireless controller is displayed.

b) Choose the required configuration.
c) Click **Clone**.

**Step 6** In the warning dialog box, click **OK**.

**Step 7** A slide-in pane displays the cloned configurations from the selected wireless controller.

**Note** Cloning a feature copies the configuration from the source wireless controller. Review the configurations before applying them to ensure compatibility with the target wireless controller.

**Step 8** Edit the required configurations.

**Note** A warning icon on the left pane indicates any configuration conflicts. Review the conflict, then select an appropriate value to continue to the next window.

**Step 9** Click **Review and Provision**.

**Step 10** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Delete a Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to delete the Per-Device Configuration for a feature if the device details window displays a table.

**Note** This procedure isn't applicable if the window doesn't display a table for the feature, such as **Airtime Fairness**.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, click the required per-device feature.

**Step 4** Check the check box next to the configurations that you want to delete.

**Step 5** Hover your cursor over **Actions** and click **Delete**.

**Step 6** In the dialog box, click **Yes**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

# SSID configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device SSID configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a WLAN profile for a wireless controller and provision it. WLAN profiles configure the Wi-Fi settings, enabling users to connect to a wireless network.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **SSID** and click **WLAN Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **General** tab of the **Create WLAN Profile** slide-in pane, complete these configurations.

a) In the **Wireless Network Name (SSID)** field, enter a unique SSID name.
b) In the **WLAN ID** field, the WLAN ID is automatically populated based on the next available number.

If necessary, update the WLAN ID. The valid range is from 1 to 4096.

c) In the **WLAN Profile Name** field, the WLAN profile name is automatically populated based on the WLAN profile name.

If necessary, update the name.

**Note** Ensure that the WLAN profile name is unique and does not match any existing RLAN profile names. Otherwise, the WLAN profile creation task fails.

d) Under **SSID State**, use the toggle button to enable or disable the corresponding status.

- **Admin Status**: enable or disable the administrative status of the WLAN.

  If you disable this toggle button, the corresponding SSID isn't broadcast in the AP beacons.

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

e) Under **Wi-Fi 7 Compatibility**, view the Wi-Fi 7 compatibility information.

To view the details, click **Show Details**.

To ensure Wi-Fi 7 compatibility, in Step 6, on page 69, complete these configurations:

- enable WPA3.
- choose one of these supported combination of cipher and authentication key management:
  - AES and 802.1X-SHA256 or FT-802.1X
  - GCMP256 and SAE-EXT-KEY, FT-SAE-EXT-KEY, or OWE
  - GCMP256 and 802.1X-SHA256 or FT-802.1X
  - GCMP256 and Suite-B-192

- set Protected Management Frame (PMF) to **Required** or **Optional**.

f) Under **Wi-Fi 7 Per Band Status**, view the per-band status for Wi-Fi 7 configuration.

To view the details for each band, click **Show Details**.

To enable Wi-Fi 7 per each band, complete these configurations:

- Enable the band under **Radio Policy**.
- Enable Global 11be for each band. For more information, refer to Configure high throughput parameters for a Cisco Catalyst 9800 Series Wireless Controller, on page 220.
- Enable the band in the Multi-Link Operation (MLO) group in the selected 802.11be profile. For more information, refer to Configure the 802.11be profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 95.

g) Under **Radio Policy**, complete these configurations.

- The supported radio slots for each 802.11 band are listed. Click **Show Slot Configuration** to view the slot configuration for the corresponding bands.

**Note** In the slot configuration, if a check box is available next to a slot, you can use it to enable or disable the slot for the corresponding band.

- Use the **6 GHz**, **5 GHz**, and **2.4 GHz** toggle buttons to enable or disable the radio policy for the corresponding band.

**Note** The 6-GHz band is supported only when

- WPA2 is disabled, and
- WPA3, protected management frame, and 802.11ax configurations are enabled.

- From the **Bg Policy** drop-down list, choose a policy.

**Note** This drop-down list is available only when you enable the **2.4 GHz** toggle button.

- (Optional) Check the required check boxes to enable the corresponding configurations.

| Check box | Description |
|---|---|
| **Band Select** | Available only when you enable the **2.4 GHz** toggle button. |
| **6 Ghz Client Steering** | Available only when you enable the **6 GHz** toggle button. |

- From the **Minimum 2.4 GHz Data Rate** and **Minimum 5 GHz Data Rate** drop-down lists, choose the minimum supported data rates for the clients connecting on the band.

A higher value can improve network performance and reduce interference from legacy devices, but may prevent older and distant clients from connecting. Choose a lower value to maximize compatibility or a higher value to optimize throughput and improve airtime efficiency.

**Note** Slot availability on APs depends on the AP model. For slots with Flexible Radio Assignment (FRA) capability, FRA can dynamically change the band. This configuration applies to the slot only when it operates in the configured band. Use this configuration to limit WLAN broadcasts by band and slot as needed. Ensure that at least one slot is enabled across the bands.

**Step 6** Under **Security**, click **Layer 2** and configure a security policy.

**Note** WLANs with the same SSID must have unique Layer 2 security policies.

- Click **Enterprise** to configure user credential validation with an 802.1X server for authentication and complete these configurations.

  **a.** (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

  Use this field if you need a different authorization policy than the global or default list.

  **b.** (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

  If you do not specify an authorization list in this field, the WLAN uses the default list.

  **c.** (Optional) Check the **Mac Filtering** check box to enable MAC-based access control or security on the wireless network.

  If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

  To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159.

  **d.** (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.

  **e.** Under **WPA Parameters**, check the required check boxes to configure the corresponding settings.

  - **WPA**: configure WPA support.

  **Note** If you check the **WPA3** or **OSEN Policy** check box, this check box is dimmed.

  - **WPA2**: configure WPA2 support.
  - **WPA3**: configure WPA3 support.

**Note** If you check the **WPA**, **GTK Randomize**, or **OSEN Policy** check box, this check box is dimmed.

If you enable WPA3, you can optionally check these check boxes to configure the corresponding settings.

- **Transition Disable**: prevent the transition from WPA3 to WPA2.
- **Beacon Protection**: enable beacon protection.

- **GTK Randomize**: enable randomized group temporal key (GTK) for hole 196 mitigation.

  Hole 196 is the name of a WPA2 vulnerability.

**Note** If you check the **WPA3** check box, this check box is dimmed.

- **OSEN Policy**: configure the Online subscription with Encryption (OSEN) support.

**Note** If you check the **WPA** or **WPA3** check box, this check box is dimmed.

**f.** If the **WPA Encryption** area is displayed, check the required check boxes to enable the corresponding cipher support for WPA.

You must enable support for at least one cipher.

**g.** If the **WPA2/WPA3 Encryption** area is displayed, complete these configurations.

- For wireless controllers running releases earlier than Cisco IOS XE Release 17.15, choose the required encryption type.
- For wireless controllers running Cisco IOS XE Release 17.15 or later, check the check box next to the required encryption types.

**h.** If the **Auth Key Management** area is displayed, check the required check boxes to choose the corresponding authentication key management types.

The types available under this area vary based on the WPA, WPA2, or WPA 3 encryption settings.

If you check the **CCKM** check box, in the **CCKM TSF Tolerance** field, enter the CCKM tolerance level in milliseconds.

The valid range for this field is from 1000 to 5000. The default value is 1000. Authenticated client devices can roam from one AP to another AP without any perceptible delay during reassociation.

**i.** Under **Protected Management Frame (802.11w)**, from the **Status** drop-down list, choose an available status.

If you chose **Optional** or **Required**, complete these configurations.

- In the **SA Query Time(msec)** field, enter the Security Association (SA) query retry timeout in milliseconds.

  The valid range is from 100 to 500. The default value is 200.

- In the **Association Comeback Timer(sec)** field, enter the association comeback time in seconds.

  The valid range is from 1 to 20. The default value is 1.

**j.** Under **Fast Transition (802.11r)**, from the **Fast Transition Mode** drop-down list, choose an available mode.

If you chose **Enabled** or **Adaptive Enabled**, complete these configurations.

- Check the **Over the DS** check box to enable fast transitions over a distributed system.
- In the **Reassociation Timeout** field, enter the reassociation timeout in seconds.

  The valid range is from 1 to 100. The default value is 20.

- Click **Personal** to configure user credential validation using password (PSK with WPA2 encryption) and complete these configurations.

**a.** (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

Use this field if you need a different authorization policy than the global or default list.

**b.** (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

If you do not specify an authorization list in this field, the WLAN uses the default list.

**c.** (Optional) Check the **Mac Filtering** check box to enable MAC-based access control or security on the wireless network.

If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159.

**d.** (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.

**e.** Under **WPA Parameters**, check the required check boxes to configure the corresponding settings.

- **WPA**: configure WPA support.

**Note** If you check the **WPA3** check box, this check box is dimmed.

- **WPA2**: configure WPA2 support.
- **WPA3**: configure WPA3 support.

**Note** If you check the **WPA** or **GTK Randomize** check box, this check box is dimmed.

If you enable WPA3, you can optionally check the required check boxes to enable the corresponding configurations.

- **Transition Disable**: prevent the transition from WPA3 to WPA2.

- **Beacon Protection**: enable beacon protection.

- **GTK Randomize**: enable randomized GTK for hole 196 mitigation.

  Hole 196 is the name of a WPA2 vulnerability.

**Note** If you check the **WPA3** check box, this check box is dimmed.

**f.** If the **WPA Encryption** area is displayed, check the required check boxes to enable the corresponding cipher support for WPA.

You must enable support for at least one cipher.

**g.** If the **WPA2/WPA3 Encryption** area is displayed, check the **AES(CCMP128)** check box to choose this encryption type.

**h.** If the **Auth Key Management** area is displayed, check the required check boxes to choose the corresponding authentication key management type.

The options available under this area vary based on the WPA, WPA2, or WPA 3 encryption settings.

Based on the options that you chose, if additional configurations are available, complete these configurations.

- (Optional) From the **PSK Format** drop-down list, choose an authentication preshared key (PSK) format.
- (Optional) From the **PSK Type** drop-down list, choose **Unencrypted**.
- In the **Pre-shared Key** field, enter a PSK value.

  For hexadecimal key format, the PSK length must be 64 characters. For ASCII key format, the PSK length must be in the range 8–63.
- In the **Anti Clogging Threshold** field, enter the Simultaneous Authentication of Equals (SAE) anticlogging threshold.

  The valid range is from 0 to 3000. The default value is 1500.
- In the **Max Retries** field, enter the maximum number of SAE retransmissions.

  The valid range is from 1 to 10. The default value is 5.
- In the **Retransmit Timeout** field, enter the SAE retransmission timeout.

  The valid range is from 1 to 10000. The default value is 400.
- (Optional) From the **SAE Password Element** drop-down list, choose an SAE password element mode.

**i.** Under **Protected Management Frame (802.11w)**, from the **Status** drop-down list, choose an available status.

If you chose **Optional** or **Required**, enter data in these fields.

- **Association Comeback Timer(sec)**: enter the association comeback time in seconds.

  The valid range is from 1 to 20. The default value is 1.
- **SA Query Time(msec)**: enter the Security Association (SA) query retry timeout in milliseconds.

  The valid range is from 100 to 500. The default value is 200.

**j.** Under **Fast Transition (802.11r)**, from the **Fast Transition Mode** drop-down list, choose an available mode.

If you chose **Enabled** or **Adaptive Enabled**, complete these configurations.

- Check the **Over the DS** check box to enable fast transitions over a distributed system.
- In the **Reassociation Timeout** field, enter the reassociation timeout in seconds.

  The valid range is from 1 to 100. The default value is 20.

**k.** (Optional) Under **MPSK**, check the **Enable MPSK** check box to configure multi-preshared key (MPSK) support, and complete these configurations.

**Note** MPSK and Easy-PSK can't be enabled simultaneously.

| If you want to... | Then... |
|---|---|
| add an MPSK<br>**Note** You can add up to five MPSKs. | **1.** Click **Add**.<br>**2.** In the **Priority** field of the **Add MPSK Configuration** dialog box, enter a priority.<br>The valid range is from 0 to 4.<br>**3.** (Optional) From the **Key Format** drop-down list, choose a format.<br>**4.** (Optional) From the **Password Type** drop-down list, choose **Unencrypted**.<br>**5.** (Optional) In the **Pre-Shared Key** field, enter an MPSK key.<br>**6.** Click **Save**. |
| edit an MPSK | **1.** Check the check box next to the MPSK that you want to edit.<br>**2.** Hover your cursor over **Actions** and choose **Edit**.<br>**3.** Edit the required configurations.<br>**4.** Click **Save**. |
| delete MPSKs | **1.** Check the check box next to the MPSKs that you want to delete.<br>**2.** Hover your cursor over **Actions** and choose **Delete**.<br>**3.** In the dialog box, click **Yes**. |

- Click **Static WEP** to configure user credential validation with an 802.1X server for authentication using static Wired Equivalent Privacy (WEP) and complete these configurations.

**Note** These configurations are unavailable for wireless controllers running Cisco IOS XE Release 26.1.1 or later.

a. (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

   Use this field if you need a different authorization policy than the global or default list.

b. (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

   If you do not specify an authorization list in this field, the WLAN uses the default list.

c. (Optional) Check the **Mac Filtering** check box to enable MAC-based access control or security on the wireless network.

   If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

   To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159.

d. (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.

e. Under **Static WEP Parameters**, complete these configurations.

   - From the **Key Size** drop-down list, choose a key size.
   - In the **Key Index** field, enter the WEP key index to indicate the key that should be used for static WEP authentication.

     The valid range is from 1 to 4.
   - From the **Key Format** drop-down list, choose a WEP key format.
   - From the **WEP Key Type** drop-down list, choose a WEP key encryption type.
   - In the **Wep Key** field, enter a static WEP key.

     The key length depends on the key size that you chose from the **Key Size** drop-down list.

f. (Optional) Under **Fast Transition**, check the **Static WEP Fast Transition** check box to enable fast transition.

- Click **Open Secured** to configure user credential validation using open secured authentication and complete these configurations.

a. (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

   Use this field if you need a different authorization policy than the global or default list.

b. (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

   If you do not specify an authorization list in this field, the WLAN uses the default list.

c. (Optional) Check the **Mac Filtering** check box to enable MAC-based access control or security on the wireless network.

   If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

   To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159.

d. (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.

**e.** Check the **WPA3** check box to configure WPA3 support.

**f.** Under **WPA2/WPA3 Encryption**, check the **AES(CCMP128)** check box to choose this encryption type.

**g.** Under **Auth Key Management**, check the required check boxes to choose the corresponding authentication key management types.

The options available under this area vary based on the WPA3 encryption settings.

If you checked the **OWE** check box, in the **Transition Mode WLAN ID** field, enter the Opportunistic Wireless Encryption (OWE) transition mode WLAN ID.

The valid range for this WLAN ID is from 0 to 4096. The default value is 0.

**h.** Under **Protected Management Frame (802.11w)**, from the **Status** drop-down list, choose an available status.

If you chose **Optional** or **Required**, complete these configurations.

- In the **Association Comeback Timer(sec)** field, enter the association comeback time in seconds.

  The valid range is from 1 to 20. The default value is 1.

- In the **SA Query Time(msec)** field, enter the Security Association (SA) query retry timeout in milliseconds.

  The valid range is from 100 to 500. The default value is 200.

- Click **Open** to configure open authentication, and check the required check boxes to enable the corresponding configurations.
  - (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

    Use this field if you need a different authorization policy than the global or default list.
  - (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

    If you do not specify an authorization list in this field, the WLAN uses the default list.
  - (Optional) **Mac Filtering**: enable MAC-based access control or security on the wireless network.

    If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

    To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159.
  - (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.
  - (Optional) **OWE Transition Mode**: configure OWE transition mode.

    If you check this check box, in the **Transition Mode WLAN ID** field, enter the OWE transition mode WLAN ID.

    The valid range for this WLAN ID is from 0 to 4096. The default value is 0.

**Step 7** (Optional) Under **Security**, click **Layer 3** and complete these configurations.

a) Check the **Web Policy** check box to configure the web authentication policy.

b) From these drop-down lists, choose the required options.

- **Web Auth Parameter Map**: choose a parameter map for web authentication. To create a web authentication parameter map, refer to Create a web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 192.
- **Authentication List**: choose an authentication list.

  To create an authentication list, refer to Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 158.

c) Check the required check boxes to enable the corresponding configurations.

- **On MAC Filter Failure**: enable web authentication on MAC filter failure.
- **Splash Web Redirect**: set a splash-page web redirect

d) (Optional) In the **Web Authorization List** field, enter the name of the web authentication authorization list for the WLAN.

This list permits or denies client access during web authentication sessions.

e) Under **Preauthentication ACL**, choose an IPv4 ACL and IPv6 ACL from the corresponding drop-down lists.

To create an IPv4 ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168. To create an IPv6 ACL, refer to Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 175.

**Step 8** (Optional) Under **Security**, click **AAA** and complete these configurations.

a) From the **Authentication List** drop-down list, choose an authentication list.

To create a **dot1x** type authentication list, refer to Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 158.

b) Check the **Local EAP Authentication** check box to enable the local Extensible Authentication Protocol (EAP) on a WLAN.

If you check this check box, from the **EAP Profile Name** drop-down list, choose a local EAP profile. To create a local EAP profile, refer to Create a local EAP profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 182.

**Step 9** (Optional) Under **Advanced**, click **11be** and choose an 802.11be profile for the WLAN.

To create an 802.11be profile, refer to Configure the 802.11be profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 95.

**Step 10** (Optional) Under **Advanced**, click **11ax** and complete these configurations.

a) Check the required check boxes to enable the corresponding configurations.

- **Enable 11ax**: enable the 802.11ax configuration.
- **Downlink MU-MIMO**: enable the 802.11ax multiuser MIMO (MU-MIMO) downlink configuration.
- **Downlink OFDMA**: enable the 802.11ax Orthogonal Frequency Division Multiplexing (OFDMA) downlink configuration.
- **Uplink MU-MIMO**: enable the 802.11ax MU-MIMO uplink configuration.
- **Uplink OFDMA**: enable the 802.11ax OFDMA uplink configuration.

- **BSS Target Wake Up Time**: enable 802.11ax target wake-up time support.
- **HE BSS Color Enable**: enable the 802.11ax basic service set (BSS) color configuration.

  If you check this check box, in the **HE BSS Color** field, enter a BSS color value.

  The valid range is from 0 to 255. The default value is 0.
- **HE TWT Enable**: enable 802.11ax target wake-up time.
- **BSS Target Wake Up Time Broadcast**: enable 802.11ax target wake-up time broadcast support.

**Step 11** (Optional) Under **Advanced**, click **11k** and complete these configurations.

a) Under **Assisted Roaming**, check the required check boxes to indicate the appropriate status for the corresponding configurations.
   - **Prediction Optimization**: indicates if 11k assisted roaming prediction optimization is enabled on the wireless controller for the WLAN.
   - **Neighbor List**: indicates if the 11k neighbor list is enabled on the wireless controller for the WLAN.
   - **Dual Band Neighbor List**: indicates if the 11k dual-band neighbor list is enabled on the wireless controller for the WLAN.

b) Under **Beacon Radio Measurement**, check the required check boxes to configure the corresponding settings.
   - **Client Scan Report on Association**: send a beacon measurement request after client association.
   - **Client Scan Report on Roam**: send a beacon measurement request on client roaming.

**Step 12** (Optional) Under **Advanced**, click **11v BSS** and complete these configurations.

a) Check the required check boxes to configure the corresponding settings.
   - **BSS Transition**: enable BSS transition per WLAN.
   - **BSS Max Idle Protected**: enable protected mode for BSS maximum idle processing per WLAN.
   - **Dual Neighbor List**: determine if the dual-band neighbor list is enabled in 802.11v BSS transition for WLAN.
   - **Directed Multicast Service**: configure Directed Multicast Service (DMS) processing per WLAN.
   - **BSS Max Idle Service**: enable BSS maximum idle processing per WLAN.
   - **802.11v Disassociate Imminent**: enable BSS transition disassociation imminent per WLAN.
   - **802.11v TFS**: enable TFS processing per WLAN.
   - **802.11v WNM Sleep Mode**: enable Wireless Network Management (WNM) sleep mode per WLAN.

b) In the **802.11v Disassociate Timer** field, enter the 802.11v disassociation imminent timer in seconds.

   The valid range is from 0 to 3000. The default value is 200.

c) In the **802.11v Disassociate Timer Optimized Roaming** field, enter the 802.11v disassociation imminent optimized-roaming timer in seconds.

   The valid range is from 0 to 40. The default value is 40.

**Step 13** (Optional) Under **Advanced**, click **Device Analytics** and check the required check boxes to enable the corresponding configurations.

- **Advertise Support**: enable device analytics support.
- **Share Data with Client**: enable sharing the Cisco device data with the client.
- **Advertise PC Analytics Support**: enable PC analytics support.

**Step 14** (Optional) Under **Advanced**, click **Max Clients** and enter data in these fields.

- **Per WLAN**: enter the maximum number of client connections per WLAN.

  The valid range is from 0 to 32000. The default value is 0.

- **Per AP Per WLAN**: enter the maximum number of client connections per AP that can be configured on a WLAN.

  The valid range is from 0 to 1200. The default value is 0.

- **Per AP Radio Per WLAN**: enter the maximum number of client connections per AP radio that can be configured on a WLAN.

  The valid range is from 0 to 500. The default value is 200.

**Step 15** Under **Advanced**, click **Off Channel Scan** and complete these configurations.

a) Under **Defer Priority**, check the required check boxes to choose the corresponding RRM off channel scan defer priority values for packets.
b) In the **Scan Defer Time (msec)** field, enter the required scan defer time in milliseconds.

   The valid range is from 0 to 60000. The default value is 100.

**Step 16** Under **Advanced**, click **Miscellaneous** and complete these configurations.

a) From the **Peer to Peer Blocking** drop-down list, choose a peer-to-peer blocking configuration on the WLAN.
b) Use the required optionsto configure the corresponding settings.

   - **Coverage Hole Detection**: enable Coverage Hole Detection (CHD) on the wireless controller
   - **Fastlane+ (ASR)**: enable advanced scheduling request handling on a WLAN
   - **Aironet IE**: enable the support for Cisco Compatible Extensions option and set the support for Aironet information element (IE) on the WLAN
   - **Advertise AP Name**: advertise the AP name status for the WLAN.
   - **Deny LAA (RCM) Clients**: deny the client joining with a locally administered address (random MAC address).
   - **IP Source Guard**: enable IP Source Guard (IPSG).

     IPSG is a Layer 2 security feature that prevents the wireless controller from forwarding the packets with source IP addresses that are not known to it.

   - **Latency Measurements Announcements**: provide latency information about a radio band so that the client can move to a radio band with better latency if the current radio band is overloaded.
   - **Multicast Buffer**: configure multicast buffer tuning mode for 802.11a radio for the WLAN.

     If you check this check box, in the **Multicast Buffer Value** field, enter a value.

     The valid range is from 30 to 60.

- **Opportunistic Key Caching (OKC)**: enable opportunistic key caching (OKC).

  OKC allows the wireless client and the WLAN infrastructure to cache only one Pairwise Master Key (PMK) for the lifetime of the client association with this WLAN, even when roaming between multiple APs.

- **Load Balance**: enable load balance on the WLAN.
- **Media Stream Multicast-Direct**: reliable multicast stream delivery for the WLAN.
- **802.11ac MU-MIMO**: configure 802.11ac MU-MIMO on the WLAN.
- **Universal Admin**: allow universal admin mode to be enabled on a 802.1X, WPA, or WPA2-enabled WLAN.
- **MBO**: enable Wi-Fi Alliance Agile Multiband (MBO) support.

  **Note** For MBO on a WPA2-enabled WLAN, **Protected Management Frame (802.11w)** must be set to **Required** or **Optional**.

- **Wi-Fi to Cellular Steering**: enable Wi-Fi to cellular steering on the WLAN.

  To enable Wi-Fi to cellular steering, you must enable MBO.

c) (Optional) From the **Wi-Fi Direct Client** drop-down list, choose a Wi-Fi direct-related policy on the WLAN.
d) (Optional) Check the required check boxes to configure the corresponding settings.

- **Ignore RSN IE Len**: enable Robust Secure Network Information Element (RSN IE) validation
- **RE Anchor Roam Clients**: configure the reanchor policy for roaming voice clients.
- **Static IP Tunneling**: enable static IP client tunneling support on the WLAN.
- **UAPSD Compliant**: enable Wi-Fi Multimedia (WMM) Unscheduled automatic power save delivery (U-APSD) compliant client support for WLAN

e) Use the **Enable Fine Timing Measurement Responder** toggle button to configure the AP to act as a Fine Timing Measurement (FTM) responder.

   This option is used for location-based services. It allows compatible clients to measure their distance from the AP for precise indoor positioning.

f) Use the **Advertise AP Location** toggle button to broadcast the physical location of the AP in beacon and probe response frames.

   Clients and location-based services can use this information to improve device positioning and navigation accuracy.

g) From the **WMM Policy** drop-down list, choose an option for the policy.
h) From the **mDNS Mode** drop-down list, choose an mDNS operational mode.
i) Under **DTIM Period (in Beacon Intervals)**, in the **5 GHz Band** and **2.4 GHz Band** fields, enter the corresponding Delivery Traffic Indication Map (DTIM) periods.

   The valid range is from 1 to 255. The default value is 1. These fields represent the DTIM configuration per WLAN for each 802.11 network.

**Step 17** Click **Review and Provision**.

**Step 18** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 19** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 20** On the **Tasks** window, monitor the task deployment.

## Create a policy profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a policy profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **SSID** and click **Policy Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **General** tab of the **Create Policy Profile** slide-in pane, complete the required configurations.

a) In the **Policy Profile Name** field, enter a unique name for the policy profile.

The policy profile name can contain up to 32 characters. Catalyst Center does not allow leading or trailing spaces in the policy profile name.

b) (Optional) In the **Description** field, enter a description.

c) Use the toggle buttons to enable or disable the required configurations.

| Toggle button | Description |
|---|---|
| **Status** | To enable or disable the policy profile. |
| **IP MAC Binding** | To configure control over support for IP-MAC address binding creation. |
| **Passive Client** | To enable or disable passive client support on a policy. |
| **Encrypted Traffic Analytics** | To enable the Encrypted Traffic Analytics feature on the WLAN. |

d) Under **WLAN Switching Policy**, enable or disable the required configurations using the toggle buttons.

- **Central Switching**
- **Central DHCP** (for locally switched clients)
- **Central Authentication**
- **Flex NAT/PAT**

**Note** Local switching, central DHCP, and IPv4 DHCP required must be enabled before enabling this option.

e) (Optional) Under **CTS Policy**, configure the required Cisco TrustSec (CTS) policies.

- Check the **Inline Tagging** check box to enable inline tagging for clients.
- Check the **SGACL Enforcement** check box to enable Security Group ACL (SGACL) enforcement of CTS policies on the device.
- In the **Default SGT** field, enter a default Security Group Tag (SGT) value.

  The valid range is from 2 to 65519. The default value is 2.

**Step 6** (Optional) Click **Access Policies** and configure the required access policies.

a) Check the required check boxes to enable the corresponding configurations.

b) Under **WLAN Local Profiling**, in the **Local Subscriber Policy Name** field, enter the name of a policy map.

To create a policy map, refer to Create a policy map for a Cisco Catalyst 9800 Series Wireless Controller, on page 289.

c) Under **VLAN**, complete the required configurations.

- In the **VLAN/VLAN Group** field, enter the text to search for a VLAN or VLAN group. From the drop-down list, choose a VLAN or VLAN group.
- In the **Multicast VLAN** field, enter the multicast VLAN ID associated with the WLAN.

The valid range is from 1 to 4094.

- In the **OSEN Encryption VLAN** field, enter VLAN ID to be used for OSEN encrypted traffic on this WLAN.

  This VLAN can contain up to 8 characters.

d) Under **WLAN ACL**, complete these configurations:

- From the **IPv4 ACL** drop-down list, choose an IPv4 ACL.

  To create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168.

- From the **IPv6 ACL** drop-down list, choose an IPv6 ACL.

  To create an ACL, refer to Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 175.

- In the **Layer 2 ACL** field, enter the name of the Layer 2 ACL for the WLAN.

e) Under **URL Filters**, choose the pre-authentication and post-authentication URL filters from the corresponding drop-down lists.

**Note** We recommend that you use enhanced URL filters for only FlexConnect local switching deployments.

To create URL filters, refer to Create a basic URL filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 186 and Create an enhanced URL filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 187.

**Step 7** Click **QoS and AVC** and complete the required configurations.

a) From the **Auto QoS** drop-down list, choose an auto-QoS mode for the WLAN.
b) (Optional) In the **Re-anchor Classmap Name** field, enter the name of the classmap containing the protocols for selective reanchoring.
c) (Optional) Check the **NBAR Protocol Discovery** check box to enable Network-Based Application Recognition (NBAR) protocol discovery for the WLAN.
d) (Optional) Check the **QBSS Load** check box to advertise QoS-enhanced BSS load IE.
e) (Optional) If you chose the auto-QoS mode **None**, under **QoS SSID Policy** and **QoS Client Policy**, choose QoS SSID policy names from the **Egress** and **Ingress** drop-down lists.

   To create a QoS policy, refer to Create a QoS policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 291.

f) Under **Flow Monitor IPv4** and **Flow Monitor IPv6**, choose flow monitors from the **Egress** and **Ingress** drop-down lists.

   To create a flow monitor, refer to Create a flow monitor for a Cisco Catalyst 9800 Series Wireless Controller, on page 297.

**Step 8** Under **SIP-CAC**, check the required check boxes to enable the corresponding configurations.

| Check box | Description |
|---|---|
| **Call Snooping** | To enable call snoop for the WLAN mapped to the policy profile<br>**Note**<br>When you enable call snoop, you must configure Platinum SSID policies. |
| **Send 486 Busy** | To enable SIP CAC to send 486 busy |
| **Send Disassociate** | To enable SIP CAC send disassociate |

**Step 9** (Optional) Click **Mobility** and configure mobility anchors.

a) Under **Mobility Anchors**, complete the required configurations.

- Check the **Export Anchor** check box to indicate that the WLAN mapped to the policy is an anchor WLAN.

**Note** When you enable this option, central switching is enabled. You must disable the Link Local Bridging feature.

- Check the **Static IP Mobility** check box to enable static IP mobility.

**Note** You can't enable static IP mobility and mobility anchor simultaneously.

b) Under **Anchors**, add or remove mobility anchors.

**Note** This action causes the WLANs that are enabled to be momentarily disabled resulting in loss of connectivity for some clients.

| If you want to... | Then... |
|---|---|
| add an anchor | **1.** Click **Add**.<br>**2.** In the **Add** dialog box<br>• From the **Anchor IP** drop-down list, choose a mobility anchor IP.<br>• From the **Anchor Priority** drop-down list, choose a priority for the mobility anchor.<br>**3.** Click **Save**. |

| If you want to... | Then... |
|---|---|
| edit an anchor | **1.** Check the check box next to the anchor IP.<br>**2.** Hover your cursor over **Actions** and choose **Edit**.<br>**3.** Edit the required configuration.<br>**4.** Click **Save**. |
| delete an anchor | **1.** Check the check box next to the anchor IP.<br>**2.** Hover your cursor over **Actions** and choose **Delete**.<br>**3.** In the dialog box, click **Yes**. |

**Step 10** Click **WLAN Scheduler** and configure a scheduler for WLAN.

| If you want to... | Then... |
|---|---|
| add a WLAN scheduler | **a.** Click **Add**.<br>**b.** In the **Add Wlan Scheduler** dialog box<br>• From the **Calendar Profile Name** drop-down list, choose a calendar profile.<br>• Use the **Client Session Disable** toggle button to enable or disable client session based on the calendar profile.<br>• Use the **Wlan Enable** toggle button to enable or disable the policy profile based on the calendar profile.<br>**c.** Click **Save**. |
| edit a WLAN scheduler | **a.** Check the check box next to the WLAN scheduler.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Edit the required configuration.<br>**d.** Click **Save**. |
| delete WLAN scheduler | **a.** Check the check box next to the WLAN scheduler.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 11** Under **Advanced**, click **WLAN Timeout** and configure the client WLAN timeout.

a) In the **Session Timeout (sec)** field, enter the client session timeout in seconds.

The valid range is from 0 to 86400. The default value is 28800.

b) In the **Idle Timeout (sec)** field, enter the duration of an idle timeout in seconds.

The valid range is from 15 to 100000. The default value is 300.

c) In the **Idle Threshold (bytes)** field, enter the idle threshold in bytes.

The default value is 0.

d) In the **Client Exclusion Timeout** field, enter the client exclusion timeout value.

The valid range is from 0 to 2147483647. The default value is 60.

e) (Optional) Check the **Guest LAN Session Timeout** check box to enable session timeout for guest LAN.

f) (Optional) Check the **Client Exclusion** check box to enable client exclusion for the WLAN.

**Step 12** (Optional) Under **Advanced**, click **WLAN Flex Policy** and configure a WLAN flex policy.

a) Check the **VLAN Central Switching** check box to configure VLAN central switching.

**Note** VLAN-based central switching isn't supported when AAA override is disabled.

b) In the **Split MAC ACL** field, enter the split MAC ACL name.

To create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168.

**Step 13** (Optional) Under **Advanced**, click **AAA Policy** and configure the AAA policy.

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

b) If you enable AAA override, use the **NAC State** check box to enable or disable Network Admission Control (NAC).

If you check this check box, from the **NAC Type** drop-down list, choose an option.

c) Check the **VLAN Fallback** check box to enable fallback to policy profile VLAN when override VLAN is unavailable.

d) From the **AAA Policy Name** drop-down list, choose an AAA policy.

To create an AAA policy, refer to Create an AAA policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 167.

e) From the **Accounting List** drop-down list, choose an accounting list.

To create an accounting list, refer to Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 161.

f) Check the **Interim Accounting** check box to enable interim accounting messages.

**Step 14** (Optional) Under **Advanced**, click **DHCP** and configure DHCP for wireless clients.

a) Check the **IPv4 DHCP Required** check box to enforce DHCP for all the clients on the WLAN.

**Note** This option must be enabled before enabling the **Flex NAT/PAT** option.

b) In the **DHCP Server IP Address** field, enter an IPv4 DHCP server for the WLAN.

c) From the **DHCP Server VRF** drop-down list, choose the VRF name for the IPv4 DHCP server.

To create a VRF interface, refer to Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 320.

d) Use the **Disable DHCP Option** toggle button to enable or disable inclusion of additional DHCP options in DHCP requests for this WLAN.

e) Use the **DHCPv6 Relay Option VPN** toggle button to enable or disable the association of DHCPv6 relay options with a VPN context for the WLAN policy.

f) In the **DHCPv6 Server Address** field, enter the IPv6 address of the IPv6 DHCP server to which the client requests are relayed for the WLAN policy.

Enter a valid IPv6 address that is reachable from the wireless controller. This IPv6 address is required for networks using external IPv6 DHCP servers.

g) From the **DHCPv6 Server VRF Name** drop-down list, choose a VRF name.

To create a VRF interface, refer to Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 320.

h) Check the required check boxes to enable the corresponding DHCP Option 82 configurations.

**Step 15** (Optional) Under **Advanced**, click **DNS Layer Security** and configure DNS layer security.

a) In the **DNS Layer Security Parameter Map** field, enter a map name.

To create an accounting list, refer to Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 161.

b) From the **Flex DNS Traffic Redirect** drop-down list, choose an umbrella DNA traffic redirect option.

c) Check the **Flex DHCP Option for DNS** check box to enable the DNS DHCP option.

**Step 16** (Optional) Under **Advanced**, click **Miscellaneous** and configure miscellaneous wireless profile configurations such as user-defined (private) network, air time fairness, and so on.

a) In the **mDNS Service Policy** field, enter a name for the service policy.

The service policy name can contain up to 64 characters. To create a service policy, refer to Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 272.

b) From the **Hotspot Server** drop-down list, choose a server.

c) Check the required check boxes to enable the corresponding configurations.

- **Link Local Bridging**: enable link-local bridging

**Note** You must disable the WLAN mobility policy anchor when link-local bridging is enabled.

- **Multicast Filter**: enable the filter to drop all multicast downstream packets
- **Rate None**: enable the client Address Resolution Protocol (ARP) rate limiting

d) In the **Burst Interval** field, enter the burst interval in seconds.

The valid range is from 3 to 255. The default value is 5.

e) In the **Rate Pps** field, enter a value for the allowed ARP packet rate.

The valid range is from 15 to 1500. The default value is 100.

f) Use the **L3 Access** toggle button to enable or disable Layer 3 access.

g) Under **User Defined (Private) Network**, check the required check boxes to enable the corresponding configurations.

- **Status**: enable user-defined (private) network
- **Drop Unicast**: set the action to drop the user-defined (private) network unicast traffic

h) Under **Air Time Fairness Policies**, from the **2.4 GHz Policy** and **5 GHz Policy** drop-down lists, choose a corresponding policy.

i) Under **WGB Parameters**, complete the required configurations.

- Check the **Broadcast Tagging** check box to enable workgroup bridge (WGB) broadcast tagging
- Check the **WGB VLAN** check box to enable client VLAN support
- Use the **Multicast Forwarding for Foreign APs** toggle button to enable or disable multicast traffic forwarding for clients connected to foreign APs in guest or mobility scenarios.

j) Under **Policy Proxy Settings**, complete the required configurations.

- Check the **ARP Proxy** check box to enable the ARP proxy feature.
- From the **IPv6 Proxy** drop-down list, choose an IPv6 Neighbor Discovery (ND) proxy feature.

k) Under **EoGRE Tunnel Profile**, from the **Tunnel Profile** drop-down list, choose a tunnel profile.

To create a tunnel profile, refer to Create an EoGRE tunnel profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 301.

**Step 17** Click **Review and Provision**.

**Step 18** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 19** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 20** On the **Tasks** window, monitor the task deployment.

## Create a remote LAN profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a remote LAN (RLAN) profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **SSID** and click **Remote LAN Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **General** tab of the **Create Remote LAN Profile** slide-in pane, complete these configurations.

a) In the **RLAN Profile Name** field, enter a unique name for the RLAN profile.

**Note** Ensure that the RLAN profile name does not match any existing WLAN profile names. Otherwise, the RLAN profile creation task fails.

b) In the **RLAN ID** field, enter an RLAN profile ID.

The valid range is from 1 to 128. The default value is 1.

c) Use the **Status** toggle button to enable or disable the RLAN profile.
d) (Optional) In the **Client Association Limit** field, enter a value for the maximum number of client connections per RLAN. The default value is 0.
e) From the **mDNS Mode** drop-down list, choose a mode on RLAN.

**Step 6** Under **Security**, click **Layer 2** and configure Layer 2 security policies for the RLAN.

a) (Optional) Check the **802.1X** check box to enable 802.1X.
b) (Optional) From the **MAC Filtering** drop-down list, choose an option.

To create an authorization list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159.

c) (Optional) From the **Authentication List** drop-down list, choose an authentication list of type DOT1x.

To create an authentication list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 158.

d) From the **Fallback Mechanism** drop-down list, choose an RLAN fallback authentication type.

e) (Optional) Check the **EAP-Identity-Request Retries Status** check box to enable the EAP identity request retry settings.

- In the **EAP-Identity-Request Max Retries** field, enter the maximum number of EAP identity request retransmissions.

  The valid range is from 1 to 20.

- In the **EAP-Identity-Request Timeout (sec)** field, enter a timeout value for the EAP identity requests in seconds.

  The valid range is from 1 to 120.

f) (Optional) Check the **EAP-Request Retries Status** check box to enable the EAP request retry settings.

- In the **EAP-Request Max Retries** field, enter the maximum number of EAP request retransmissions.

  The valid range is from 1 to 20.

- In the **EAP-Request Timeout (sec)** field, enter a timeout value for the EAP requests in seconds.

  The valid range is from 1 to 120.

**Step 7** (Optional) Under **Security**, click **Layer 3** and configure the Layer 3 policies and ACL for the RLAN.

a) Check the **Web Auth** check box to enable security web authentication.

**Note** You can't enable web authentication and 802.1X simultaneously.

b) From the **Web Auth Parameter Map** drop-down list, choose a map.

To create a web authentication profile, see Create a web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 192.

Associating an RLAN profile with web authentication provides user authentication through a web portal, which enhances security and provides better access control over the wireless network.

c) From the **Authentication List** drop-down list, choose an authentication list of the type login.

To create an authentication list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 158.

d) Under **Preauthentication ACL**, choose the required ACL from the corresponding drop-down list.

- **IPv4** (to create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168)
- **IPv6** (to create an IPv6 ACL, see Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 175)

**Step 8** (Optional) Under **Security**, click **AAA** and check the **Local EAP Authentication** check box to enable an EAP profile on an RLAN.

If you check this check box, from the **EAP Profile Name** drop-down list, choose an EAP profile name.

Associating an RLAN profile with local EAP enhances security, access control, compliance, network performance, user management, troubleshooting, and scalability in a wireless network environment.

**Step 9** Click **Review and Provision**.

**Step 10** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create a remote LAN policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a remote LAN (RLAN) policy for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **SSID** and click **Remote LAN Policies**.

**Step 4** Click **Add**.

**Step 5** In the **General** tab of the **Create Remote LAN Policy** slide-in pane, complete the required configurations.

a) In the **RLAN Policy Name** field, enter a name for the RLAN policy.

The RLAN policy name can contain up to 32 characters.

b) (Optional) In the **Description** field, enter a description.
c) Use the **Status** toggle button to enable or disable the RLAN policy.
d) (Optional) Check the **PoE** check box to enable Point over Ethernet (PoE).
e) From the **Power Level** drop-down list, choose a power level for the AP PoE port.
f) Under **RLAN Switching Policy**, use the **Central Switching** and **Central DHCP** toggle buttons to enable or disable the corresponding configurations.

**Step 6** Click **Access Policies** and complete the required configurations.

a) (Optional) Check the **Pre-Authentication** check box to enable pre-authentication.
b) (Optional) From the **VLAN** drop-down list, enter the text to search for a VLAN. From the drop-down list, choose a VLAN.

To create a VLAN, see Create a VLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 315.

c) From the **Host Mode** drop-down list, choose a host mode for the RLAN.
d) (Optional) Under **RLAN ACL**, choose an IPv4 ACL and IPv6 ACL from the drop-down lists.

- **IPv4 ACL** (to create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168)
- **IPv6 ACL** (to create an IPv6 ACL, see Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 175)

**Step 7** Click **Advanced** and complete the required configurations.

a) From the **Violation Mode** drop-down list, choose a violation mode for the RLAN.
b) (Optional) In the **Session Timeout (sec)** field, enter a value for the session timeout in seconds.

The valid range is from 0 to 86400. The default value is 28800.

**Note** To disable the session timeout, enter 0.

c) (Optional) From the **mDNS Service Policy** drop-down list, choose an mDNS service policy name.

To create an mDNS service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 272.

d) (Optional) Under **User Defined (Private) Network**, check the required check boxes to enable the corresponding configurations.

- **Status**: enable user-defined (private) network
- **Drop Unicast**: set the action to drop the user-defined (private) network unicast traffic

e) (Optional) Under **AAA Policy**, complete the required configurations.

- Check the **AAA Override** check box to enable AAA override.
- From the **AAA Policy Name** drop-down list, choose an AAA policy.

  To create an AAA policy, see Create an AAA policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 167.

- From the **Accounting List** drop-down list, choose an accounting list.

  To create an accounting list, see Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 161.

f) (Optional) Under **Split Tunnel**, complete the required configurations.

- Check the **Status** check box to enable a split tunnel.
- From the **ACL** drop-down list, choose an ACL.

  To create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168.

g) (Optional) Under **Exclusionlist**, complete the required configurations.

- Uncheck the **Status** check box to disable the client exclusion.
- In the **Exclusionlist Timeout** field, enter the time for which the client is excluded.

  The valid range is from 0 to 2147483647. The default value is 60.

h) (Optional) Under **DHCP**, complete the required configurations.

- Check the **IPv4 DHCP Required** check box to enforce DHCP for all the clients on the remote LAN.
- In the **DHCP Server IP Address** field, enter an IPv4 DHCP server for the remote LAN.
- From the **DHCP Server VRF** drop-down list, choose an IPv4 DHCP server VRF name for the remote LAN.

i) Under **Miscellaneous**, check the required check boxes to enable the corresponding configurations.

| Check box | Description |
|---|---|
| **ARP Rate None** | To enable the client Address Resolution Protocol (ARP) rate limiting.<br>If you check this check box, complete these configurations.<br>• In the **ARP Rate PPS** field, enter a value for the allowed ARP packet rate. The valid range is from 15 to 1500. The default value is 100.<br>• In the **ARP Burst Interval** field, enter the burst interval in seconds. The valid range is from 3 to 255. The default value is 5. |
| **NDP Rate None** | To enable the client Neighbor Discovery Protocol (NDP) rate limiting.<br>If you check this check box, complete these configurations.<br>• In the **NDP Rate PPS** field, enter a value for the allowed NDP packet rate. The valid range is from 15 to 1500. The default value is 100.<br>• In the **NDP Burst Interval** field, enter the burst interval in seconds. The valid range is from 3 to 255. The default value is 5. |

**Step 8** Click **Review and Provision**.

**Step 9** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Create a policy tag for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a policy tag for the APs associated with a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **SSID** and click **Policy Tags**.

**Step 4** Click **Add**.

**Step 5** In the **Tag Name** field of the **Create Policy Tags** slide-in pane, enter a unique name for the policy tag.

**Step 6** (Optional) In the **Description** field, enter a description.

**Step 7** (Optional) Under **WLAN Profile - Policy Profile Mapping**, configure the WLAN profile to policy profile mapping.

| If you want to... | Then... |
|---|---|
| add a WLAN profile to policy profile mapping | **a.** Click **Add**.<br>**b.** From the **WLAN Profile** drop-down list, choose a WLAN profile.<br>**c.** From the **Policy Profile** drop-down list, choose a policy profile.<br>**d.** Click **Save**. |
| edit a WLAN profile to policy profile mapping | **a.** Check the check box next to the required WLAN profile name.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Edit the required configurations.<br>**d.** Click **Save**. |
| delete WLAN profile to policy profile mappings | **a.** Check the check box next to the required WLAN profile names.<br>**b.** Hover your cursor over **Actions** and choose **Delete**<br>**c.** In the dialog box, click **Yes**. |

**Step 8** (Optional) Under **RLAN Profile - RLAN Policy Mapping**, configure RLAN profile to RLAN policy mapping.

| If you want to... | Then... |
|---|---|
| add an RLAN profile to RLAN policy mapping | **a.** Click **Add**.<br>**b.** From the **Port ID** drop-down list, choose the RLAN port ID value of the AP.<br>**c.** From the **RLAN Profile** drop-down list, choose an RLAN profile.<br>**d.** From the **RLAN Policy Profile** drop-down list, choose an RLAN policy profile.<br>**e.** Click **Save**. |
| edit an RLAN profile to RLAN policy mapping | **a.** Check the check box next to the required port ID.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Edit the required configurations.<br>**d.** Click **Save**. |
| delete RLAN profile to RLAN policy mappings | **a.** Check the check box next to the required port IDs.<br>**b.** Hover your cursor over **Actions** and choose **Delete**<br>**c.** In the dialog box, click **Yes**. |

**Step 9** Click **Review and Provision**.

**Step 10** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Configure the 802.11be profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure or create an 802.11be profile for a wireless controller and provision it. 802.11be profile is applicable for wireless controllers that are running Cisco IOS XE Release 17.15.1 or later.

Wireless controllers that are running versions earlier than Cisco IOS XE Release 17.18.1 use a single 802.11be profile, which is the default-dot11be-profile. Wireless controllers that are running Cisco IOS XE Release 17.18.1 or later support custom 802.11be profiles.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **SSID** and click **802.11be Profiles**.

**Step 4** Complete one of these applicable configurations:

| If you want to... | Then... |
|---|---|
| configure 802.11be profile for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1 | **a.** Click the radio button next to the default 802.11be profile.<br>**b.** Hover your cursor over **Actions** and click **Edit**. |
| create 802.11be profile for a wireless controller running Cisco IOS XE Release 17.18.1 or later | click **Add**. |

**Step 5** In the **Profile Name** field, enter a unique name for the 802.11be profile for a wireless controller running Cisco IOS XE Release 17.18.1 or later.

The profile name can contain up to 32 characters. Catalyst Center does not support leading and trailing spaces in the profile name.

**Step 6** (Optional) In the **Description** field, update the description.

The description can contain up to 64 characters,

**Step 7** (Optional) Use the available toggle buttons to enable or disable the corresponding parameters.

- **Downlink OFDMA**: enables downlink connection to use OFDMA for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1.
- **Uplink OFDMA**: enables uplink connection to use OFDMA for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1.
- **Downlink MU-MIMO**: enables downlink connection to use MU-MIMO for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1.
- **Uplink MU-MIMO**: enables uplink connection to use MU-MIMO for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1.
- **OFDMA Multi-RU**: enables the assignment of multiple Resource Units (RUs) simultaneously to a single user using OFDMA.



**Note** To configure OFDMA and MU-MIMO for a wireless controller running Cisco IOS XE Release 17.18.1 or later, use the **Advanced** > **11ax** tab in the WLAN profile. For more information, see Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 66.

**Step 8** (Optional) Use the toggle buttons to enable or disable these MLO group configurations for a wireless controller running Cisco IOS XE Release 17.18.1 or later:

- **Primary 2.4GHz**: configures the 2.4-GHz band in the MLO group
- **Primary 5GHz**: configures the 5-GHz band in the MLO group
- **Secondary 5GHz**: configures a secondary 5-GHz band in the MLO group
- **Primary 6GHz**: configures the 6-GHz band in the MLO group

**Step 9** Click **Review and Provision**.

**Step 10** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

# RF configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device RF configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Create an RF profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an RF profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **RF** and click **RF Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **General** tab of the **Create RF Profiles** slide-in pane, configure the required parameters.

a) In the **RF Profile Name** field, enter a unique name for the RF profile.

The profile name can contain up to 32 characters. Catalyst Center does not allow the ? character in the profile name.

b) (Optional) In the **Description** field, enter a description.

c) From the **Radio Band** drop-down list, choose a radio band for the RF profile.

If you chose **6 GHz**, you can optionally allow the AP to operate in the standard power mode. Check the **Allow Standard Power Mode** check box to enable standard power mode.

d) Use the **Status** toggle button to enable or disable the RF profile.

e) From the **NDP Mode** drop-down list, choose an operating mode.

**Step 6** Click **802.11** and do these steps:

a) Under **Operational Data Rates**, choose the required configuration for the corresponding data rates from the drop-down lists.

b) For the 5-GHz and 2.4-GHz bands, under **802.11n MCS Rates**, check the check box for the required Modulation Coding Scheme (MCS) index.

**Step 7** Under **RRM**, click **Trap Thresholds** and complete the required configurations.

a) In the **Interference (%)** field, enter an interference threshold in percent.

The valid range is from 0 to 100. The default value is 10.

When the interference exceeds this threshold, traps are generated.

b) In the **Clients** field, enter a threshold for the number of clients per AP radio to trigger a trap.

The valid range is from 1 to 200. The default value is 12.

c) In the **Noise (dBm)** field, enter the noise threshold in dBm.

The valid range is from -127 to 0. The default value is -70.

d) In the **Utilization (%)** field, enter a threshold for the bandwidth used by an AP in percent.

The valid range is from 0 to 100. The default value is 80.

**Step 8** Under **RRM**, click **Coverage** and complete the required configurations.

a) In the **Minimum Client Level (clients)** field, enter the minimum client exception level.

The valid range is from 1 to 200. The default value is 3.

b) In the **Data RSSI Threshold (dBm)** field, enter the Received Signal Strength Indicator (RSSI) threshold value for data packets in dBm.

The valid range is from -90 to -60. The default value is -80.

c) In the **Voice RSSI Threshold (dBm)** field, enter the RSSI threshold value for voice packets in dBm.

The valid range is from -90 to -60. The default value is -80.

d) In the **Exception Level (%)** field, enter the coverage exception level in percent.

The valid range is from 1 to 100. The default value is 25.

**Step 9** Under **RRM**, click **TPC** and complete the required configurations.

a) In the **Maximum Power Level (dBm)** field, enter the upper limit of the transmit power in dBm.

The valid range is from -10 to 30. The default value is 30.

For 802.11 networks, this configuration is accepted only when Transmit Power Control (TPC) is in Auto or Run Once mode.

b) In the **Minimum Power Level (dBm)** field, enter the lower limit of the transmit power in dBm.

The valid range is from -10 to 30. The default value is -10.

For 802.11 networks, this configuration is accepted only when TPC is in Auto or Run Once mode.

c) In the **Power Control Threshold (dBm)** field, enter the TPC version 1 threshold for RRM in dBm.

The valid range is from -80 to -50. The default value is -70.

d) In the **Tx Power V2 Threshold** field, enter the TPC version 2 threshold for RRM in dBm.

The valid range is from -80 to -50. The default value is -67.

**Step 10** Under **RRM**, click **DCA** and complete the required configurations.

a) (Optional) Check the **Avoid AP Foreign AP Interference** check box to configure Dynamic Channel Assignment (DCA) for RF profiles.

If you configure DCA, the device RRM algorithms consider 802.11 traffic from foreign APs that aren't included in your wireless network when assigning channels.

b) Under **DCA Channels**, check the check box for the required channel numbers.

c) (Optional) Check the **Zero Wait DFS** check box to enable the 802.11a Zero Wait DFS feature.

**Note** This feature is applicable for only the 5-GHz band.

d) From the **Channel Width** drop-down list, choose a DCA channel width for the RF profile.

**Note** This drop-down list is available for only the 6-GHz and 5-GHz bands.

e) If you chose the 5-GHz or 6-GHz band, choose the minimum and maximum channel width allowed for DBS from the **Channel Width Min** and **Channel Width Max** drop-down lists.

f) (Optional) Check the **PSC Enforcement** check box to enable Preferred Channel Scanning (PSC) for the 6-GHz DCA.

g) Under **High Speed Roam**, complete these configurations.

- For the 2.4-GHz and 5-GHz bands, complete these configurations:
  - (Optional) check the **Mode Enable** check box to configure high-speed roam (HSR) mode for the RF profile, and
  - In the **Neighbor Timeout** field, enter the timeout interval of the neighbors for the RF profile.

    The valid range is from 5 to 60. The default value is 5.
- From the **Client Network Preference** drop-down list, choose a client network preference.

- **Connectivity**: the RRM algorithm uses connectivity of the clients as network preference.
- **Throughput (Bps)**: the RRM algorithm uses the high throughput of the clients as network preference.
- **Default**: the RRM algorithm doesn't use any network preferences.

**Step 11** If you chose the 2.4-GHz band, under **RRM**, click **Band Select** and complete these configurations.

a) (Optional) Check the **Band Select Probe Response** check box to enable the 802.11ax broadcast probe response.

b) In the **Client RSSI (dBm)** field, enter the minimum mobile station RSSI threshold in dBm.

The valid range is from -90 to -20. The default value is -80.

c) In the **Client Mid-RSSI (dBm)** field, enter the medium mobile station RSSI threshold in dBm.

The valid range is from -90 to -20. The default value is -80.

d) In the **Cycle Count (cycles)** field, enter the number of suppression cycles for a new client.

The valid range is from 1 to 10. The default value is 2.

e) In the **Cycle Threshold (msec)** field, enter the scan cycle threshold for band select in milliseconds.

The valid range is from 1 to 1000. The default value is 200.

f) In the **Expire Dual Band (sec)** field, enter the expiration time for dual band in seconds.

The valid range is from 10 to 300. The default value is 60.

g) In the **Expire Suppression (sec)** field, enter the expiration time of suppression in seconds.

The valid range is from 10 to 200. The default value is 20.

**Step 12** Click **802.11ax** and complete the required configurations.

a) If you chose the 6-GHz band, complete these configurations.

- From the **6 GHz Discovery Frames** drop-down list, choose a discovery frame for the 802.11ax 6-GHz band.
- In the **He Bcast Probe Resp Intvl** field, enter an 802.11ax broadcast probe response interval.

  The valid range is from 5 to 25. The default value is 20.
- From the **Multi BSSID Profile** drop-down list, choose a multi-BSSID profile.

  To create a multi-BSSID profile, refer to Create a multi-BSSID profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 107.

b) Under **Spatial Reuse**, complete the required configurations.

- (Optional) Check the **OBSS PD** check box to enable Overlapping BSS Packet Detect (OBSS-PD) spatial reuse.
- 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 to -62. The default value is -62.
- (Optional) Check the **SRG OBSS PD** check box to enable SRG OBSS-PD spatial reuse.
- 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 to -62. The default value is -82.

- 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 o -62. The default value is -62.

**Step 13** Click **Advanced** and complete the required configurations.

a) (Optional) In the **A-MPDU Window Size** field, enter Aggregated MAC Protocol Data Unit (A-MPDU) window size.

   The valid range is from 1 to 255. The default value is 255.

b) Under **High Density Parameters**, complete the required configurations.

   - In the **Max Clients** field, enter the maximum number of clients per AP in a high-density environment.

     The valid range is from 0 to 500. The default value is 200.

   - From the **Multicast Data Rate (Mbps)** drop-down list, choose a minimum data rate at which the multicast clients can associate with AP.

     **Note** The value 0 indicates that the AP automatically adjusts the data rates.

   - From the **Rx SOP Threshold (dBm)** drop-down list, choose a Receiver Start of Packet Detection (RX SOP) sensitivity threshold in dBm.

     If you chose 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 to -60.

c) Under **Client Distribution**, complete the required configurations.

   - In the **Load Balancing Window** field, enter the number of clients to load balance across APs.

     The valid range is from 0 to 20. The default value is 5.

   - In the **Load Balancing Denial Count** field, enter the load balance denial count for APs.

     The valid range is from 1 to 10. The default value is 3.

d) Under **ATF Configuration**, complete the required configurations.

   From the **ATF Optimization** drop-down list, choose an option to enable or disable airtime fairness for the RF profile. When airtime fairness optimization is enabled, the wireless controller dynamically reallocates airtime from underutilized clients to the clients that need more bandwidth. This optimization improves network efficiency.

   For the 5-GHz and 2.4-GHz bands, complete these configurations:

   - From the **Status** drop-down list, configure the airtime fairness operating mode.
   - Check the **Bridge Client Access** check box to enable the air time allocation mode on the default RF policy.

     If you check this check box, in the **Airtime Allocation** field, you can optionally enter an air time allocation weight percentage.

     The valid range is from 5 to 90. The default value is 5.

e) Under **FRA**, complete the required configurations.

| Band | Action |
|---|---|
| 6 GHz | • In the **Client Reset Count** field, enter the client-aware FRA client count for dual-band radios to switch from the 6-GHz to 5-GHz band.<br>The valid range is from 1 to 10. The default value is 1.<br>• In the **Client utilization threshold (%)** field, enter the client-aware FRA utilization threshold value for dual-band radios to switch from the 6-GHz to 5-GHz band. |
| 5 GHz | Use the **Client Aware** check box to enable or disable client-aware FRA.<br>Client-aware FRA allows the dual-band radios to operate in 5-GHz or monitor mode depending on the load on the dedicated 5-GHz band.<br>If you check this check box, enter data in these fields:<br>• **Client Select**: enter the client-aware FRA utilization threshold value for dual-band radios to switch from monitor mode to client-serving mode.<br>The valid range is from 0 to 100. The default value is 50.<br>• **Client Select**: enter the client-aware FRA utilization threshold value for dual-band radios to switch from client-serving mode to monitor mode.<br>The valid range is from 0 to 100. The default value is 5. |
| 2.4 GHz | From the **FRA Action** drop-down list, choose an FRA action for dual-band radios. |

f) Under **RSSI Settings**, complete the required configurations.

- (Optional) Check the **RSSI Low Check** check box to indicate if the RSSI low check is enabled before enabling the optimized roaming feature.
- In the **RSSI Threshold (dBm)** field, enter the minimum RSSI threshold for optimized roaming.

  The valid range is from -127 to 0. The default value is -127.

g) Under **UNII Band Settings**, use the **UNII-3 Low Power Channels** check box to enable or disable the use of UNII-3 low power channels within the 5-GHz band for the RF profile.

When enabled, APs can use these channels to potentially reduce interference and improve the network performance.

**Note** This check box is not applicable to the 6-GHz and 2.4-GHz bands.

h) (Optional) Under **Retry Limits**, enter data in these fields:

- **Aggregate Retries**: enter the maximum number of retransmission attempts for aggregated data frames before dropping them.

  The valid range is from -1 to 255. The default value is -1.

- **Management Retries**: enter the maximum number of retransmission attempts for management frames before dropping them.

  The valid range is from -1 to 255. The default value is -1.

- **Non-Aggregate Retries**: enter the maximum number of retransmission attempts for non-aggregated data frames before dropping them.

  The valid range is from -1 to 255. The default value is -1.

**Step 14** Click **802.11be** and use the **Preamble Puncture** toggle button to enable or disable preamble puncturing.

Preamble puncturing improves spectral efficiency by excluding portions of channels with interference while maintaining wider bandwidths.



**Note** This tab is not available for the 2.4-GHz band.

**Step 15** Click **Review and Provision**.

**Step 16** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 17** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 18** On the **Tasks** window, monitor the task deployment.

## Create a radio profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a radio antenna profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **RF** and click **Radio Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **General** tab of the **Create Radio Profile** slide-in pane, complete these configurations:

a) In the **Radio Profile Name** field, enter a unique name for the radio antenna profile.

The profile name can contain up to 32 characters. Catalyst Center does not support leading and trailing spaces in the profile name.

b) (Optional) In the **Description** field, enter a description.
c) From the **Antenna Beam** drop-down list, choose a beam steering mode for the AP slot.
d) (Optional) In the **Number of Antennas to be Enabled** field, enter the number of antennas to be enabled for the AP slot.

The valid range is from 0 to 8.

e) (Optional) Check the required check boxes to enable the corresponding configurations.

| Check box | Description |
|---|---|
| **Mesh Backhaul** | To enable mesh backhaul on this radio. |
| **Mesh Designated Downlink** | To use this radio as a designated mesh downlink backhaul.<br>If a designated downlink backhaul is available, the uplink radio isn't used as a downlink radio. |

f) From the **Wireless Active Testing Radio Administrative State** drop-down list, choose the required state.

If you choose **Enabled (Always)**, the radio is always available to be selected for Wireless Active Testing (WAT).

g) Under **DTIM Period**, in the **6 GHz Band** field, enter a Delivery Traffic Indication Map (DTIM) interval for the 6-GHz band.

The valid range is from 1 to 255. The default value is 1.

**Step 6** In the **URWB** tab, from the **URWB Radio Role** drop-down list, choose a radio role.

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create an RF tag for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an RF tag for the APs associated with a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **RF** and click **RF Tags**.

**Step 4** Click **Add**.

**Step 5** In the **Tag Name** field of the **Create RF Tag** slide-in pane, enter a unique name for the RF tag.

The name can contain up to 32 characters.

**Step 6** (Optional) In the **Description** field, enter a description.

**Step 7** (Optional) From these drop-down lists, choose the required RF profile for the corresponding band.

- **6 GHz RF Profile** (to create a 6-GHz RF profile, see Create an RF profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 97)
- **5 GHz RF Profile** (to create a 5-GHz RF profile, see Create an RF profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 97)
- **2.4 GHz RF Profile** (to create a 2.4-GHz RF profile, see Create an RF profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 97)

**Step 8** From the **AP Beam State** drop-down list, choose the beamforming state of the AP.

**Step 9** (Optional) Click **Show Slot Configuration** to view and update the slot configurations.

From these drop-down lists, choose the required radio antenna profile for the corresponding band and slot.

- **6 GHz Slot 2 Radio Profile**
- **6 GHz Slot 3 Radio Profile**
- **6 GHz Slot 1 Radio Profile**
- **5 GHz Slot 1 Radio Profile**
- **5 GHz Slot 2 Radio Profile**
- **5 GHz Slot 0 Radio Profile**
- **2.4 GHz Slot 0 Radio Profile**
- **2.4 GHz Slot 2 Radio Profile**

To create a radio antenna profile, refer to Create a radio profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 103.

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Create a multi-BSSID profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a multi-basic service set identifier (BSSID) profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **RF** and click **Multi BSSID Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **Multi BSSID Profile Name** field of the **Create Multi BSSID Profile** slide-in pane, enter a name for the multi-BSSID profile.

**Step 6** (Optional) In the **Description** field, enter a description.

**Step 7** (Optional) Under **802.11ax**, use the available check boxes to enable the corresponding parameters.

**Step 8** (Optional) Under **802.11be**, use the available check boxes to enable the corresponding parameters.

**Note** For a wireless controller running Cisco IOS XE Release 17.18.1 or later, use the **Downlink OFDMA**, **Uplink OFDMA**, **Downlink MU-MIMO**, and **Uplink MU-MIMO** check boxes under **802.11ax** in Step 7, on page 107 to configure the corresponding parameters.

**Step 9** Click **Review and Provision**.

**Step 10** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |

| Option | Description |
|---|---|
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create a URWB network profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a Ultra Reliable Wireless Backhaul (URWB) network profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the URWB network profile configuration page.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.
d) Click the device name.
e) In the dialog box with the device information, click **View Device Details** to open the device details window.
f) In the **Configuration** tab, expand **RF** and click **URWB Network Profile**.

**Step 2** Click **Add**. In the **General** tab of the **Create URWB Network Profile** slide-in pane, configure the settings as described:

a) Click the **URWB Status** toggle button to enable the URWB feature.
b) In the **URWB Network Profile Name** field, enter a unique name for the URWB network profile.
c) (Optional) In the **Description** field, enter a description.
d) Check the **Strong Network Key** check box to configure a strong password evaluation for the network key.
e) Select **Unencrypted** or **AES** from the **Network Key Type** drop-down list.
f) In the **Network Key** field, enter the URWB network key.

The network key must be between 8 and 63 characters long. Additionally, the network key must include at least one uppercase letter, one lowercase letter, and at least one digit or special character.

**Step 3** In the **Mobility** tab of the **Create URWB Network Profile** slide-in pane, configure these settings:

a) In the **Mobility Role** drop-down list, select **Base**, **Base Relay**, or **Client** for the Backhaul device.
b) In the **Traffic Egress Point** field, select the coordinator or the wireless controller for mobility traffic.
c) Configure these **Mobility Backhaul Check** parameters:
   1. **Ethernet Down**: Configure handoff when all ethernet ports are disconnected.
   2. **Coordinator Down**: Configure handoff when coordinator is unreachable.
d) Configure these **Mobility Scan** parameters:
   1. **Isolation**: Enter the timeout value to trigger an active scan when the device is disconnected from the infrastructure.
   2. **Periodic**: Enter the time interval to perform periodic background channel scanning while the device is idle.
   3. **RSSI Threshold**: Enter the RSSI threshold value to trigger scanning when the received signal strength falls below this level.

**Step 4** In the **MPO** tab, configure the **Packet Duplication Mode**.

**Step 5** In the **Advanced** tab, complete these configurations:
a) In the **Ethernet Protocols** area, choose **None**, **All**, or a specific protocol from the **Allow Ether Types** drop-down list.

   To allow only custom Ether values, select **List** from the **Allow Ether Types** drop-down list.
b) Check the **Legacy Ethernet** check box to allow Ethernet I frames forwarding.
c) In the **Unicast** area, check the **Unicast Flood** check box to enable unicast flood and enter unicast flood limitation.
d) Check the **Unicast Flood Limitation** check box to flood one packet every 5 seconds
e) Select the **Multicast** option from the drop-down list.
f) In the **High Availability** area, check the **High Availability Enabled** check box.
g) In the **High Availability Timeout** field, enter the timeout value.

**Step 6** In the **Wired Ports** tab, complete these configurations:
a) (Optional) In the **Ethernet Settings area**, select the port associated with the URWB network profile from the **Secondary LAN Port** drop-down list.
b) Check the **LAN Port PoE** check box to specify whether Power over Ethernet is configured for the secondary LAN port associated with this profile.

   Only the C9124AXI, C9124AXE, and C9124AXD models support LAN Port PoE.
c) In the **Local Authentication** area, choose the server from the **RADIUS Server Group** drop-down list to be used for authentication, authorization and accounting in this wireless profile.

   This option is disabled if the mobility role is not client. To create a RADIUS server group, refer to Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 153.
d) In the **NAT** area, complete these configurations:
   1. **Enable NAT**: Check this check box to configure NAT settings for the URWB profile.
   2. **NAT Address**: Enter the public IP address to be used for NAT. This address will be presented to external networks for client traffic originating from this wireless profile.
   3. **Netmask**: Enter the subnet mask for the NAT IP address. This defines the network range for NAT operations and should match your network's addressing scheme.

4. **Outside Port Range**: Enter the starting port number and ending port number for the range of outbound NAT ports.
5. **NAT Rules:** Click **Add** to create NAT rules using these parameters:
   - **Protocol**: Choose the TDP or UDP protocol from the drop-down list.
   - **Outside Port**: Enter a port number between 1 and 65535.
   - **Inside IP**: Enter a valid IPv4 address.
   - **Inside Port**: Enter a port number between 1 and 65535.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Edit default RF settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to edit the default RF settings for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **RF** and click **RF Defaults**.

**Step 4** Select the required band. Hover your cursor over **Actions** and choose **Edit**.

Alternatively, click the required band.

**Step 5** In the **Edit RF Defaults** slide-in pane, under **Roaming & Client Settings**, complete these configurations:

- In the **Maximum Clients per Radio** field, enter the maximum number of clients allowed to connect to each radio on APs that use this band.

  The valid range is from 0 to 500.

- From the **Client Network Preference** drop-down list, choose the preferred network behavior for clients associated with this band.
  - **Connectivity Optimized**: Prioritize stable connection.
  - **Throughput Optimized**: Maximize data rates.
  - **Default (Controller Decision)**: Use the default settings on the wireless controller.

**Step 6** (Optional) For the default 5-GHz RF profile, under **Channel Width Settings**, select the minimum and maximum channel width allowed for dynamic bandwidth selection from the corresponding drop-down lists.

**Note** The minimum channel width must be less than or equal to the maximum channel width.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

# AP configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device AP configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Create an AP join profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AP join profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **AP** and click **AP Join Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **General** tab of the **Create AP Join Profile** slide-in pane, complete these configurations.

a) In the **AP Join Profile Name** field, enter a unique name for the AP join profile.

AP join profile name can contain up to 32 characters. Catalyst Center does not allow leading and trailing spaces in the AP join profile name.

b) (Optional) In the **Description** field, enter a description.

c) From the **Country Code** drop-down list, choose a country code for the AP.



**Important** As required by the End-User License Agreement (EULA), choose an appropriate country code to ensure that the network complies with local and national regulatory restrictions. Improper country code assignment can disrupt wireless transmissions and result in government-imposed penalties and sanctions on wireless network operators using devices with incorrect country codes.

d) From the **Time Zone** drop-down list, choose an option for the time zone.

If you chose **Delta From WLC**, in the **Offset** area, enter data in these fields.

- **HH**: enter an offset hour for time zone.

  The valid range is from -12 to 14. The default value is 0.

- **MM**: enter an offset minute for time zone.

  The valid range is from 0 to 59. The default value is 0.

e) From the **Deployment Mode** drop-down list, choose an AP deployment mode.



**Note** Changing the deployment mode may cause the AP to rejoin and result in loss of connectivity for the associated clients.

f) Check the required check boxes to enable the corresponding configurations.

- **LED State**: enable the LED status
- **USB Enable**: enable USB
- **LAG Mode**: enable the AP LAG mode
- **Apphost**: enable IOX application hosting

g) (Optional) In the **NTP Server** field, enter a valid NTP server IP address.

h) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Fallback to DHCP**: enable AP fallback to DHCP

  When this check box is checked, if the AP fails to join through the static IP address, the AP falls back to the DHCP.

- **GAS AP Rate Limit**: enable the Generic Advertisement Services (GAS) rate limit on the AP

  If you check this check box, enter data in these fields.

- **GAS Request limit interval (msec)**: enter the interval to define the GAS request rate limit in milliseconds.

  The valid range is from 100 to 10000.

- **Maximum Allowed GAS/ANQP Requests**: enter the maximum number of GAS requests allowed per AP slot in an interval.

  The valid range is from 1 to 100.

i) (Optional) Enter data in these fields.

- **NTP Server Info Key**: enter a key ID that identifies the NTP authentication key.

  The valid range is from 1 to 65535. The default value is 1.

- **NTP Server Trust Key**: enter the trust key to use in NTP authentication.

j) From the **NTP Server Key type** drop-down list, choose the encryption to use when storing the trust key locally.

k) (Optional) In the **Led Flash (sec)** field, enter the LED flash timer duration for AP in seconds.

The valid range is from 0 to 3600. The default value is 0.

l) (Optional) Check the **DHCP Server Enable** check box to enable the DHCP server.

m) (Optional) In the **Fast Channel** field, enter a value for the fast channel mode number.

The valid range is from 0 to 4294967295.

n) Under **OfficeExtend AP Configuration**, check the required check boxes to enable the corresponding configurations.

- **Local Access**: enable local access on Office Extended AP (OEAP)
- **Rogue Detection**: enable rogue detection on OEAP
- **Link Encryption**: enable data encryption on OEAP
- **Provisioning SSID**: enable provisional SSID on OEAP

o) Under **Antenna Monitoring**, complete these configurations.

- (Optional) Check the **Antenna Monitoring** check box to enable antenna monitoring.
- In the **RSSI Fail Threshold (dB)** field, enter the RSSI failure threshold value for antenna monitoring in dB.

  The valid range is from 10 to 90. The default value is 40.

- In the **Weak RSSI (dBm)** field, enter the weak RSSI value for antenna monitoring.

  The valid range is from -90 to -10. The default value is -60.

- In the **Detection Time (min)** field, enter the detection time for antenna monitoring.

  The valid range is from 9 to 180. The default value is 12.

**Step 6** Click **Client** and complete these configurations.

a) In the **Maximum Client Limit** field, enter the maximum number of clients per AP configuration.

The valid range is from 0 to 1200. The default value is 0.

b) In the **Statistics Timer (sec)** field, enter the time in seconds that the AP sends its 802.11 statistics to the wireless controller.

c) (Optional) Check the **RSSI Client Statistics** check box to enable client RSSI statistics reporting from AP.
d) (Optional) In the **RSSI Statistics Interval** field, enter the reporting interval for the client RSSI statistics from AP to wireless controller.

The valid range is from 30 to 300. The default value is 30.

e) Under **TCP MSS Configuration**, complete these configurations.

- (Optional) Use the **Enable Adjust MSS** check box to enable or disable the TCP MSS adjustment.
- In the **Adjust MSS** field, enter the global AP TCP MSS value.

  The valid range is from 536 to 1363. The default value is 1250.

**Step 7** Under **CAPWAP**, click **High Availability** and complete these configurations.

a) Under **CAPWAP Timers**, enter data in these fields.

- **Fast Heartbeat Timeout (sec)**: enter a timeout value for the heartbeat timer for all APs in seconds.

  The valid range is from 0 to 10. The default value is 0.
- **Heartbeat Timeout (sec)**: enter a timeout value for the heartbeat timer for AP discovery in seconds.

  The valid range is from 0 to 30. The default value is 30.
- **Discovery Timeout (sec)**: enter a timeout value for the AP discovery in seconds.

  The valid range is from 1 to 10. The default value is 10.
- **Primary Discovery Timeout (sec)**: enter a timeout value for the primary AP discovery in seconds.

  The valid range is from 30 to 3000. The default value is 120.
- **Primed Join Timeout (sec)**: enter a primed timeout value for AP discovery in seconds.

  The valid range is from 0 to 43200. The default value is 0.

b) Under **Retransmit Timers**, enter data in these fields.

- **Count**: enter the retransmit timer count.

  The valid range is from 3 to 8. The default value is 5.
- **Interval (sec)**: enter the retransmit timer interval in seconds.

  The valid range is from 2 to 5. The default value is 3.

c) Under **AP Fallback to Primary Controller**, use the **Enable** check box to enable or disable fallback to backup controllers.

Fallback applies to the primary controller and doesn't apply to the backup primary controller.

d) (Optional) Under **Backup Primary Controller** and **Backup Secondary Controller**, enter data in these fields.

- **Name**: enter the controller name for the AP
- **IPv4/IPv6 Address**: enter the IP address of the controller for the AP

**Step 8** Under **CAPWAP**, click **Advanced** and complete these configurations.

a) Check the required check boxes to enable the corresponding configurations.

**Enable Data Encryption**: enable data encryption for the AP

- **Enable Jumbo MTU**: enable Jumbo MTU for the AP

b) From the **Link Latency** drop-down list, choose a link auditing option.
c) From the **Preferred Mode** drop-down list, choose a preferred mode for CAPWAP.
d) In the **CAPWAP Window Size** field, enter a CAPWAP window size for request packets in a multiwindow queue.

The valid range is from 1 to 50. The default value is 1.

e) Under **Discovery**, complete these configurations:

- Use the **Private** check box to enable or disable discovery response from a private IP address.
- Use the **Public** check box to enable or disable discovery response from public IP address.
- From the **Onboarding Configuration** drop-down list, choose the CAPWAP discovery onboarding configuration for AP.

**Step 9** Under **AP**, click **General** and complete these configurations.

a) Under **Power Over Ethernet**, complete these configurations.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Switch Flag**: enable 802.3af switches
  - **Power Injector State**: if a power injector is being used
- From the **Power Injector Type** drop-down list, choose the type of power injector.

  If you chose **Installed** or **Override**, in the **Injector Switch MAC** field, enter the MAC address of the power injector switch.

b) Under **AP EAP Authentication**, complete these configurations.

Under **EAP Type**, choose an authentication method.

- **No-Auth**: default authentication method.
- **EAP-TLS**: EAP-Transport Level Security (EAP-TLS) uses certificate-based authentication.

  If you choose EAP-TLS, enter a username. Catalyst Center generates a certificate and applies it during the PnP claim process.
- **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 to be applied during the PnP claim process.

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 the 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.

From the **AP Authorization Type** drop-down list, choose a Locally Significant Certificates (LSC) AP authorization type.

c) Under **Client Statistics Reporting Interval**, enter a report interval (in seconds) at which the AP sends client statistics for all the clients connected to the corresponding band in the **5 GHz (sec)** and **2.4 GHz (sec)** fields.

The valid range is from 5 to 90. The default value is 90.

d) (Optional) Under **Extended Module**, check the **Enable** check box to enable the AP extended module.

e) (Optional) Under **Mesh**, in the **Mesh Profile Name** field, enter a mesh profile name.

To create a mesh profile, see Create a mesh profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 130.

f) (Optional) Under **Interface Settings**, in the **AP Static MTU Size** field, enter the Maximum Transmission Unit (MTU) size for AP.

The valid values are 0 (to disable) or range from 576 and 1485.

g) (Optional) Under **MACsec Encryption**, complete these configurations.

- Check the **Enable MACsec Encryption** check box to enable Media Access Control Security (MACsec) for AP. This option provides Layer 2 encryption, enhancing security on wired connections to protect data in transit between the AP and wireless controller.
- From the **MACsec Pre-shared Key Chain** drop-down list, choose a key chain.

  To create a key chain, see Create a key chain for a Cisco Catalyst 9800 Series Wireless Controller, on page 212.
- In the **MACsec Replay Window Size** field, enter a number to specify the size of the replay protection window for MACsec.

  This value determines how many out-of-order packets are accepted, helping to prevent replay attacks while accommodating some network jitter.
- Check the **Automatic MACsec** check box to enable automatic detection and MACsec establishment between Cisco Catalyst 9350 Switches and Wi-Fi 7 APs that support this feature.

h) (Optional) Under **Advanced AP Features**, check the required check boxes to enable the corresponding configurations.

- **RLAN Fast Switching**: enable or disable fast switching for Remote LAN (RLAN) interfaces. When enabled, APs can switch RLAN traffic efficiently and reduce latency.
- **NSI Ports**: enable or disable the Network Service Interface (NSI) on the AP.

  NSI ports are used for advanced network network services and diagnostics.
- **CAPWAP Packet Aggregation**: enable or disable CAPWAP aggregation for the AP.

  Aggregation improves performance by reducing overhead on CAPWAP tunnels.
- **Accelerometer Sensor**: enable or disable the accelerometer sensor on the AP. When enabled, AP can detect motion or tampering events.

**Step 10** (Optional) Under **AP**, click **Power Management** and complete these configurations.

a) Under **Regular Power Profile**, from the **Regular Power Profile** drop-down list, choose a power profile that is applied to APs.

If an AP doesn't receive the required power, it functions in a derated state as defined by the sequence of rules in the power profile.

To create a power profile, see Create a power profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 134.

b) Under **Calendar Profile - Power Profile Mapping**, configure power profile mapping.

| If you want to... | Then... |
|---|---|
| add a power profile mapping | 1. Click **Add Mapping**.<br>2. In the **Add Calendar Profile - Power Profile Mapping** dialog box, from the **Calendar Profile** drop-down list, choose a calendar profile.<br>To create a calendar profile, see Create a calendar profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 142.<br>3. From the **Power Profile** drop-down list, choose a power profile.<br>To create a power profile, see Create a power profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 134.<br>4. Click **Save**. |
| edit a power profile mapping | 1. Check the check box next to the required calendar profile.<br>2. Hover your cursor over **Actions**, and choose **Edit**.<br>3. Edit the mapping.<br>4. Click **Save**. |
| delete a power profile mapping | 1. Check the check box next to the required calendar profile.<br>2. Hover your cursor over **Actions** and choose **Delete**<br>3. In the dialog box, click **Yes**. |

**Step 11** Under **AP**, click **Hyperlocation** and complete these configurations.

a) (Optional) Check the **Enable Hyperlocation** check box to enable hyperlocation.

b) If you uncheck the **Enable Hyperlocation** check box, enter data in these fields.

- **Detection Threshold (dBm)**: enter a value to filter out packets with low RSSI.

  The valid range is from -100 to -50. The default value is -100.

- **Trigger Threshold (cycles)**: enter a value to set the number of scan cycles before sending a BAR to clients.

  The valid range is from 1 to 100. The default value is 10.

- **Reset Threshold**: enter a value to reset the value in scan cycles after the trigger.

  The valid range is from 0 to 99. The default value is 8.

**Step 12** Under **AP**, click **AP Statistics** and complete these configurations.

a) Under **System Monitoring**, complete these configurations.

- (Optional) Check the **Monitor Real Time Statistics** check box to enable AP statistics collection and processing.
- (Optional) Check the **Trigger Alarm for AP** check box to enable the AP statistics alarm.
- In the **CPU Threshold to Trigger Alarm (%)** and **Memory Threshold to Trigger Alarm (%)** fields, enter the threshold percentage for CPU and memory usage respectively.

  The valid range is from 0 to 100. The default value is 0.

  An SNMP trap is sent when this threshold is crossed.
- In the **Interval to Hold Alarm (sec)** field, enter the time in seconds for which the alarm is held before it gets triggered.

  The valid range is from 0 to 3600. The default value is 6.
- In the **Trap Retransmission Time (sec)** field, enter the time between retransmissions of the alarm in seconds.

  The valid range is from 0 to 65535. The default value is 0.
- In the **Sampling Interval (sec)** field, enter a value in seconds to define how often the data is collected from the AP.

  The valid range is from 2 to 900. The default value is 30.
- In the **Statistics Interval (sec)** field, enter a value in seconds to define the interval at which AP statistics are calculated.

  The valid range is from 120 to 900. The default value is 300.
- (Optional) Check the **Reload the AP** check box to automatically reload the AP when there's high CPU and memory usage in the defined sampling interval.

b) Under **Radio Monitoring**, complete these configurations.

- (Optional) Check the **Monitoring of AP Radio Stuck** check box to enable AP radio statistics collection and processing.
- (Optional) Check the **Alarms for AP Radio Stuck** check box to generate an alarm for the AP radio when there's no increment in the statistics.
- Check the **Reset the Stuck AP Radio** check box to enable AP radio reset and recover the radio when there's no increment in the statistics.
- In the **Sampling Interval (sec)** field, enter a value in seconds to define how often data is collected from the radio.

  The valid range is from 720 to 3600. The default value is 720.

**Step 13** Under **Management**, click **Device** and complete these configurations.

a) (Optional) Under **TFTP Downgrade**, enter data in these fields.

- **IPv4/IPv6 Address**: enter the TFTP downgrade IP address of the TFTP server
- **Image File Name**: enter the name of the TFTP downgrade file

b) Under **System Log**, complete these configurations.

- From the **Facility Value** drop-down list, choose a facility value.
- (Optional) In the **Host IPv4/IPv6 Address** field, enter the IPv4 or IPv6 address of the host.
- From the **Log Trap Value** drop-down list, choose a log level.
- (Optional) Check the **Secured** check box to enable TLS mode for secure syslog.

c) Under **Telnet/SSH**, complete these configurations.

- Use the **Telnet** check box to enable or disable a Telnet session to the AP.
- Use the **SSH** check box to enable or disable an SSH session to the AP.
- Use the **Serial Console** check box to enable or disable access to the serial console to the AP.
- From the **Console Port Speed** drop-down list, choose a baud rate for the AP console port to match your terminal or console server settings for serial access.

d) Under **AP Core Dump**, complete these configurations.

- From the **Kernel Core Dump** drop-down list, choose a type of kernel core dump.



**Note** Changing the kernel core dump type may cause the AP to rejoin and result in loss of connectivity for the associated clients.

- In the **Max AP Kernel Core Dumps** field, enter the maximum number of kernel core dumps.

  The valid range is from 1 to 5. The default value is 5.

- (Optional) Check the **Radio Core Dump** check box to enable AP core dump.

  If you enable AP core dump, complete these configurations.

  - (Optional) Check the **Enable File Compression** check box to enable file compression.
  - In the **TFTP Server (IPv4/IPv6)** field, enter the TFTP server address to move the core dump.
  - In the **File Name** field, enter a core file name.

- In the **Kernel Coredump File Limit** field, enter the maximum number of core dump files to retain on the AP. When the limit is reached, older files are deleted.

  The valid range is from 15 to 25. The default value is 25.

**Step 14** Under **Management**, click **User** and complete these configurations.

- (Optional) In the **Username** field, enter a user name for AP user management.

  You can enter up to 32 characters.

- From the **Password Type** drop-down list, choose a type of password for AP user management.
- (Optional) In the **Password** field, enter a password for AP user management.

- From the **Secret Type** drop-down list, choose a type for secret for AP user management.
- (Optional) In the **Secret** field, enter a secret for AP user management.

**Step 15** Under **Management**, click **Credentials** and complete these configurations.

- (Optional) In the **Dot1x Username** field, enter a user name for AP Dot1x authentication.

  You can enter up to 32 characters.
- (Optional) In the **Dot1x Password** field, enter a password for AP Dot1x authentication.
- From the **Dot1x Password Type** drop-down list, choose a type of password for AP Dot1x authentication.

**Step 16** (Optional) Under **Management**, click **CDP** and check the **CDP State** check box to enable CDP for the AP.

**Step 17** Click **Security** and complete these configurations.

a) Under **Rogue Detection**, complete these configurations.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Rogue Detection**: detect APs that are installed on a secure network without authorization from the system administrator.
  - **Rogue Containment Automatic Rate Selection**: enable rogue containment automatic rate selection.
  - **Auto Containment on FlexConnect Standalone**: enable rogue containment for FlexConnect mode.
- Enter data in these fields.
  - **Rogue Detection Minimum RSSI**: enter the minimum RSSI for AP rogue detection.

    The valid range is from -128 to -70. The default value is -90.
  - **Rogue Detection Transient Interval (sec)**: enter the transient interval in seconds for which the rogue AP should be seen before reporting the wireless controller.

    The valid values are 0 or range from 120 to 1800. The default value is 0.
  - **Rogue Detection Report Interval (sec)**: enter the interval in seconds at which the monitor mode report is generated for AP rogue detection.

    The valid range is from 10 to 300.

b) (Optional) Under **PMF - Denial**, check the **Rogue Containment PMF-Denial** check box to enable 802.11w Protected Management Frames (PMF) denial rogue AP containment.

If you check this check box, you can optionally use these check boxes to enable or disable the corresponding configurations:

- **Rogue Containment PMF-Deauth**: PMF denial rogue AP containment using deauthentication.
- **Rogue Detection PMF Off-Channel**: off-channel PMF rogue AP containment

c) (Optional) Under **aWIPS and Forensic Capture**, check the **aWIPS** check box to enable the Advanced Wireless Intrusion Prevention System (aWIPS).

If you enable aWIPS, the **Forensic Capture** check box is displayed. To enable aWIPS forensic capture, check the **Forensic Capture** check box.

**Step 18** (Optional) Under **iCAP Client Telemetry**, click **Full Packet Trace** and complete these configurations.

a) Check the required check box to enable the corresponding configurations.

- **Topic Status**: enable the full packet trace subscription for Intelligent Capture (iCAP) clients
- **Aggregate Trace**: enable aggregation of full packet traces

b) Under **Client MAC Filters**, in the **MAC Address** field, enter the MAC address of the client.

**Step 19** (Optional) Under **iCAP Client Telemetry**, click **Partial Packet Trace** and complete the configurations.

a) Check the **Topic Status** check box to enable partial packet trace subscription for iCAP clients.

b) Under **Client MAC Filters**, in the **MAC Address** field, enter the MAC address of the client.

To include additional MAC addresses, click the plus icon.

c) Under **Protocol Filters**, complete these configurations.

- Under **Protocol Filter Type**, check the **All** check box to collect partial packet traces for all protocols.
- Under **Management Type**, check the check box next to the required management protocols to collect the partial packet traces: **All**, **Assoc**, and **Auth**
- Under **Data Type**, check the check box next to the required data protocols to collect the partial packet traces: **All**, **ARP**, **DHCP**, **DHCPv6**, **DNS**, **EAP**, **ICMP**, and **ICMPv6**
- Under **Cisco Type**, check the check box next to the required Cisco protocols to collect the partial packet traces: **All** and **NDP**

**Step 20** Under **iCAP Client Telemetry**, click **Anomaly Detection** and complete these configurations.

a) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Topic Status**: enable the anomaly detection subscription for iCAP clients
- **Packet Trace Trigger AP**: trigger an AP packet trace on anomaly detection

b) (Optional) Under **Client MAC Filters**, in the **MAC Address** field, enter the MAC address of the client.

To include additional MAC addresses, click the plus icon.

c) Under **Timeout**, in the **DHCP Frequency (sec)** field, enter a DHCP timeout for anomaly detection in seconds.

The valid range is from 1 to 120. The default value is 5.

**Step 21** Under **iCAP Client Telemetry**, click **Statistics** and complete these configurations.

a) Under **Client Statistics Subscription**, complete these configurations.

- (Optional) Check the **Topic Status** check box to enable client statistics subscription for iCAP clients.
- In the **Frequency (sec)** field, enter the frequency for client statistics collection in seconds.

  The valid range is from 30 to 3600. The default value is 30.

b) Under **Client Filter Statistics Subscription**, complete these configurations.

- (Optional) Check the **Topic Status** check box to enable client statistics subscription for iCAP filtered clients.
- In the **Frequency (sec)** field, enter the frequency for filtered client statistics collection in seconds.

The valid range is from 5 to 3600. The default value is 5.

c) (Optional) Under **Client MAC Filters**, in the **MAC Address** field, enter the MAC address of the client.

To include additional MAC addresses, click the plus icon.

**Step 22** Click **iCAP AP Telemetry Subscriptions** and complete these configurations.

a) Check the required check boxes to enable the corresponding configurations.

- **RF Spectrum**: enable iCAP AP telemetry subscription for RF spectrum
- **Slot 0**: use radio slot 0 for RF spectrum measurements
- **Slot 1**: use radio slot 1 for RF spectrum measurements
- **Slot 2**: use radio slot 2 for RF spectrum measurements
- **Slot 3**: use radio slot 3 for RF spectrum measurements

b) (Optional) Configure the statistics subscription.

- Check the required check boxes to enable the corresponding AP statistics subscription.
- In the corresponding **Frequency (sec)** fields, enter a frequency for the corresponding AP statistics collection in seconds.

  The valid range is from 30 to 3600. The default value is 30.

**Step 23** (Optional) Click **QoS** and complete these configurations.

a) Use the required check boxes to enable or disable the corresponding configurations.

- **Action Frame**: send an 802.11 QoS map action frame when the DSCP to User Priority (UP) mapping changes
- **Trust DSCP Upstream**: configure the AP to trust the upstream DSCP instead of UP

b) Under **DSCP to UP Range**, configure the DSCP to UP range mapping.

| If you want to... | Then... |
|---|---|
| add a DSCP to UP range mapping | 1. Click **Add**.<br>2. From the **User Priority** drop-down list in the **Add DSCP to UP Range** dialog box, choose a user priority.<br>3. In the **UP to DSCP Upstream** field, enter an AP upstream traffic UP to DSCP mapping.<br>The valid range is from 0 to 63. The default value is 0.<br>4. In the **Lower DSCP Range** field, enter a lower boundary for the DSCP range.<br>The valid range is from 0 to 63. The default value is 0.<br>5. In the **Upper DSCP Range** field, enter an upper boundary for the DSCP range.<br>The valid range is from 0 to 63. The default value is 0.<br>6. Click **Save**. |
| edit a DSCP to UP range mapping | 1. Check the check box next to the required user priority.<br>2. Hover your cursor over **Actions** and choose **Edit**.<br>3. Edit the required configurations.<br>4. Click **Save**. |
| delete a DSCP to UP range mapping | 1. Check the check box next to the required user priority.<br>2. Hover your cursor over **Actions**, and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

c) Under **DSCP to UP Exception**, configure the DSCP to UP exception mapping.

| If you want to... | Then... |
|---|---|
| add a DSCP to UP exception mapping | 1. Click **Add**.<br>2. In the **DSCP** field of the **Add DSCP to UP Exception** dialog box, enter DSCP to map to UP.<br>The valid range is from 0 to 63.<br>3. From the **User Priority** drop-down list, choose a user priority.<br>4. Click **Save**. |

| If you want to... | Then... |
|---|---|
| edit a DSCP to UP exception mapping | **1.** Check the check box next to the required DSCP.<br>**2.** Hover your cursor over **Actions** and choose **Edit**.<br>**3.** Edit the required configurations.<br>**4.** Click **Save**. |
| delete DSCP to UP exception mapping | **1.** Check the check box next to the required DSCP.<br>**2.** Hover your cursor over **Actions**, and choose **Delete**.<br>**3.** In the dialog box, click **Yes**. |

**Step 24** Click **Geolocation** and configure the required settings.

Under **Fine Timing Measurement**, complete these configurations:

- Use the **FTM Enabled** check box to enable or disable Fine Timing Measurement (FTM).
- From the **FTM Initiator Burst Duration** drop-down list, choose a duration.
- In the **FTM Initiator Burst Size** field, enter the FTM initiator burst size.

  The valid range is from 2 to 31. The default value is 16.

Under **Ultra-Wide Band (UWB)**, complete these configurations:

- Use the **UWB** check box to enable or disable Ultra-Wide Band (UWB) for AP location tracking.
- In the **UWB Burst Duration** field, enter the UWB burst duration for optimized AP location tracking.

  The valid range is from 5 to 30. The default value is 10.
- In the **UWB Burst Size** field, enter the UWB burst size for optimized AP location tracking.

  The valid range is from 10 to 100. The default value is 32.
- Use the **UWB Wi-Fi Blocking** check box to enable or disable the blocking of Wi-Fi transmissions during Ultra-Wide Band (UWB) operations.

  Enable this setting to reduce interference between UWB and Wi-Fi, which may be necessary for certain location-based services.

  If you check this check box, from the **UWB Wi-Fi Block Duration** drop-down list, choose a duration for which Wi-Fi is blocked during UWB operations on the AP.

  Longer durations may improve UWB accuracy but can temporarily impact Wi-Fi connectivity.

**Step 25** Click **Miscellaneous** and complete these configurations.

- (Optional) In the **Packet Capture Profile** field, enter a name for the packet capture profile.
- (Optional) In the **AP Trace Profile** field, choose an AP trace profile.
- (Optional) In the **Beacon Power** field, enter a Bluetooth Low Energy (BLE) beacon power value.

  The valid range is from 40 to 100. The default value is 59.

- (Optional) In the **Beacon Interval** field, enter a BLE beacon interval for the AP.

  The valid range is from 1 to 10. The default value is 1.

- (Optional) Check the **SSID Statistics Enable** check box to enable BSSID statistics on an AP.

  **Note** You can't enable BSSID statistics and client traffic distribution status on an AP simultaneously.

- (Optional) In the **SSID Profile Statistics Frequency** field, enter the time frequency on AP to send BSSID statistics.

  The valid range is from 1 to 180. The default value is 30.

- (Optional) Check the **SSID Neighbor Statistics Enable** check box to enable BSSID neighbor statistics on AP.
- (Optional) In the **SSID Neighbor Statistics Frequency** field, enter the time interval between consecutive BSSID neighbor statistics update sent from the AP.

  The valid range is from 0 to 180. The default value is 180.

- (Optional) Use the **ICAP Individual Enable** check box to enable the anomaly detection report for individual anomalies.
- (Optional) In the **ICAP Individual Throttle** field, enter the number of events per five minutes for anomaly detection individual reports.

  The valid range is from 0 to 500. The default value is 5.

- (Optional) Check the **ICAP Summary Enable** check box to enable the anomaly detection report summary.
- (Optional) In the **ICAP Summary Frequency** field, enter a frequency for anomaly detection summary reports.

  The valid range is from 3 to 60. The default value is 5.

- (Optional) Check the **Partial Trace Management Probe** check box to collect partial packet traces for probing management protocols.
- (Optional) In the **AUX LAN ID** field, enter the VLAN ID to which auxiliary client traffic is assigned.

  The valid range is from 0 to 4094. The default value is 0.

- From the **Press Sense Config State** drop-down list, choose an AP pressure sensor configuration state.
- (Optional) In the **Proxy Hostname** field, enter the HTTP proxy host name.
- (Optional) In the **Proxy List** field, enter a list of URLs to exclude from the proxy.
- (Optional) In the **Proxy Port** field, enter the HTTP proxy port number.

  The valid range is from 0 to 65535.

- (Optional) From the **Accounting Method List** field, choose an accounting method list name.

  To create an accounting method list, see Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 161.

- (Optional) In the **AP Management IPv4 ACL Name** field, enter the name of the IPv4 ACL to restrict management access to the AP.

The ACL name can contain up to 32 characters. Only the devices permitted in this ACL can manage the AP over IPv4.

- (Optional) In the **AP Management IPv6 ACL Name** field, enter the name of the IPv6 ACL to restrict management access to the AP.

  The ACL name can contain up to 32 characters. Only the devices permitted in this ACL can manage the AP over IPv6.

- (Optional) Check the **Traffic Distribution Status** check box to enable client traffic distribution statistics.

  **Note** You can't enable BSSID statistics and client traffic distribution status on an AP simultaneously.

- (Optional) In the **Traffic Distribution Interval** field, enter an interval at which the AP sends the statistics.

  The valid range is from 30 to 3600. The default value is 300.

- (Optional) In the **Session Limit** field, enter the maximum Dot1x sessions allowed per AP.

  The default value is 0.

- From the **Tunnel UDP Lite** drop-down list, choose an IPv6 CAPWAP data checksum type.

- (Optional) Check the required check boxes to enable or disable the corresponding configurations.
  - **GPRC Enable**: enable gRPC server on the AP, check the check box
  - **TLS Config Control Preference**: configure preference to cipher suites defined in the wireless controller
  - **BLE scan state**: enable the BLE scan state
  - **Persistent SSID Broadcast Enable**: enable persistent SSID broadcast
  - **Adr Individual Aggr Enable**: enable the anomaly detection individual report aggregation

- In the **Adr Individual Pc Throttle** field, enter the number of events per client per 5 minutes for anomaly detection individual reports.

  The valid range is from 0 to 50. The default value is 5.

- In the **Adr Individual Pt Throttle** field, enter the number of events per type per 5 minutes for anomaly detection individual reports.

  The valid range is from 0 to 100. The default value is 5.

- (Optional) Under **BLE Beacons**, view the BLE becaon configurations.

  You can manage the BLE beacon configurations through spatial mapping in Cisco Connected Mobile Experiences (CMX) and Cisco Spaces. These attributes are read-only for visibility and alignment with location-based services.

**Step 26** Click **Review and Provision**.

**Step 27** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 28** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 29** On the **Tasks** window, monitor the task deployment.

## Configure global mesh parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global mesh parameters for a wireless controller and provision them.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **AP** and click **Mesh**.

**Step 4** Click the **Global** tab.

**Step 5** (Optional) Under **General**, use the check boxes to enable or disable the corresponding configurations.

- **Ethernet Bridging Allow BPDU**: allow BPDU packets on the mesh network when Ethernet bridging is enabled
- **Subset Channel Sync**: enable synchronization of mesh root AP (RAP) channels across the mobility group
- **Public Safety Enabled**: enable the public safety band

- **Auto DCA RF ASCI APs**: indicate if RRM DCA should always be enabled on the backhaul radio of an RF ASIC-integrated mesh RAP
- **CAC Enabled**: enable the Call Admission Control (CAC) on the mesh AP (MAP)

**Step 6** (Optional) Under **Backhaul**, use the check boxes to enable or disable the corresponding configurations.

- **Extended UNII B Domain Channels**: enable the UNII B domain channels in the backhaul radio of MAPs
- **RRM**: enable RRM on the backhaul radio of a root MAP that doesn't have any child MAPs

**Step 7** (Optional) Under **Security**, check the **PSK Provisioning** check box to enable PSK provisioning for the MAP.

- (Optional) Check the **Default PSK** check box to enable the default PSK for MAPs.
- From the **PSK Inuse Index** drop-down list, choose a PSK in-use key index.

  To create a PSK key, see Create a mesh PSK for a Cisco Catalyst 9800 Series Wireless Controller, on page 129.

**Step 8** Under **Alarm**, enter data in these fields.

- **Max Hop Count**: enter the threshold value for the number of hops from the MAP node to the RAP node for generating the mesh alarm.

  The valid range is from 1 to 16.
- **Recommended Max Children for MAP**: enter the threshold value for the number of children MAPs on a parent MAP for generating the mesh alarm.

  The valid range is from 1 to 50.
- **Recommended Max Children for RAP**: enter the threshold value for the number of children MAPs on a parent RAP for generating the mesh alarm.

  The valid range is from 1 to 50.
- **Parent Change Count**: enter the threshold value for the number of times a child mesh node changes its parent node for generating the mesh alarm.

  The valid range is from 1 to 30.
- **Low Link SNR (dB)**: enter the threshold value for lower SNR on the backhaul link of a child mesh node for generating the mesh alarm.

  The valid range is from 1 to 30.
- **High Link SNR (dB)**: enter the threshold value for higher SNR on the backhaul link of a child mesh node for generating the mesh alarm.

  The valid range is from 31 to 100.
- **Association Count**: enter the threshold value for cumulative association count at the parent mesh node for generating the alarms.

  The valid range is from 1 to 30.

**Step 9** Click **Review and Provision**.

**Step 10** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create a mesh PSK for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a mesh preshared key (PSK) for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **AP** and click **Mesh**.

**Step 4** Click the **PSK Keys** tab.

**Step 5** Click **Add**.

**Note** This option isn’t available if five PSK keys are already created.

**Step 6** From the **Index** drop-down list of the **Create Mesh Profile Key** slide-in pane, choose an index for the PSK.

**Step 7** In the **Psk Key** field, enter the PSK.

The PSK can contain from 3 to 32 characters.

**Step 8** From the **Psk Key Type** drop-down list, choose a PSK type.

**Step 9** (Optional) In the **Description** field, enter a description for the PSK.

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Create a mesh profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a mesh profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **AP** and click **Mesh**.

**Step 4** Click the **Mesh Profiles** tab.

**Step 5** Click **Add**.

**Step 6** In the **General** tab of the **Create Mesh Profile** slide-in pane, complete these configurations.

a) In the **Mesh Profile Name** field, enter a name for the mesh profile.

b) (Optional) In the **Description** field, enter a description.

c) In the **Range (Root AP to Mesh AP)** field, enter the maximum range between outdoor RAP and MAP.

The valid range is from 150 to 132000. The default value is 12000.

d) From the **Multicast Mode** drop-down list, choose a multicast mode for the Ethernet bridged multicast traffic over mesh networks.

e) (Optional) Check the required check boxes to enable the corresponding configurations.

- **IDS (Rogue/Signature Detection)**: enable the MAP to send IDS and rogue reports to the wireless controller
- **Backhaul Client Access**: enable client access on the backhaul radio of the MAP
- **Background Scanning**: enable background scanning on the backhaul radio of the MAP
- **Battery State for an AP**: enable the external battery state for the MAP
- **Channel Change Notification**: enable the parent MAP to send channel change notification to child MAPs
- **Full Sector DFS Status**: enable full-sector Dynamic Frequency Selection (DFS) on the mesh network
- **LSC**: enable Locally Significant Certificate (LSC) authentication for the MAP
- **Daisychain STP Redundancy**: enable daisy chain Spanning Tree Protocol (STP) redundancy on the MAP
- **Backhaul amsdu**: enable Aggregated MAC Service Data Unit (A-MSDU) on the backhaul radio of the MAP
- **Map Fast Ancestor Find**: enable the MAP fast ancestor find feature on the backhaul radio of the MAP
- **RAP Ethernet Daisy Chain**: enable the RAP Ethernet daisy chain for RAP

f) From the **Convergence Method** drop-down list, choose a convergence method used in the MAPs.

**Step 7** Click **Advanced** and complete these configurations.

a) In the **Channel Width** field, enter the backhaul channel width.

b) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Keep Wireless Connection**: allow an AP to retain its wireless connection with the parent AP without switching to a wired channel
- **Least Congested Channel Scan**: enable the least congested channel scan
- **Unii3 Bias**: add a 20% bias towards UNII-3 channels over the other channels
- **Use Unii2**: consider the channels in the UNII-2 band in the least congested channel scan

c) Under **Security**, choose the required option from the corresponding drop-down lists.

| From the drop-down list... | Choose... |
|---|---|
| **Method** | the security method that is used for MAPs |
| (Optional) **Authentication Method** | an AAA authentication method list<br>To create an authentication method list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 158. |
| (Optional) **Authorization Method** | an AAA authorization method list<br>To create an authorization method list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159. |

d) (Optional) Under **Ethernet Bridging**, check the required check box to enable the corresponding configurations.

- **VLAN Transparent**: indicate that the Ethernet bridging on MAPs must use the VLAN configuration
- **Ethernet Bridging**: enable Ethernet bridging for MAPs

e) (Optional) Under **Bridge Group**, complete these configurations.

- In the **Bridge Group Name** field, enter a name for the bridge group.
- Check the **Strict Match** check box to enable strict matching of the bridge group name for MAPs for parent selection.

f) Under **5 GHz Band Backhaul**, complete these configurations.

- From the **5 GHz Band Rate Types** drop-down list, choose a backhaul data rate type.
- If you chose the **dot11abg** backhaul data rate type, from the **Rate (Mbps)** drop-down list, choose an enum value for mesh backhaul 802.11 transmission.
- If you chose the **dot11n** backhaul data rate type, in the **Dot11n MCS index** field, enter the 802.11n MCS index for mesh backhaul transmission.

  The valid range is from 0 to 31. The default value is 0.
- If you chose the **dot11ac** backhaul data rate type, you can also configure these optional settings:
  - In the **Dot11ac MCS index** field, enter the 802.11ac MCS index for mesh backhaul transmission.

    The valid range is from 0 to 9. The default value is 0.
  - In the **AC Spatial Stream** field, enter the 802.11ac spatial stream value for mesh backhaul transmission.

    The valid range is from 1 to 4. The default value is 1.
- If you chose the **dot11ax** backhaul data rate type, you can also configure these optional settings:
  - In the **Dot11ax MCS index** field, enter the 802.11ax MCS index for mesh backhaul transmission.

    The valid range is from 0 to 11. The default value is 0.
  - In the **AX Spatial Stream** field, enter the 802.11ax spatial stream value for mesh backhaul transmission.

    The valid range is from 1 to 8. The default value is 1.

g) Under **2.4 GHz Band Backhaul**, complete these configurations.

- From the **2.4 GHz Band Rate Types** drop-down list, choose a backhaul data rate type.
- If you chose the **dot11abg** backhaul data rate type, from the **Rate (Mbps)** drop-down list, choose an enum value for mesh backhaul 802.11 transmission.
- If you chose the **dot11n** backhaul data rate type, in the **Dot11n MCS index** field, enter the 802.11n MCS index for mesh backhaul transmission.

  The valid range is from 0 to 31. The default value is 0.
- If you chose the **dot11ax** backhaul data rate type, you can also configure these optional settings:
  - In the **Dot11ax MCS index** field, enter the 802.11ax MCS index for mesh backhaul transmission.

    The valid range is from 0 to 11. The default value is 0.
  - In the **AX Spatial Stream** field, enter the 802.11ax spatial stream value for mesh backhaul transmission.

    The valid range is from 1 to 4. The default value is 1.

h) (Optional) Under **Fast Roaming**, check the **Fast Teardown** check box to enable fast teardown, and enter data in these fields.

- **Number of Retries**: enter the number of retries until the gateway is considered unreachable.

  The valid range is from 1 to 10. The default value is 4.
- **Interval (seconds)**: enter the retry interval.

  The valid range is from 1 to 10. The default value is 1.
- **Latency Threshold (milliseconds)**: enter the ping latency threshold in milliseconds.

  The valid range is from 1 to 500. The default value is 10.
- **Latency Exceeded Threshold (seconds)**: enter the interval in seconds in which at least one ping must succeed in less than the threshold time.

  The valid range is from 1 to 30. The default value is 8.
- **Uplink Recovery Interval (seconds)**: enter the time in seconds during which the RAP uplink must be stable to accept child connections.

  The valid range is from 1 to 3600. The default value is 60.

**Step 8** Click **Review and Provision**.

**Step 9** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |

| Option | Description |
|---|---|
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Create a power profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a power profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **AP** and click **Power Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **Profile Name** field of the **Create Power Profile** slide-in pane, enter a name for the power profile.

**Step 6** (Optional) In the **Description** field, enter a description.

**Step 7** (Optional) In the **Power Save Client Threshold** field, enter the threshold up to which the AP can stay on the power save mode.

The valid range is from 1 to 32. The default value is 1.

**Step 8** (Optional) Under **Rules**, click **Add** to add a rule.

a) In the **Sequence** field, enter a unique interface sequence number.

The valid range is from 0 to 4294967295.

b) From the **Interface** drop-down list, choose an interface.

| If you choose... | Then... |
|---|---|
| **Ethernet** | complete these configurations:<br>• From the **Interface ID** drop-down list, choose an interface ID.<br>• From the **Parameter Value** drop-down list, choose a parameter value. |
| **Radio** | complete these configurations:<br>• From the **Parameter** drop-down list, choose a parameter.<br>• From the **Interface ID** drop-down list, choose an interface ID.<br>• From the **Parameter Value** drop-down list, choose a parameter value.<br>**Note**<br>If you choose the **State** parameter, this drop-down list is disabled. |

c) Click **Save**.

**Step 9** (Optional) To delete the rules, complete these steps.

**a.** Check the check box next to the required rules.

**b.** Hover your cursor over **Actions** and click **Delete**.

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

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Create a flex profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a flex profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **AP** and click **Flex Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **General** tab of the **Create Flex Profile** slide-in pane, complete these configurations.

a) In the **Flex Profile Name** field, enter a unique name for the flex profile.

The profile name can contain up to 32 characters.

b) (Optional) In the **Description** field, enter a description.
c) In the **Native VLAN ID** field, enter a VLAN ID for the AP.

The valid range is from 1 to 4094. The default value is 1.

d) (Optional) From the **mDNS Flex Profile** drop-down list, choose an mDNS flex profile name.

To create an mDNS flex profile, refer to Create an mDNS flex profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 274.

e) (Optional) Enter data in these fields.

- **HTTP Proxy Port**: enter the HTTP proxy port.

  The valid range is from 0 to 65535. The default value is 0.

- **HTTP Proxy IP Address**: enter the HTTP proxy IP address.

f) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Fallback Radio Shut**: enable the FlexConnect Ethernet Fallback feature for the APs connected to the wireless controller

- **OfficeExtend AP**: use the APs connected to this profile as home APs
- **Flex Resilient**: enable standalone mode support on a Remote-Edge AP (REAP)
- **Join Minimum Latency**: enable the REAP AP to join the wireless controller with minimum latency
- **ARP Caching**: enable ARP cache for the FlexConnect APs connected to the wireless controller
- **IP Overlap**: enable IP overlap support for the site
- **Efficient Image Upgrade**: enable efficient AP image upgrade support
- **Pmk Dist Method**: enable Pairwise Master Key (PMK) distribution with APs

g) (Optional) In the **Maximum Retry Attempts (Secondary)** field, enter the maximum number of retry attempts for secondary devices when trying to establish or maintain a connection.

Increasing the value can improve reliability in unstable environments, but may delay failure detection.

h) (Optional) Under **CTS Policy**, complete these configurations.

- Check the **Inline Tagging** check box to enable Cisco TrustSec (CTS) inline tagging for the FlexConnect APs connected to the wireless controller.
- Check the **SGACL Enforcement** check box to enable CTS role-based enforcement for FlexConnect APs connected to the wireless controller.
- From the **CTS Profile Name** drop-down list, choose a CTS profile.

  To create a profile, refer to Create an SXP AP profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 201.

**Step 6** (Optional) Click **Local Authentication** and complete these configurations.

a) From the **RADIUS Server Group** drop-down list, choose a RADIUS server group.

To create a RADIUS server group, refer to Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 153.

b) From the **Local Accounting RADIUS Server Group** drop-down list, choose a RADIUS server group.

To create a RADIUS server group, refer to Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 153.

c) From the **EAP Fast Profile** drop-down list, choose an EAP Fast profile name.

To create an EAP fast profile, refer to Create an EAP-FAST profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 183.

d) Check the required check boxes to enable the corresponding configurations.

- **Local Client Roaming**: enable distributed client data caching on AP for local roaming
- **LEAP**: enable the Lightweight Extensible Authentication Protocol (LEAP)
- **TLS**: enable TLS
- **PEAP**: enable the Protected Extensible Authentication Protocol (PEAP)
- **RADIUS**: enable RADIUS

e) Under **Users**, add, edit, or delete the users.

| If you want to... | Then... |
|---|---|
| add a flex local authentication user | click **Add** and complete these steps.<br>**1.** In the **Username** field, enter a username for authenticating a client associated to an AP within the group.<br>**2.** From the **Password Type** drop-down list, choose a password encryption type for authenticating a client associated to an AP within the group.<br>**3.** In the **Password** field, enter a password for authenticating a client associated to an AP within the group.<br>**4.** Click **Save**. |
| edit a flex local authentication user | **1.** Check the check box next to the required username<br>**2.** Hover your cursor over **Actions**, and click **Edit**.<br>**3.** Edit the required configurations.<br>**4.** Click **Save**. |
| delete flex local authentication users | **1.** Check the check box next to the required usernames<br>**2.** Hover your cursor over **Actions**, and click **Delete**.<br>**3.** In the dialog box, click **Yes**. |

**Step 7** (Optional) Click **Policy ACL** and configure the ACLs.

| If you want to... | Then... |
|---|---|
| add a policy ACL | Click **Add** and complete these steps.<br>**a.** From the **ACL Name** drop-down list, choose an ACL.<br>To create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168.<br>**b.** To enable central web authentication for the ACL, check the **Central Web Authentication** check box.<br>**c.** In the **URL Filter** field, enter the URL filter list for the ACL.<br>To create URL filters, refer to Create a basic URL filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 186 and Create an enhanced URL filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 187.<br>**d.** Click **Save**. |

| If you want to... | Then... |
|---|---|
| edit a policy ACL | **a.** Check the check box next to the required policy ACL<br>**b.** Hover your cursor over **Actions**, and click **Edit**.<br>**c.** Edit the required configurations.<br>**d.** Click **Save**. |
| delete policy ACLs | **a.** Check the check box next to the required policy ACLs<br>**b.** Hover your cursor over **Actions**, and click **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** (Optional) Click **VLAN** and configure VLANs.

| If you want to... | Then... |
|---|---|
| add a VLAN | Click **Add** and complete these steps.<br>**a.** From the **VLAN Name** drop-down list, choose a VLAN name.<br>To create a VLAN, refer to Create a VLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 315.<br>**b.** In the **ID** field, enter the VLAN ID to map to the ACL for the AP identified by the VLAN name.<br>The valid range is from 1 to 4096. The default value is 1.<br>**c.** Under **Direction**, click the **Unidirectional** or **Bidirectional** radio button.<br>**d.** If you chose **Unidirectional**, choose an ingress and egress ACL from the corresponding drop-down lists.<br>• **Ingress ACL** (to create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168)<br>• **Egress ACL** (to create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168)<br>**e.** If you chose **Bidirectional**, from the **Acl Name** drop-down list, choose an ACL.<br>To create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168.<br>**f.** Click **Save**. |

| If you want to... | Then... |
|---|---|
| edit a VLAN | **a.** Check the check box next to the required VLAN.<br>**b.** Hover your cursor over **Actions**, and click **Edit**.<br>**c.** Edit the required configurations.<br>**d.** Click **Save**. |
| delete VLANs | **a.** Check the check box next to the required VLANs.<br>**b.** Hover your cursor over **Actions**, and click **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 9** (Optional) Click **DNS Layer Security** and configure parameter maps.

| If you want to... | Then... |
|---|---|
| add a parameter map | Click **Add** and complete these steps.<br>**a.** In the **Parameter Map Name** field, enter the umbrella profile name.<br>**b.** Click **Save**. |
| edit a parameter map | **a.** Check the check box next to the required parameter map.<br>**b.** Hover your cursor over **Actions**, and click **Edit**.<br>**c.** Edit the required configurations.<br>**d.** Click **Save**. |
| delete parameter maps | **a.** Check the check box next to the required parameter maps.<br>**b.** Hover your cursor over **Actions**, and click **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |

| Option | Description |
|---|---|
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Create a site tag for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a site tag for the APs associated with a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **AP** and click **Site Tags**.

**Step 4** Click **Add**.

**Step 5** In the **Site Tag Name** field of the **Create Site Tag** slide-in pane, enter a unique name for the site tag.

The site tag name can contain up to 32 alphanumeric characters and special characters. Catalyst Center does not support leading and trailing spaces in the site tag name.

**Step 6** (Optional) In the **Description** field, enter a description.

The description can contain up to 64 alphanumeric characters and special characters.

**Step 7** From the **AP Join Profile** drop-down list, choose an AP join profile.

To create an AP join profile, see Create an AP join profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 111.

**Step 8** Use the **Local Site** check box to enable or disable the local site.

If this check box is unchecked, from the **Flex Profile** drop-down list, choose a flex profile.

To create a flex profile, see Create a flex profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 136.

**Step 9** In the **Load** field, enter an estimate of the relative load contributed by the site.

The valid range is 0 to 1000. The default value is 0.

You can use the AP count for an approximate value.

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Create a calendar profile for a Cisco Catalyst 9800 Series Wireless Controller

You can set up daily, weekly, or monthly recurrence schedules for calendar profiles. When associated with a power policy, this configuration automates the powering down of interfaces connected to APs. Use this procedure to create a calendar profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **AP** and click **Calendar Profiles**.

**Step 4** Click **Add**.

**Step 5** In the **Profile Name** field of the **Create Calendar Profile** slide-in pane, enter a name for the calendar profile.

**Step 6** Under **Recurrence**, choose the recurrence frequency for the calendar profile.

- **Daily**: applies the calendar profile rules daily.
- **Weekly**: applies the calendar profile rules every week on the selected days. Click the required days to choose them.
- **Monthly**: applies the calendar profile rules every month on the selected dates. Click the required dates to choose them.

**Step 7** Under **Start Time** and **End Time**, enter the start time and end time for the recurrence schedule.

**Step 8** Click **Review and Provision**.

**Step 9** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

# Tag mapping configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device tag mapping configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Create an AP priming profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AP priming profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Tag Mapping** and click **AP Priming**.

**Step 4** Click **Add**.

**Step 5** In the **Profile Name** field of the **Create AP Priming** slide-in pane, enter a name for the priming profile.

**Step 6** (Optional) Enter the wireless controller configuration name and the corresponding wireless controller IP address of the AP for these controllers, as required:

- Primary controller
- Secondary controller
- Tertiary controller

**Step 7** (Optional) Check the **Geolocation** check box to enable the geographical location for the AP priming profile.

If you enable geographic location for the profile, you can optionally enter data in both these fields:

- **Height (meters)**: enter the height from the ground in meters (rounded to the nearest whole number).

  The valid range is from -100 to 1000.

- **Height Uncertainty (meters)**: enter the height uncertainty in meters.

  The valid range is from 1 to 100.

**Step 8** (Optional) Use the **Priming Override** slider to push all the configured priming profile attributes to the AP.

**Step 9** Click **Review and Provision**.

**Step 10** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Configure tag priority for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the tag priority for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Tag Mapping** and click **Tag Mapping**.

**Step 4** (Optional) In the **Tag Priority** tab, use the toggle buttons to enable or disable the required configurations.

- **Rule-Based**: enable or disable rule-based tag priority configuration
- **AP**: enable or disable AP-based tag priority configuration

**Step 5** (Optional) Check the **AP Tag Persistency** check box to enable persistent AP tags.

**Step 6** Click **Review and Provision**.

**Step 7** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create static tag mapping for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create static tag mapping for APs associated with a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Tag Mapping** and click **Tag Mapping**.

**Step 4** Click the **Static** tab.

**Step 5** Click **Add**.

**Step 6** In the **AP Ethernet MAC Address** field of the **Add Access Point** slide-in pane, enter the Ethernet MAC address of the AP.

**Step 7** From these drop-down lists, choose the required tags.

- **Policy Tag**: choose a policy tag for the AP.
- **Site Tag**: choose a site tag for the AP.
- **RF Tag**: choose an RF tag for the AP.

**Step 8** From the **Priming Profile** drop-down list, choose an AP priming profile.

To create an AP priming profile, see Create an AP priming profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 144.

**Step 9** Click **Review and Provision**.

**Step 10** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create a location-based tag-mapping rule for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a location-based tag-mapping rule for APs associated with a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Tag Mapping** and click **Tag Mapping**.

**Step 4** Click the **Location** tab.

**Step 5** Click **Add**.

**Step 6** In the **General** tab of the **Create Location Rule** slide-in pane, complete these configurations.
a) In the **Location Name** field, enter the name of the AP location.
b) (Optional) In the **Description** field, enter a description.
c) From these drop-down lists, choose the required tags.
- **Site Tag**: choose a site tag for the AP location.
- **Policy Tag**: choose a policy tag for the AP location.
- **RF Tag**: choose an RF tag for the AP location.

**Step 7** (Optional) Click **AP Provisioning** and complete these configurations.

| If you want to... | Then... |
|---|---|
| add a nonoperational AP to the rule | **a.** Hover your cursor over **Add** and click **Non-Operational APs**.<br>**b.** In the **AP MAC field** of the **Add AP** dialog box, enter the MAC address of the APs.<br>**c.** Click **Save**. |
| add an operational AP to the rule | **a.** Hover your cursor over **Add** and click **Operational APs**.<br>**b.** In the **Add AP** dialog box, check the check box next to the APs that you want to add.<br>To search for specific APs, click the Search field and choose the required filter option. Then click **Apply**.<br>**c.** Click **Save**. |
| delete APs from the rule | **a.** Check the check box next to the APs that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** Click **Review and Provision**.

**Step 9** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Create a rule-based tag-mapping profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a rule-based tag-mapping profile for APs associated with a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Tag Mapping** and click **Tag Mapping**.

**Step 4** Click the **Rule-Based** tab.

**Step 5** Click **Add**.

**Step 6** In the **Rule Name** field of the **Add Regex Rule Profile** slide-in pane, enter a name for the rule.

**Step 7** In the **AP Name Regex** field, enter a regular expression for filtering the AP name.

For example, if you have an AP *ap-lab-12*, you can configure the filter with a regular expression, such as **ap-lab**, to match the AP name.

**Step 8** (Optional) Use the **Active** toggle button to enable or disable the rule.

If you enable the rule, in the **Priority** field, enter a priority for the rule.

If you enter 0, the rule becomes inactive. You must enter a valid priority value for an active rule.

**Step 9** From the **Type** drop-down list, choose either the priming or the tag type.

a) For the **priming** type, choose the priming profile for the AP from the **Priming Profile** drop-down list.

**Note** To create AP priming profiles, see Create an AP priming profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 144.

b) For the **tag** type, choose the required tags from the following drop-down lists:

- **Policy Tag**: choose a policy tag for the AP.
- **Site Tag**: choose a site tag for the AP.
- **RF Tag**: choose an RF tag for the AP.

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

# Security configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device security configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Create a RADIUS server for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a RADIUS server for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **Servers/Groups**, under **RADIUS**, click **Servers**.

**Step 5** Click **Add**.

**Step 6** In the **Server Name** field of the **Create RADIUS Server** slide-in pane, enter a unique name for the RADIUS server.

**Step 7** From the **Type** drop-down list, choose the required type.

**Step 8** Based on the type of the RADIUS server, enter data in the corresponding field.

- If the **Server IP Address** field is displayed, enter the IPv4 address for the RADIUS server.
- If the **Server IPv6 Address** field is displayed, enter the IPv6 address for the RADIUS server.
- If the **Server FQDN** field is displayed, enter the FQDN for the RADIUS server.

**Step 9** (Optional) Check the **PAC Key** check box to transition from key to Proxy Auto Configuration (PAC) key.

**Step 10** Complete these configurations.

| If you... | Then... |
|---|---|
| enabled the PAC key | • From the **PAC Key Type** drop-down list, choose a key type.<br>• In the **PAC Key** field, enter the PAC key for a secure RADIUS server authentication.<br>• In the **Confirm PAC Key** field, confirm the PAC key. |

| If you... | Then... |
|---|---|
| didn't enable the PAC key | • From the **Key Type** drop-down list, choose a key type.<br>• In the **Key** field, enter the key for a secure RADIUS server authentication.<br>• In the **Confirm Key** field, confirm the key. |

**Step 11** (Optional) Enter data in these fields.

- **Authentication Port**: enter the UDP port number for authentication requests and responses.

  The valid range is from 0 to 65534. The default value is 1812.

- **Accounting Port**: enter the UDP port number for accounting requests and responses.

  The valid range is from 0 to 65534. The default value is 1813.

- **Server Timeout (sec)**: enter the time in seconds to wait for a response from the RADIUS server.

  The valid range is from 1 to 1000.

- **Retry Count**: enter the number of times a client can attempt to retransmit a request to the RADIUS server.

  The valid range is from 0 to 100.

**Step 12** (Optional) To enable a change of authorization (CoA) key for dynamic updates to user sessions, check the **Support for CoA** check box.

**Note** If you chose the type **Hostname**, this check box isn't available.

(Optional) If you check this check box, from the **CoA Server Key Type** drop-down list, choose a key type.

If you chose a CoA server key type, enter data in these fields.

- **CoA Server Key**: enter the CoA server key.
- **Confirm CoA Server Key**: confirm the key.

**Step 13** (Optional) Check the **Automate Tester** check box to set up automated network testing.

If you check this check box, complete these configurations.

- In the **Username** field, enter the test user name to include in the RADIUS request.
- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Ignore Auth Port**: ignore the testing of authentication ports of servers
  - **Ignore Acct Port**: ignore the testing of accounting ports of servers
  - **Enable Probe**: enable probing and send a packet to verify the server status

    If you didn't enable probing, in the **Idle Time (minutes)** field, enter the time, in minutes, after which the server state must be verified.

The valid range is from 1 to 35791.

**Step 14** Click **Review and Provision**.

**Step 15** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 16** On the **Tasks** window, monitor the task deployment.

## Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a RADIUS server group for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **Servers/Groups**, under **RADIUS**, click **Server Groups**.

**Step 5** Click **Add**.

**Step 6** In the **Server Group Name** field of the **Create RADIUS Server Group** slide-in pane, enter a name for the RADIUS server group.

**Step 7** From the **MAC Delimiter** drop-down list, choose the character for RADIUS compatibility mode.

**Step 8** From the **MAC Filtering** drop-down list, choose a MAC filtering option.

**Step 9** (Optional) In the **Dead Time (min)** field, enter the time, in minutes, to stop using an unresponsive server.

The valid range is from 0 to 1440.

**Step 10** (Optional) Check the **Load Balance** check box to enable load balancing in the RADIUS server group.

**Step 11** Choose the IPv4 and IPv6 source interface from the corresponding drop-down lists.

You can choose a physical, logical, or SVI interface for RADIUS traffic.

**Step 12** Choose the IPv4 and IPv6 VRF from the corresponding drop-down lists.

**Step 13** Under **Servers**, add servers using one of these options.

- Click the plus icon next to the required server.
- Click the required server and click **Add Selected**.

  To choose multiple servers, press **Shift**, click the server, and click **Add Selected**.
- To add all the servers, click **Add All**.

  You can use the **Search** field to filter the servers.

**Step 14** Click **Review and Provision**.

**Step 15** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 16** On the **Tasks** window, monitor the task deployment.

## Create a TACACS+ server for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a TACACS+ server for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **Servers/Groups**, under **TACACS+**, click **Servers**.

**Step 5** Click **Add**.

**Step 6** In the **Server Name** field of the **Create TACACS+ Server** slide-in pane, enter a name for the TACACS+ server.

**Step 7** From the **Type** drop-down list, choose the required type.

**Step 8** Based on the type of the TACACS+ server, enter data in the corresponding field.

- If the **Server IP Address** field is displayed, enter the IPv4 address for the TACACS+ server.
- If the **Server IPv6 Address** field is displayed, enter the IPv6 address for the TACACS+ server.
- If the **Server FQDN** field is displayed, enter the FQDN for the TACACS+ server.

**Step 9** From the **Key Type** drop-down list, choose a key type.

**Step 10** In the **Key** field, enter the key for the TACACS+ server for secure authentication.

**Step 11** In the **Confirm Key** field, confirm the key for the TACACS+ server.

**Step 12** (Optional) In the **Port** field, enter the port number to listen for the incoming requests.

The valid range is from 0 to 65535. The default value is 49.

**Step 13** (Optional) In the **Server Timeout (sec)** field, enter the time in seconds to wait for a response from the TACACS+ server.

The valid range is from 1 to 1000.

**Step 14** Click **Review and Provision**.

**Step 15** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 16** On the **Tasks** window, monitor the task deployment.

## Create a TACACS+ server group for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a TACACS+ server group for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **Servers/Groups**, under **TACACS+**, click **Server Groups**.

**Step 5** Click **Add**.

**Step 6** In the **Server Group Name** field of the **Create TACACS+ Server Group** slide-in pane, enter a name for the server group.

**Step 7** Choose the IPv4 and IPv6 source interface from the corresponding drop-down lists.

You can choose a physical, logical, or SVI interface for TACACS+ traffic.

**Step 8** Choose the IPv4 and IPv6 VRF from the corresponding drop-down lists.

**Step 9** Under **Servers**, add servers using one of these options.

- Click the plus icon next to the required server.
- Click the required server and click **Add Selected**.

  To choose multiple servers, press **Shift**, click the server, and click **Add Selected**.
- To add all the servers, click **Add All**.

  You can use the **Search** field to filter the servers.

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create an LDAP server for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an LDAP server for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **Servers/Groups**, under **LDAP**, click **Servers**.

**Step 5** Click **Add**.

**Step 6** In the **Server Name** field of the **Create LDAP Server** slide-in pane, enter a name for the LDAP server.

**Step 7** From the **Type** drop-down list, choose the required type.

**Step 8** Based on the type of the LDAP server, enter data in the corresponding field.

- If the **Server IP Address** field displays, enter the IPv4 address for the LDAP server.
- If the **Server IPv6 Address** field displays, enter the IPv6 address for the LDAP server.
- If the **Server FQDN** field displays, enter the FQDN for the LDAP server.

**Step 9** (Optional) Check the **Authenticate** check box to enable a secure and compliant connection between the wireless controller and the LDAP server.

If you check this check box, enter data in these fields.

- **Bind Username**: enter the user name for the LDAP bind operation.
- **Bind Password**: enter the password for the LDAP bind operation.
- **Confirm Bind Password**: confirm the password for the LDAP bind operation.

**Step 10** In the **Port** field, enter the server listening port number.

The valid range is from 1 to 65535. The default value is 389.

**Step 11** In the **User Based DN** field, enter the base Distinguished Name (DN).

**Step 12** (Optional) In the **Server Timeout (sec)** field, enter the time, in seconds, to wait for a response from the LDAP server before retransmission.

The valid range is from 1 to 65535. The default value is 30.

**Step 13** (Optional) Check the **Secure Mode** check box to ensure that the communication between the wireless controller and LDAP server is encrypted.

(Optional) If you check this check box, from the **Trustpoint Name** drop-down list, choose a trustpoint.

**Step 14** (Optional) Under **User Object Types**, configure user object types.

| If you want to... | Then... |
|---|---|
| add a user object type | **a.** Click **Add**.<br>**b.** In the **User Object Type** field, enter the object type attribute name.<br>**c.** Click **Save**. |
| delete user object types | **a.** Check the check box next to the user object types that you want to delete.<br>**b.** Hover your cursor over **Actions** and click **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 15** Click **Review and Provision**.

**Step 16** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 17** On the **Tasks** window, monitor the task deployment.

# Create an LDAP server group for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an LDAP server group for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **Servers/Groups**, under **LDAP**, click **Server Groups**.

**Step 5** Click **Add**.

**Step 6** In the **Server Group Name** field of the **Create LDAP Server Group** slide-in pane, enter a name for the server group.

**Step 7** Under **Servers**, add servers using one of these options.

- Click the plus icon next to the required server.
- Click the required server and click **Add Selected**.

  To choose multiple servers, press **Shift**, click the server, and click **Add Selected**.
- To add all the servers, click **Add All**.

  You can use the **Search** field to filter the servers.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

# Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an authentication method list for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **AAA Method List** and click **Authentication**.

**Step 5** Hover your cursor over **Add** and choose an authentication type.

- **Type - Login**: for AAA authentication
- **Type - Dot1x**: for web authentication or TACACS

**Step 6** In the **Method List Name** field of the **Create Authentication Method List Profile** slide-in pane, enter a name for the authentication method list profile.

**Step 7** From the **Group Type** drop-down list, choose an option.

- **Group**: for AAA authentication
- **Local**: for authentication on a local device

**Step 8** (Optional) If you chose **Group**, check the **Fallback to Local** check box to use the fallback to the local username authentication.

**Step 9** (Optional) From the **Server Groups** drop-down list, choose a server group.

To create a server group, see Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 153 and Create a TACACS+ server for a Cisco Catalyst 9800 Series Wireless Controller, on page 154.

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an authorization method list for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **AAA Method List** and click **Authorization**.

**Step 5** Hover your cursor over **Add** and choose an authorization type.

- **Type - Network**
- **Type - Exec**
- **Type - Credential-download**

For MAC filter authorization, choose **Type - Network**.

**Step 6** In the **Method List Name** field of the **Create Authorization Method List Profile** slide-in pane, enter a name for the authorization method list profile.

Catalyst Center does not allow spaces or ? in the method list name.

**Step 7** Use the **AAA New Model** toggle button to enable or disable the modular approach to AAA.

This setting determines whether the wireless controller applies the new model method for AAA configuration. Advanced security features and integration with external authentication servers require this method.

**Step 8** From the **Group Type** drop-down list, choose an option.

- **Group**: for AAA authorization
- **Local**: for authorization on a local device

**Step 9** (Optional) If you chose **Group**, check the **Fallback to Local** check box to use the fallback to the local username authentication.

**Step 10** (Optional) Check the **Authenticated** check box to indicate success when the authentication is completed.

**Step 11** (Optional) From the **Server Groups** drop-down list, choose a server group.

For information about how to create a server group, see Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 153 and Create a TACACS+ server for a Cisco Catalyst 9800 Series Wireless Controller, on page 154.

**Step 12** Click **Review and Provision**.

**Step 13** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 14** On the **Tasks** window, monitor the task deployment.

## Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an accounting method list for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **AAA Method List** and choose **Accounting**.

**Step 5** Hover your cursor over **Add** and choose an AAA accounting type.

- **Type - Exec**
- **Type - Network**
- **Type - Identity**
- **Type - Command**

For AAA-based accounting, choose **Type - Identity**.

**Step 6** In the **Method List Name** field of the **Create Accounting Method List Profile** slide-in pane, enter a name for the accounting method list profile.

**Step 7** From the **Server Groups** drop-down list, choose a server group for accounting.

To create a server group, see Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 153 and Create a TACACS+ server for a Cisco Catalyst 9800 Series Wireless Controller, on page 154.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Configure global AAA parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global AAA parameters for a wireless controller and provision them.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **AAA Advanced** and choose **Global Configuration**.

**Step 5** Under **Global Configurations**, complete these configurations.

- Use the **System Auth Control** check box to enable or disable system authorization control.
- From the **Local Authentication** drop-down list, choose an authentication.

| If you chose... | Then... |
|---|---|
| **None** | ensure that you choose **None** for local authorization. |
| **Method List** | from the **Authentication Method List** drop-down list, choose an authentication method list.<br>To create an authentication method list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 158. |

- From the **Local Authorization** drop-down list, choose an authorization.

| If you chose... | Then... |
|---|---|
| **None** | ensure that you choose **None** for local authentication. |
| **Method List** | from the **Authorization Method List** drop-down list, choose an authorization method list.<br>To create an authorization method list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159. |

- Use the **RADIUS Server Load Balance** check box to enable or disable load balancing for a RADIUS server.

- Use the **Interim Update** check box to enable or disable interim accounting updates.

**Step 6** Under **RADIUS Attributes - Accounting**, complete these configurations.

- From the **Called-station-id** drop-down list, choose the attribute that is appended as the Called-Station-ID.
- From the **Called-station-id Case** drop-down list, choose the capitalization option for the values that are sent on the Called-Station-ID.
- (Optional) From the **MAC Delimiter** drop-down list, choose the character that is used to separate the octets in MAC addresses within accounting records.
- From the **Username Case** drop-down list, choose the capitalization option for the user names.
- From the **Username Delimiter** drop-down list, choose the delimiters for user names.

**Step 7** Under **RADIUS Attributes - Authentication**, complete these configurations.

- From the **Called-station-id** drop-down list, choose the attribute that is appended as the Called-Station-ID.
- From the **Called-station-id Case** drop-down list, choose the capitalization option for the values that are sent on the Called-Station-ID.
- From the **MAC Delimiter** drop-down list, choose the character that is used to separate the octets in MAC addresses within accounting records.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create a password policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a password policy for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **AAA Advanced** and choose **Password Policy**.

**Step 5** Click **Add**.

**Step 6** Enter data in these fields of the **Create Password Policy** slide-in pane.

- **Password Policy Name**: enter a name for the password policy.
- **Minimum Length**: enter the minimum length of the password.

  The valid range is from 1 to 127. The default value is 1.
- **Maximum Length**: enter the maximum length of the password.

  The valid range is from 1 to 127. The default value is 127.
- **Upper Count**: enter the number of allowed uppercase letters in the password.

  The valid range is from 0 to 127. The default value is 0.
- **Lower Count**: enter the number of allowed lowercase letters in the password.

  The valid range is from 0 to 127. The default value is 0.
- **Numeric Count**: enter the number of allowed numbers in the password.

  The valid range is from 0 to 127. The default value is 0.
- **Special Count**: enter the number of allowed special characters in the password.

  The valid range is from 0 to 127. The default value is 0.
- **Character Changes**: enter the number of characters that must be changed between the old and new passwords.

  The valid range is from 1 to 127. The default value is 4.
- (Optional) **Max Number of Character Repetition**: enter the maximum number of times for repeating a character consecutively in the password.

  The valid values are 0 and 2–5. The default value is 0. To disable this rule, enter 0.

**Step 7** (Optional) Check the **Prohibit Consecutive Four Keyboard Letters** check box to prohibit the use of consecutive characters or numbers on the keyboard in the password.

If you check this check box, the password can't contain four consecutive letters or numbers on the keyboard in both directions.

**Step 8** From the **Validity** drop-list, choose a validity for the password.

For the user-defined validity, enter data in these fields:

- **Years**: enter the number of years for password expiration.

  The valid range is from 0 to 99.
- **Months**: enter the number of months for password expiration.

  The valid range is from 0 to 11.
- **Days**: enter the number of days for password expiration.

The valid range is from 0 to 30.

- **Hours**: enter the number of hours for password expiration.

  The valid range is from 0 to 23.

- **Minutes**: enter the number of minutes for password expiration.

  The valid range is from 0 to 59.

- **Seconds**: enter the number of seconds for password expiration.

  The valid range is from 0 to 59.

**Step 9** Click **Review and Provision**.

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Configure RADIUS fallback for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure RADIUS fallback for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **AAA Advanced** and choose **RADIUS Fallback**.

**Step 5** (Optional) Enter data in these fields.

- **Retransmit Count**: enter the number of retries to the active server.

  The valid range is from 0 to 100.

- **Timeout Interval (sec)**: enter the time, in seconds, to wait for a RADIUS server to reply.

  The valid range is from 1 to 1000.

- **Dead Time (min)**: enter the time, in minutes, to stop using an unresponsive server.

  The valid range is from 1 to 1440.

- **Dead Criteria Time (sec)**: enter the time, in seconds, to determine how quickly the system switches to a backup server to ensure uninterrupted network authentication and access.

  The valid range is from 1 to 120.

- **Dead Criteria Retries**: enter the required number of consecutive response failures from the RADIUS server to the router to mark the RADIUS server as inactive.

  The valid range is from 1 to 100.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Create an attribute list for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an attribute list for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA**.

**Step 4** Hover your cursor over **AAA Advanced** and choose **Attribute Lists**.

**Step 5** Click **Add**.

**Step 6** In the **Attribute List Name** field of the **Create Attribute List** slide-in pane, enter a name for the attribute list.

**Step 7** (Optional) Under **Attributes**, configure the required attributes.

| If you want to... | Then... |
|---|---|
| add an attribute | **a.** Click **Add**.<br>**b.** In the **Add Attribute** dialog box, enter data in these fields.<br>• **Attribute Type**: enter the name of the attribute type for streamlined user access control.<br>Alternatively, when you start typing, the list of available attribute types is displayed. You can choose the required attribute type from this list.<br>• **Attribute Value**: enter the value associated with the chosen attribute type.<br>Alternatively, if the **Attribute Value** drop-down list is displayed, choose the required value.<br>**c.** Click **Save**. |
| delete attributes | **a.** Check the check box next to the required attributes.<br>**b.** Hover your cursor over **Actions**, and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create an AAA policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AAA policy profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AAA Policy**.

**Step 4** Click **Add**.

**Step 5** In the **Policy Name** field of the **Create AAA Policy Profile** slide-in pane, enter a name for the AAA policy.

**Step 6** From the NAS ID option drop-down lists, choose the required RADIUS NAS ID options.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv4 ACL for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **ACL**.

**Step 4** Hover your cursor over **IPv4/IPv6**, under **IPv4**, choose **Standard**.

**Step 5** Click **Add**.

**Step 6** In the **ACL Name** field of the **Create IPv4 Standard ACL** slide-in pane, enter a unique name for the IPv4 ACL.

The ACL name can contain up to 231 alphanumeric characters and special characters. If you're entering only numbers, the valid range is either 1 to 99 and 1300 to 1999. If the ACL name has a special character, it must start with an alphabetic character. Catalyst Center does not support ? and spaces in the ACL name.

**Step 7** (Optional) Under **Rules**, configure the required rules.
a) To create a rule, complete these steps:
1. Click **Add**.
2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

The valid range is from 1 to 2147483647.

3. From the **Action** drop-down list, choose an action.
   - **permit**: allow the traffic
   - **deny**: block the traffic
4. From the **Source Type** drop-down list, choose a traffic source to apply for the rule.
   - **Any**: applies to traffic from any source IPv4 address.
   - **Host**: applies to traffic from a specific IPv4 address.

     If you choose **Host**, in the **Source IP** field, enter the IP address of a source host. Catalyst Center does not support 0.0.0.0 as the IP address of a source host.
   - **Network**: applies to traffic from a network.

     If you choose **Network**, enter data in these fields:
     - **Subnet IP**: Enter the subnet IP address. Catalyst Center does not support 0.0.0.0 as the subnet IP address.
     - **Source Wildcard**: enter the wildcard bits to apply to the source. Catalyst Center does not support 0.0.0.0 as the wildcard.
5. (Optional) Check the **Log** check box to create logs for matches against this entry.
6. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create an IPv4 role-based ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv4 role-based ACL for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **ACL**.

**Step 4** Hover your cursor over **IPv4/IPv6**, under **IPv4**, choose **Role-based**.

**Step 5** Click **Add**.

**Step 6** In the **ACL Name** field of the **Create IPv4 Role-based ACL** slide-in pane, enter a unique name for the IPv4 ACL.

The ACL name can contain up to 229 alphanumeric characters and special characters. If the ACL name has a special character, it must start with an alphabetic character. Catalyst Center does not support ? and spaces in the ACL name.

**Step 7** (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

   The valid range is 1 to 2147483647.
3. From the **Action** drop-down list, choose an action.

   - **permit**: allow the traffic
   - **deny**: block the traffic
4. In the **Protocol** field, specify a protocol to apply for the rule. You can enter a number in the range 0 to 255 or an IOS keyword such as bgp, tcp, udp, and so on.

   If you use TCP or UDP, choose a port operator to specify how the port numbers are evaluated from these drop-down lists:

   - **Source Port Operator**: choose a source port operator.

| If you choose... | Then... |
|---|---|
| **eq**, **gt**, **lt**, or **neq** | In the **Source Port** field, enter the source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |
| **range** | Enter the range of port numbers in these fields:<br>• **Start Source Port**: enter the starting source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.<br>• **End Source Port**: enter the ending source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |

• **Destination Port Operator**: choose a destination port operator.

| If you choose... | Then... |
|---|---|
| **eq**, **gt**, **lt**, or **neq** | In the **Destination Port** field, enter the destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |
| **range** | Enter the range of port numbers in these fields:<br>• **Start Destination Port**: enter the starting destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.<br>• **End Destination Port**: enter the ending destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |

5. (Optional) From the **Dscp** drop-down list, choose a DSCP value for the rule.
6. (Optional) Check the **Log** check box to create logs for matches against this entry.
7. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.

3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create an IPv4 extended ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv4 extended ACL for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **ACL**.

**Step 4** Hover your cursor over **IPv4/IPv6**, under **IPv4**, choose **Extended**.

**Step 5** Click **Add**.

**Step 6** In the **ACL Name** field of the **Create IPv4 Extended ACL** slide-in pane, enter a unique name for the IPv4 extended ACL.

The ACL name can contain up to 231 alphanumeric characters and special characters. If you're entering only numbers, the valid range is either 1 to 99 or 1300 to 1999. If the ACL name has a special character, it must start with an alphabetic character. Catalyst Center doesn't support ? and spaces in the ACL name.

**Step 7** (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

   The valid range is 1 to 2147483647.
3. From the **Action** drop-down list, choose an action.
   - **permit**: allow the traffic
   - **deny**: block the traffic
4. From the **Source Type** drop-down list, choose a traffic source to apply for the rule.
   - **Any**: applies to traffic from any source IPv4 address.
   - **Host**: applies to traffic from a specific IPv4 address.

     If you choose **Host**, in the **Source IP** field, enter the IP address of a source host. Catalyst Center does not support 0.0.0.0 as the IP address of a source host.
   - **Network**: applies to traffic from a network.

     If you choose **Network**, enter data in these fields:
     - **Subnet IP**: Enter the subnet IP address. Catalyst Center does not support 0.0.0.0 as the subnet IP address.
     - **Source Wildcard**: enter the wildcard bits to apply to the source. Catalyst Center does not support 0.0.0.0 as the wildcard.
5. From the **Destination Type** drop-down list, choose a traffic destination to apply for the rule.
   - **Any**: applies to traffic to any destination IPv4 address.
   - **Host**: applies to traffic to a specific IPv4 address.

     If you choose **Host**, in the **Destination IP** field, enter the IP address of a destination host. Catalyst Center does not support 0.0.0.0 as the IP address of a destination host.
   - **Network**: applies to traffic to a network.

     If you choose **Network**, enter data in these fields:
     - **Subnet IP**: Enter the subnet IP address. Catalyst Center does not support 0.0.0.0 as the subnet IP address.
     - **Destination Wildcard**: enter the wildcard bits to apply to the source. Catalyst Center does not support 0.0.0.0 as the wildcard.
6. In the **Protocol** field, specify a protocol to apply for the rule. You can enter a number in the range 0 to 255 or an IOS keyword such as bgp, tcp, udp, and so on.

   If you use TCP or UDP, choose a port operator to specify how the port numbers are evaluated from these drop-down lists:
   - **Source Port Operator**: choose a source port operator.

| If you choose... | Then... |
|---|---|
| **eq**, **gt**, **lt**, or **neq** | In the **Source Port** field, enter the source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |
| **range** | Enter the range of port numbers in these fields:<br>• **Start Source Port**: enter the starting source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.<br>• **End Source Port**: enter the ending source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |

• **Destination Port Operator**: choose a destination port operator.

| If you choose... | Then... |
|---|---|
| **eq**, **gt**, **lt**, or **neq** | In the **Destination Port** field, enter the destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |
| **range** | Enter the range of port numbers in these fields:<br>• **Start Destination Port**: enter the starting destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.<br>• **End Destination Port**: enter the ending destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |

7. (Optional) From the **Dscp** drop-down list, choose a DSCP value for the rule.
8. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.

4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv6 ACL for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **ACL**.

**Step 4** Hover your cursor over **IPv4/IPv6**, under **IPv6**, choose **IPv6**.

**Step 5** Click **Add**.

**Step 6** In the **ACL Name** field of the **Create IPv6 ACL** slide-in pane, enter a unique name for the IPv6 ACL.

The ACL name can contain up to 233 alphanumeric characters and special characters. It must not start with a number. Catalyst Center doesn't support ? and spaces in the ACL name.

**Step 7** (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.

2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

   The valid range is 1 to 4294967294.

3. From the **Action** drop-down list, choose an action.

   - **permit**: allow the traffic
   - **deny**: block the traffic

4. From the **Source Type** drop-down list, choose a traffic source to apply for the rule.

   - **Any**: applies to traffic from any source IPv6 address.
   - **Host**: applies to traffic from a specific IPv6 address.

     If you choose **Host**, in the **Source IP** field, enter the valid IPv6 address of a source host. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as the IPv6 address.

   - **Network**: applies to traffic from a network.

     If you choose **Network**, enter data in these fields:

     - **Source IP**: Enter the source subnet IP address. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: for the IPv6 address.
     - **Source Wildcard Bits**: enter the wildcard bits to apply to the source. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as a value in this field.

5. From the **Destination Type** drop-down list, choose a traffic destination to apply for the rule.

   - **Any**: applies to traffic to any destination IPv6 address.
   - **Host**: applies to traffic to a specific IPv6 address.

     If you choose **Host**, in the **Destination IP** field, enter the IP address of a destination host. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as the IPv6 address.

   - **Network**: applies to traffic to a network.

     If you choose **Network**, enter data in these fields:

     - **Destination IP**: Enter the destination subnet IP address. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as the IPv6 address.
     - **Destination Wildcard Bits**: enter the wildcard bits to apply to the destination. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as a value in this field.

6. In the **Protocol** field, specify a protocol to apply for the rule. You can enter a number in the range 0 to 255 or an IOS keyword such as bgp, tcp, udp, and so on.

   If you use TCP or UDP, choose a port operator to specify how the port numbers are evaluated from these drop-down lists:

   - **Source Port Operator**: choose a source port operator.

| If you choose... | Then... |
|---|---|
| **eq**, **gt**, **lt**, or **neq** | In the **Source Port** field, enter the source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |
| **range** | Enter the range of port numbers in these fields:<br>• **Start Source Port**: enter the starting source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.<br>• **End Source Port**: enter the ending source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |

• **Destination Port Operator**: choose a destination port operator.

| If you choose... | Then... |
|---|---|
| **eq**, **gt**, **lt**, or **neq** | In the **Destination Port** field, enter the destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |
| **range** | Enter the range of port numbers in these fields:<br>• **Start Destination Port**: enter the starting destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.<br>• **End Destination Port**: enter the ending destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |

7. (Optional) From the **Dscp** drop-down list, choose a DSCP value for the rule.
8. (Optional) Check the **Log** check box to create logs for matches against this entry.
9. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.

3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create an IPv6 role-based ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv6 role-based ACL for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **ACL**.

**Step 4** Hover your cursor over **IPv4/IPv6**, under **IPv6**, choose **Role-based**.

**Step 5** Click **Add**.

**Step 6** In the **ACL Name** field of the **Create IPv6 Role-based ACL** slide-in pane, enter a unique name for the IPv6 ACL.

The ACL name can contain up to 222 alphanumeric characters and special characters. It must not start with a number. Catalyst Center doesn't support ? and spaces in the ACL name.

**Step 7** (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

   The valid range is 1 to 4294967294.
3. From the **Action** drop-down list, choose an action.
   - **permit**: allow the traffic
   - **deny**: block the traffic
4. In the **Protocol** field, specify a protocol to apply for the rule. You can enter a number in the range 0 to 255 or an IOS keyword such as bgp, tcp, udp, and so on.

   If you use TCP or UDP, choose a port operator to specify how the port numbers are evaluated from these drop-down lists:
   - **Source Port Operator**: choose a source port operator.

| If you choose... | Then... |
|---|---|
| **eq**, **gt**, **lt**, or **neq** | In the **Source Port** field, enter the source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |
| **range** | Enter the range of port numbers in these fields:<br>• **Start Source Port**: enter the starting source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.<br>• **End Source Port**: enter the ending source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |

   - **Destination Port Operator**: choose a destination port operator.

| If you choose... | Then... |
|---|---|
| **eq**, **gt**, **lt**, or **neq** | In the **Destination Port** field, enter the destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |

| If you choose... | Then... |
|---|---|
| **range** | Enter the range of port numbers in these fields:<br>• **Start Destination Port**: enter the starting destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.<br>• **End Destination Port**: enter the ending destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on.<br>Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. |

5. (Optional) From the **Dscp** drop-down list, choose a DSCP value for the rule.
6. (Optional) Check the **Log** check box to create logs for matches against this entry.
7. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

# Create a MAC-based ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a MAC-based ACL for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **ACL**.

**Step 4** Click the **MAC-Based** tab.

**Step 5** Click **Add**.

**Step 6** In the **ACL Name** field of the **Create MAC-Based ACL** slide-in pane, enter a unique name for the MAC-based ACL.

The ACL name can contain up to 230 alphanumeric characters and special characters. Catalyst Center doesn't support ? and spaces in the ACL name. If the ACL name has an alphanumeric or special character, it must start with an alphabetic character.

**Step 7** (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. From the **Action** drop-down list, choose an action.
   - **permit**: allow the traffic
   - **deny**: block the traffic
3. From the **Source Type** drop-down list, choose a traffic source to apply for the rule.
   - **Any**: applies to traffic from any source MAC address.
   - **Host**: applies to traffic from a specific MAC address.

     If you choose **Host**, in the **Source MAC** field, enter the source MAC address. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
   - **Network**: applies to traffic from a network.

     If you choose **Network**, enter data in these fields:
     - **Source MAC**: Enter the source MAC address. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
     - **Source MAC Wildcard**: enter the wildcard bits to apply to the source. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.

4. From the **Destination Type** drop-down list, choose a traffic destination to apply for the rule.
   - **Any**: applies to traffic to any destination MAC address.
   - **Host**: applies to traffic to a specific MAC address.

     If you choose **Host**, in the **Destination MAC** field, enter the destination MAC address. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
   - **Network**: applies to traffic to a network.

     If you choose **Network**, enter data in these fields:
     - **Destination MAC**: Enter the destination MAC address. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
     - **Destination MAC Wildcard**: enter the wildcard bits to apply to the destination. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
5. Click **Save**.

b) To edit a rule, complete these steps:
1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:
1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:
- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create a local EAP profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a local EAP profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **EAP**.

**Step 4** In the **Local EAP Profiles** tab, click **Add**.

**Step 5** In the **Local EAP Profile Name** field of the **Create Local EAP Profiles** slide-in pane, enter a unique name for the local EAP profile.

The profile name can contain up to 63 alphanumeric and special characters.

**Step 6** (Optional) Check the required check boxes to allow the corresponding EAP methods.

**Step 7** (Optional) Based on the EAP method that you chose, complete these configurations.

| If you chose... | Then... |
|---|---|
| **EAP-TLS**, **EAP-FAST**, or **PEAP** | from the **Trustpoint Name** drop-down list, choose a default PKI trustpoint. |
| **EAP-FAST** | from the **EAP-FAST Profile** drop-down list, choose an EAP FAST profile.<br>To create an EAP FAST profile, see Create an EAP-FAST profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 183. |

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create an EAP-FAST profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an EAP-FAST profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **EAP**.

**Step 4** Click the **EAP-FAST Profiles** tab.

**Step 5** Click **Add**.

**Step 6** In the **Create EAP-FAST Profiles** slide-in pane, enter data in these fields.

- **EAP-FAST Profile Name**: enter a unique name for the EAP-FAST profile.

  The profile name can contain up to 63 alphanumeric and special characters.

- **Server Key**: enter a local key for the profile.
- **Confirm Server Key**: reenter the same local key for the profile.
- **Time to Live (sec)**: enter the Protected Access Credential (PAC) time-to-live in seconds.

  The valid range is 1 to 700000000. The default value is 86400.

- (Optional) **Authority ID**: enter an authority ID for the profile.

  The authority ID can contain up to 231 alphanumeric and special characters.

- (Optional) **Authority ID Information**: enter the authority ID information.

  The authority ID information can contain up to 228 alphanumeric and special characters.

- (Optional) **Description**: enter a description.

  The description can contain up to 241 alphanumeric and special characters.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

# Configure advanced EAP for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the advanced EAP profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **EAP**.

**Step 4** Click the **Advanced** tab.

**Step 5** Enter data in these fields.

- **EAP-Identity-Request Timeout (sec)**: enter an EAP identity request timeout in seconds.

  The valid range is from 1 to 120. The default value is 40.

- **EAP-Identity-Request Max Retries**: enter the maximum number of EAP identity request retransmissions.

  The valid range is from 1 to 20. The default value is 2.

**Step 6** (Optional) Check the **EAP Max-Login Ignore Identity Response** check box to limit the number of clients that can be connected to the device with the same username.

**Step 7** Enter data in these fields.

- **EAP-Request Timeout (sec)**: enter the EAP request retransmission timeout in seconds.

  The valid range is from 1 to 120. The default value is 30.

- **EAP-Request Max Retries**: enter the maximum number of EAP request retransmissions.

  The valid range is from 0 to 20. The default value is 2.

- **EAPOL-Key Timeout (msec)**: enter the EAP over LAN (EAPOL) key retransmission timeout in milliseconds.

  The valid range is from 200 to 5000. The default value is 1000.

- **EAPOL-Key Max Retries**: enter the maximum number of EAPOL key retries.

  The valid range is from 0 to 4. The default value is 2.

- **EAP-Broadcast Key Interval (sec)**: enter the EAP broadcast key renewal interval in seconds.

  The valid range is from 120 to 86400. The default value is 3600.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create a basic URL filter for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a basic URL filter for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **URL Filters**.

**Step 4** In the **Basic** tab, click **Add**.

**Step 5** In the **Url List Name** field of the **Create Basic URL Filter** slide-in pane, enter a unique name for the URL filter.

The URL filter name can contain up to 32 characters. Catalyst Center does not support ? # % + ' or spaces in the URL filter name.

**Step 6** From the **Filter Type** drop-down list, choose the authentication that is used for the URL filter.

If you chose **POST-AUTH**, enter data in these fields.

- **IPv4 Redirect Server**: enter the IPv4 address of the redirect server.
- **IPv6 Redirect Server**: enter the IPv6 address of the redirect server.

**Step 7** From the **Action** drop-down list, choose an action to indicate if the URLs in the URL filter are allowed or blocked.

**Step 8** (Optional) Under **URLs**, configure URL domain names for the URL filter.

| If you want to... | Then... |
|---|---|
| add a URL domain name to the URL filter | **a.** Click **Add**.<br>**b.** In the **Url Name** field of the **Add URL** dialog box, enter a domain name for the URL filter.<br>The domain name can contain up to 255 characters. Catalyst Center supports the special characters - _ . and * in the domain name. * is used as a wildcard character (for example, *cisco.com). Catalyst Center does not support subdomains using backslash (/).<br>**c.** Click **Save**. |
| delete domain names from the URL filter | **a.** Check the check box next to the domain names that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 9** Click **Review and Provision**.

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Create an enhanced URL filter for a Cisco Catalyst 9800 Series Wireless Controller

Enhanced URL filters are the Fully Qualified Domain Name (FQDN) ACLs that are applied to the wireless network.

Use this procedure to create an enhanced URL filter for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **URL Filters**.

**Step 4** Click the **Enhanced** tab.

**Step 5** Click **Add**.

**Step 6** In the **Url List Name** field of the **Create Enhanced URL Filter** slide-in pane, enter a unique name for the enhanced URL filter.

The URL filter name can contain up to 32 characters. Catalyst Center does not support ? # % + ' or spaces in the URL filter name.

**Step 7** (Optional) Under **Rules**, configure rules for the URL filter.

| If you want to... | Then... |
|---|---|
| add a rule | **a.** Click **Add**.<br>**b.** In the **URL** field of the **Add URL** dialog box, enter a URL, FQDN, or domain name for the enhanced URL rule.<br>The domain name can contain up to 255 characters. Catalyst Center supports the special characters - _ . and * in the domain name. * is used as a wildcard character (for example, *cisco.com). Catalyst Center does not support subdomains using backslash (/).<br>**c.** In the **Preference** field, enter a priority for the rule.<br>The valid range is from 0 to 65535.<br>**d.** Click **Save**.<br>**e.** From the **Action** drop-down list, choose an action. |
| edit a rule | **a.** Check the check box next to the required rule.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** From the **Action** drop-down list, update the action for the rule.<br>**d.** Click **Save**. |
| delete rules | **a.** Check the check box next to the rules that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create a guest user for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a guest user for a wireless controller and provision.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Guest User**.

**Step 4** Click **Add**.

**Step 5** In the **Create Guest User** slide-in pane, under **General**, complete these configurations.

- In the **User Name** field, enter a username for the guest user.
- (Optional) Check the **Generate Password** check box to generate a password for the guest user.
- In the **Password** field, enter a password for the guest user.

  **Note** If you check the **Generate Password** check box, this field is automatically populated.

- In the **Confirm Password** field, reenter the password.

  **Note** If you check the **Generate Password** check box, this field is automatically populated.

- In the **Description** field, enter a description.
- In the **No. of Simultaneous User Logins** field, enter the maximum allowed simultaneous login attempts for the guest user.

  The valid range is from 0 to 64.

**Step 6** Under **Lifetime**, enter data in these fields.

- **Years**: enter the number of years for which the guest user credentials can be used.

  The valid range is from 0 to 1. The default value is 0.

- **Months**: enter the number of months for which the guest user credentials can be used.

  The valid range is from 0 to 11. The default value is 0.

- **Days**: enter the number of days for which the guest user credentials can be used.

  The valid range is from 0 to 30. The default value is 1.

- **Hours**: enter the number of hours for which the guest user credentials can be used.

  The valid range is from 0 to 23. The default value is 0.

- (Optional) **Minutes**: enter the number of minutes for which the guest user credentials can be used.

  The valid range is from 0 to 59. The default value is 0.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure web authentication parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the web authentication parameters for a wireless controller and provision.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Web Auth**.

**Step 4** In the **Global** tab, complete these configurations.

a) Under **General**, complete these configurations.

- (Optional) In the **Maximum HTTP Connections** field, enter the maximum number of allowed HTTP connections per client.

  The valid range is from 1 to 200.

- In the **Init-State Timeout(Secs)** field, enter the timeout in seconds.

The valid range is from 60 to 3932100.

- From the **Type** drop-down list, choose the authentication type.
- (Optional) If you chose the authentication type **consent**, check the **Turn-On Consent with Email** check box to enable consent with email.
- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Captive Bypass Portal**: enable captive bypassing for web authentication
  - **Disable Success Window**: disable the default success window for the wireless controller after successful web authentication
  - **Disable Logout Window**: disable the web authentication logout window
  - **Disable Cisco Logo**: disable the Cisco logo on internal HTML windows
- (Optional) Enter data in these fields.
  - **Sleeping Client Timeout (Minutes)**: enter the client sleep timeout in minutes.

    The valid range is from 10 to 43200.
  - **Trustpoint**: enter the trustpoint name.
  - **Virtual IPv4 Address**: enter the virtual IPv4 address.
  - **Virtual IPv6 Address**: enter the virtual IPv6 address.
- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Web Auth intercept HTTPS**: enable the interception of the HTTPS traffic
  - **Enable HTTP server for Web Auth**: configure an HTTP server for web authentication
  - **Disable HTTP secure server for Web Auth**: disable the HTTPS server for web authentication

b) (Optional) Under **Banner Configuration**, complete these configurations.

- In the **Banner Title** field, enter the text for the banner title.

  You can enter up to 127 characters. For example, *c* **banner-title-text** *c*, where *c* is a delimiter.
- Under **Banner Type**, click the radio button next to the required option.

| If you chose... | Then... |
|---|---|
| **Banner Text** | in the **Banner Text** field, enter the text to display in the banner.<br>You can enter up to 400 characters. For example, *c* **banner-text** *c*, where *c* is a delimiter. |
| **File Name** | in the **Read from File** field, enter the name of the file from which the banner text can be read. |

c) (Optional) Under **Redirect to external server**, enter data in these fields for external web authentication.

- **Redirect URL for login**: enter the URL to redirect the user for a login request.

You can enter up to 230 characters.

- **Redirect On-Success**: enter the URL to redirect the user after a successful login.

  You can enter up to 230 characters.

- **Redirect On-Failure**: enter the URL to redirect the user after a failed login.

  You can enter up to 230 characters.

- **Redirect Append for AP MAC Address**: enter the AP MAC address to be appended to the redirection.
- **Redirect Append for Client MAC Address**: enter the client MAC address to be appended to the redirection.
- **Redirect Append for WLAN SSID**: enter the WLAN SSID to be appended to the redirection.
- **Portal IPV4 Address**: enter the IPv4 address of the portal to send redirects.
- **Portal IPV6 Address**: enter the IPv6 address of the portal to send redirects, if the IPv6 address is used.

d) (Optional) Under **Customized page**, enter data in these fields for customized web authentication.

- **Login Page**: enter the file details for the customized login window for web authentication in the *bootflash:filename* format.
- **Logout Page**: enter file details for the customized logout window for web authentication in the *bootflash:filename* format.
- **Login Successful Page**: enter the file details for the customized window for a successful login in the *bootflash:filename* format.
- **Login Failed Page**: enter the file details for the customized window for a failed login in the *bootflash:filename* format.

**Step 5** Click **Review and Provision**.

**Step 6** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 7** On the **Tasks** window, monitor the task deployment.

## Create a web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a web authentication profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Web Auth**.

**Step 4** Click the **Web Auth Profiles** tab.

**Step 5** Click **Add**.

**Step 6** In the **General** tab of the **Create Web Auth** slide-in pane, complete these configurations.

- In the **Parameter Map Name** field, enter a name for the web authentication profile.
- (Optional) In the **Maximum HTTP connections** field, enter the maximum number of allowed HTTP connections.

  The valid range is from 1 to 200.
- From the **Type** drop-down list, choose an authentication type: **authbypass**, **webauth**, **consent**, or **webconsent**
- (Optional) In the **Init-State Timeout(secs)** field, enter the web authentication timeout in seconds.

  The valid range is from 60 to 3932100.
- (Optional) Check the **Sleeping Client Status** check box to enable authentication of sleeping clients.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

### What to do next

To configure additional parameters for the web authentication profile, refer to Configure web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 193.

## Configure web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure additional parameters for web authentication profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Web Auth**.

**Step 4** Select the web authentication profile for which you want to configure additional parameters:

a) Click the **Web Auth Profiles** tab.
b) Check the check box for the required web authentication profile.
c) Hover your cursor over **Actions** and choose **Edit**.

**Step 5** In the **General** tab of the **Edit Web Auth** slide-in pane, complete these configurations.

a) Under **General**, complete these configurations:

- (Optional) In the **Maximum HTTP connections** field, enter the maximum number of allowed HTTP connections.

  The valid range is from 1 to 200.

- From the **Type** drop-down list, choose an authentication type: **authbypass**, **webauth**, **consent**, or **webconsent**
- (Optional) In the **Init-State Timeout(secs)** field, enter the web authentication timeout in seconds.

  The valid range is from 60 to 3932100.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Captive Bypass Portal**: enable captive bypassing for web authentication
  - **Disable Success Window**: disable the default success window for the wireless controller after successful web authentication
  - **Disable Logout Window**: disable the web authentication logout window
  - (Optional) Check the **Sleeping Client Status** check box to enable authentication of sleeping clients.

    If you enable this option, in the **Sleeping Client Timeout (minutes)** field, you can optionally enter the sleep timeout in minutes.

    The valid range is from 10 to 43200 minutes.

b) (Optional) Under **Banner Configuration**, complete these configurations.

- In the **Banner Title** field, enter the text for the banner title.

  The title can contain up to 127 characters.

- Under **Banner Type**, select the required option: **None**, **Banner Text**, or **File Name**.

| If you chose... | Then... |
|---|---|
| **Banner Text** | in the **Banner Text** field, enter the text to display in the banner.<br>For example, *c* **banner-text** *c*, where *c* is a delimiter. |

| If you chose... | Then... |
|---|---|
| **Read From File** | in the **File Name** field, enter the name of the file from which the banner text can be read.<br>The file name can contain up to 61 characters. |

**Step 6** In the **Advanced** tab, complete these configurations:

a) (Optional) Under **Redirect to external server**, enter data in these fields for external web authentication.

- **Redirect URL for login**: enter the URL to redirect the user for a login request.

  You can enter up to 230 characters. Catalyst Center does not allow spaces in the URL.

- **Redirect On-Success**: enter the URL to redirect the user after a successful login.

  You can enter up to 230 characters. Catalyst Center does not allow spaces in the URL.

- **Redirect On-Failure**: enter the URL to redirect the user after a failed login.

  You can enter up to 230 characters. Catalyst Center does not allow spaces in the URL.

- **Redirect Append for AP MAC Address**: enter the redirect append for the AP MAC address to be appended to the redirect ACL.

  You can enter up to 227 characters. Catalyst Center does not allow spaces and ? in the redirect append.

- **Redirect Append for Client MAC Address**: enter the redirect append for the client MAC address to be appended to the redirect ACL.

  You can enter up to 223 characters. Catalyst Center does not allow spaces and ? in the redirect append.

- **Redirect Append for WLAN SSID**: enter the redirect append for the WLAN SSID to be appended to the redirect ACL.

  You can enter up to 224 characters. Catalyst Center does not allow spaces and ? in the redirect append.

- **Portal IPV4 Address**: enter the IPv4 address of the portal to send redirects.

  Enter the IP address in the *xxx.xxx.xxx.xxx* format.

- **Portal IPV6 Address**: enter the IPv6 address of the portal to send redirects, if the IPv6 address is used.

  Enter the IP address in the *X:X:X:X:X:X:X:X* format.

b) (Optional) Under **Customized page**, enter data in these fields for customized web authentication.

- **Login Page**: enter the file details for the customized login window for web authentication in the *bootflash:filename* format.

  File details must start with *bootflash:*, *harddisk:*, or *flash:*.

- **Logout Page**: enter file details for the customized logout window for web authentication in the *bootflash:filename* format.

  File details must start with *bootflash:*, *harddisk:*, or *flash:*.

- **Login Successful Page**: enter the file details for the customized window for a successful login in the *bootflash:filename* format.

File details must start with *bootflash:*, *harddisk:*, or *flash:*.

- **Login Failed Page**: enter the file details for the customized window for a failed login in the *bootflash:filename* format.

  File details must start with *bootflash:*, *harddisk:*, or *flash:*.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure CTS for a Cisco Catalyst 9800 Series Wireless Controller

Cisco TrustSec provides security improvements to Cisco network devices based on the capability to strongly identify users, hosts, and network devices within a network. TrustSec provides topology-independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

Use this procedure to configure Cisco TrustSec (CTS) for a Cisco Catalyst 9800 Series Wireless Controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Trustsec**.

**Step 4** In the **Global** tab, configure the Cisco TrustSec (CTS) parameters.

**Step 5** (Optional) In the **CTS Device ID** field, enter a name for the TrustSec network access device.

The name can contain up to 32 characters. The name must be same as the name configured in Cisco Identity Services Engine.

**Step 6** (Optional) In the **CTS Password**, enter a password for the CTS.

The password can contain up to 162 characters. Catalyst Center does not support ? and spaces in the password.

**Step 7** (Optional) From the **CTS Authorization List** drop-down list, choose a list of AAA servers for the TrustSec device.

To create an authorization list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159.

**Step 8** (Optional) In the **CTS Device SGT** field, enter a number for the local device security group.

The valid range is from 2 to 65519. For Cisco IOS XE Release 17.17.1 or later, the valid range is from 2 to 65521.

**Step 9** (Optional) Under **Policy Server Configuration**, complete these configurations:

- In the **Device Name** field, enter the name of the device used in Cisco ISE.
- In the **Username** field, enter the user name.

  The user name can contain up to 32 characters.
- From the **Encryption** drop-down list, choose the encryption type for the password.
- In the **Password** field, enter the password.

  The password can contain up to 24 characters.

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

### What to do next

In the **Policy Servers** table, you can optionally add, edit, or delete policy servers. To add a policy server, see Create a policy server for CTS configuration, on page 197.

## Create a policy server for CTS configuration

Use this procedure to create a policy server for CTS policy server configuration for a Cisco Catalyst 9800 Series Wireless Controller and provision it.

For information about CTS configuration for a wireless controller, see Configure CTS for a Cisco Catalyst 9800 Series Wireless Controller, on page 196.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Trustsec**.

**Step 4** In the **Global** tab, under **Policy Servers** table, click **Add**.

**Step 5** In the **Create Policy Server** slide-in pane, under **Policy Server Profile**, complete these configurations:

- In the **Policy Server Profile Name** field, enter a unique name for the policy server profile.

  The profile name can contain up to 255 characters. Catalyst Center does not support question mark (?) and spaces in the profile name. This name identifies the policy server configuration in the wireless controller.

- (Optional) In the **Domain Name** field, enter the Fully Qualified Domain Name (FQDN) of the policy server. To use DNS resolution, use this name instead of an IP address.

  The domain name can contain up to 128 characters.

- (Optional) In the **Server Port** field, enter the port number that is used to connect to the policy server.

  The valid range is from 1025 to 65535. Ensure that this port matches the listening port configured on the policy server.

- (Optional) In the **Retransmit Attempts** field, enter the number of times the wireless controller retries sending a request to the policy server if it does not receive a response.

  The valid range is from 0 to 5. A higher value increases reliability but may delay failure detection.

- (Optional) In the **Timeout (seconds)** field, enter the time, in seconds, that the wireless controller waits before considering this attempt as a failed attempt.

  The valid range is from 1 to 60.

- From the **TLS Server Trustpoint** drop-down list, choose a TLS server trustpoint.

- (Optional) If available, use the **Use JSON Content Type** toggle button to enable or disable the usage of JSON as the content type for communication with the policy server.

**Step 6** Under **IP Address**, configure IP address.

| If you want to... | Then... |
|---|---|
| add an IP address | **a.** Click **Add**.<br>**b.** In the **IP Address** field of the **Add IP Address** dialog box, enter a valid IPv4 or IPv6 address. |
| delete IP addresses | **a.** Check the check box for the IP addresses that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure SXP for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure SGT Exchange Protocol (SXP) for Cisco TrustSec (CTS) for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Trustsec**.

**Step 4** (Optional) In the **SXP** tab, complete these configurations.

a) Use the **SXP Status** toggle button to enable or disable the support for CTS SXP.
b) Configure these parameters:

- **Default SXP Source IPv4 Address**: enter a valid default SXP source IPv4 address.
- **Default SXP Password Type**: choose a default SXP password type.
- **Default SXP Password**: enter a default SXP password.

  The password can contain up to 162 characters.
- **Reconciliation Period (sec)**: enter the reconciliation time in seconds.

  The valid range is from 0 to 64000.
- **Retry Period (sec)**: enter the retry period for SXP connection in seconds.

  The valid range is from 0 to 64000.
- **Source Ipv6**: enter a valid source IPv6 address.

**Step 5** Click **Review and Provision**.

**Step 6** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 7** On the **Tasks** window, monitor the task deployment.

### What to do next

If you enable the support for CTS SXP, in the **Peer Connections** table, you can optionally add, edit, or delete the peer connections.

To add a peer connection, click **Add** and complete these configurations.

1. From the **Mode of Local Device** drop-down list, choose a role for the local device.
2. From the **IP Type** drop-down list, choose an IP address type.
3. In the **Peer IP** field, enter an SXP peer IP address based on the selected IP address type.
4. (Optional) In the **Source IP** field, enter an SXP source IP address based on the selected IP address type.
5. From the **Password** drop-down list, choose a type of password.
6. Complete Step 5, on page 199 to Step 7, on page 200.

## Create a CTS link configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a CTS link configuration for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Trustsec**.

**Step 4** In the **CTS Link Configuration** tab, click **Add**.

**Step 5** In the **Create CTS Link Configuration** slide-in pane, complete these configurations:

a) (Optional) From the **Interface Name** drop-down list, choose an interface.
b) Use the **CTS Manual** toggle button to enable or disable the CTS manual mode.

If you enable the CTS manual mod, complete the required configurations.

- In the **Port SGT** field, enter the source Security Group Tag (SGT) number to apply to untagged or nontrusted incoming traffic.

The valid range is from 2 to 65519.

- (Optional) Check the **Trusted** check box to trust the source SGT that the peer uses for sending.
- Use the **Propagate SGT** toggle button to configure CTS SGT propagation configuration.

**Note** If you check the **Trusted** check box, this option is dimmed.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Create an SXP AP profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a CTS SXP AP profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Trustsec**.

**Step 4** Click the **AP** tab.

**Step 5** Click **Add**.

**Step 6** In the **Profile Name** field of the **Create SXP AP Profiles** slide-in pane, enter a unique name for the profile.

The profile name can contain up to 31 characters. Catalyst Center does not support leading and trailing spaces in the profile name.

**Step 7** (Optional) Click the **Status** toggle button to enable the CTS SXP configuration.

**Step 8** Enter data in these fields.

- (Optional) **Default Password**: enter a default password for CTS SXP.

The password can contain up to 80 characters.

- **CTS Listener Minimum (sec)**: enter the minimum CTS SXP listener hold time in seconds.

  The valid range is from 1 to 65534. The default value is 90.

- **CTS Listener Maximum (sec)**: enter the maximum CTS SXP listener hold time in seconds.

  The valid range is from 1 to 65534. The default value is 120.

- **CTS Speaker Seconds (sec)**: enter the CTS SXP speaker hold time in seconds.

  The valid range is from 1 to 65534. The default value is 120.

- **CTS Recon Period (sec)**: enter the CTS SXP reconcile period in seconds.

  The valid range is from 0 to 64000. The default value is 120.

- **CTS Retry Period (sec)**: enter the CTS SXP retry period in seconds.

  The valid range is from 0 to 64000. The default value is 120.

**Step 9** (Optional) Under **CTS SXP Profile Connections**, configure CTS SXP profile connections.

| If you want to... | Then... |
|---|---|
| add a CTS SXP profile connection | **a.** Click **Add**.<br>**b.** In the **Peer IP** field of the **Add CTS SXP Profile Connections** dialog box, enter a peer IP address for the SXP connection.<br>**c.** From the **Connection Mode** drop-down list, choose an SXP connection mode.<br>**d.** From the **Password Type** drop-down list, choose a password type for the SXP connection.<br>**e.** Click **Save**. |
| edit a CTS SXP profile connection | **a.** Check the check box next to the peer IP address that you want to edit.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Edit the required configurations.<br>**d.** Click **Save**. |
| delete CTS SXP profile connections | **a.** Check the check box next to the peer IP addresses that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Configure rogue policies for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure rogue policies to detect rogue APs for a wireless controller and provision them.

The default AP profile and these global rogue parameters are automatically configured for the high, low, or critical rogue detection security levels and you can't edit them:

- **Adhoc Rogue AP**
- **Auto Containment Level**
- **Detect and Report Adhoc Networks**
- **Expiration timeout for Rogue APs (seconds)**
- **Rogue AP Expiration Timeout (sec)**
- **Rogue Auto Contain Ad Hoc**
- **Rogue Init Timer (sec)**
- **Rogue Polling Interval (sec)**
- **Using our SSID**
- **Valid client on Rogue AP**
- **Validate Rogue Clients Against AAA**
- **Validate Rogue APs Against AAA**

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Wireless Protection Policies**.

**Step 4** In the **Rogue Policies** tab, under **General**, complete the required configurations.

a) From the **Rogue Detection Security Level** drop-down list, choose a security level.

If you chose the **Custom** security level, complete these configurations.

- In the **Rogue AP Expiration Timeout (sec)** field, enter the timeout value in seconds for rogue APs.

  The valid range is from 240 to 3600. The default value is 1200.

- Use the **Validate Rogue Clients Against AAA** check box to enable or disable the validation of rogue clients against the AAA server.
- Use the **Validate Rogue APs Against AAA** check box to enable or disable validation of rogue APs against the AAA server.
- In the **Rogue Polling Interval (sec)** field, enter the interval to poll the AAA server for rogue information.

  The valid range is from 60 to 86400. The default value is 3600.

- Check the **Detect and Report Adhoc Networks** check box to enable the detection and reporting of ad hoc rogue APs.
- In the **Rogue Init Timer (sec)** field, enter the init timer in seconds for rogue APs.

  The valid range is from 0 to 360. The default value is 60.

  When a rogue AP is detected, an init timer is started and the rules are applied when this timer expires.

b) In the **Rogue Detection Client Number Threshold** field, enter the threshold for rogue client per rogue AP SNMP trap.

The valid range is from 0 to 256. The default value is 56.

c) Use the **AP Authentication** check box to enable or disable AP authentication.

**Note** AP authentication can't be enabled if global MFP is enabled in Step 6, on page 204.

d) In the **AP Authentication Alarm Threshold** field, enter the threshold for AP authentication alarm.

The valid range is from 1 to 255. The default value is 22.

e) Use the **Syslog Notification** check box to enable or disable the rogue event notifications through syslog.

**Step 5** If you chose the **Custom** security level, under **Auto Contain**, complete these configurations:

- From the **Auto Containment Level** drop-down list, choose a level for automatic containment of rogue APs.
- Use these check boxes to enable or disable the corresponding configurations:
  - **Auto Containment only for Monitor Mode APs**: Configure auto containment for only the APs that are in monitor mode.
  - **Using our SSID**: Configure auto containment of rogue APs that are advertising our SSID.
  - **Valid client on Rogue AP**: Configure auto containment for valid clients that are using rogue APs.
  - **Adhoc Rogue AP**: Configure auto containment for ad hoc rogue APs.

**Step 6** Under **MFP Configuration**, complete these configurations:

- Use the **Global MFP State** check box to enable or disable Management Frame Protection (MFP) globally.

  **Note** Global MFP cannot be enabled if AP authentication is enabled.

- Use the **AP Impersonation Detection** check box to enable or disable AP impersonation detection.
- In the **MFP Key Refresh Interval (hours)** field, enter the MFP key refresh interval in hours.

  The valid range is from 1 to 24.

**Step 7** Under **Rogue Device Authorization**, use the **Rogue Authorization Mode** check box to enable or disable the authorization mode for identifying and managing rogue devices on the network.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create a rogue AP rule for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a rogue AP rule for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Wireless Protection Policies**.

**Step 4** Click the **Rogue AP Rules** tab.

**Step 5** Click **Add**.

**Step 6** In the **Rule Name** field of the **Create Rogue AP Rules** slide-in pane, enter a unique name for the rogue AP rule.

The rule name can contain up to 32 alphanumeric characters and special characters. The rule name must contain at least one alphanumeric character, period (.), underscore (_), or hyphen (-). Catalyst Center does not support ? and spaces in the rule name.

**Step 7** In the **Priority** field, enter a number to indicate the priority of the rogue AP rule.

The valid range is from 1 to 512. A lower number indicates a higher priority.

**Step 8** From the **Type** drop-down list, choose a classification type.

**Step 9** Based on the classification type, complete these configurations.

| If you chose... | Then... |
|---|---|
| **Friendly** or **Malicious** | From the **State** drop-down list, choose a state for the rogue AP rule. |
| **Custom** | • From the **State** drop-down list, choose a state for the rogue AP rule.<br>• In the **Severity Score** field, enter a score for the classification type.<br>The valid range is from 1 to 100.<br>• (Optional) In the **Custom Name** field, enter a custom name for the classification type. |

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

### What to do next

To configure additional parameters for the rule, see Configure a rogue AP rule for a Cisco Catalyst 9800 Series Wireless Controller, on page 206.

## Configure a rogue AP rule for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure additional parameters for a rogue AP rule for a wireless controller and provision it.

### Before you begin

Create rogue AP rules. To create a rogue AP rule, see Create a rogue AP rule for a Cisco Catalyst 9800 Series Wireless Controller, on page 205.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Wireless Protection Policies** > **Rogue AP Rules**.

**Step 4** Check the check box for the rule that you want to configure. Hover your cursor over **Actions** and choose **Edit**.

**Step 5** (Optional) In the **Priority** field of the **Edit Rogue AP Rules** slide-in pane, update the existing priority of the rogue AP rule.

The valid range is 1 to 512. A lower number indicates a higher priority.

**Step 6** Use the **Enable Rule** check box to enable or disable the rule.

**Note** If you enable the rule, you can edit only the **Priority** field. The other options are disabled.

If you disable the rule, complete these configurations:

a) From the **Type** drop-down list, choose a classification type: **Friendly**, **Malicious**, **Delete**, or **Custom**

Based on the classification type, complete these configurations.

| If you chose... | Then... |
|---|---|
| **Friendly** or **Malicious** | From the **State** drop-down list, choose a state for the rogue AP rule. |
| **Custom** | • From the **State** drop-down list, choose a state for the rogue AP rule.<br>• In the **Severity Score** field, enter a score for the classification type. The valid range is 1 to 100.<br>• (Optional) In the **Custom Name** field, enter a custom name for the classification type.<br>The custom name can contain up to 215 alphanumeric and special characters. |

b) From the **Match Operation** drop-down list, choose a criterion for the rogue AP to adopt the classification type of the rule.

- **All**: The detected rogue AP must meet all of the conditions specified in the rule for the rule to be matched.
- **Any**: The detected rogue AP must meet any of the conditions specified in the rule for the rule to be matched.

c) (Optional) Under **Conditions**, check the required check boxes to configure the corresponding conditions to adopt the classification type of the rule:

- **client-count**: This condition requires that a minimum number of clients be associated with the rogue AP.

  If you check this check box, in the **Minimum Number of Rogue Clients** field, enter the minimum number of clients to be associated with the rogue AP. The valid range is 1 to 10. The default value is 0.

  If the number of clients connected exceeds the specified limit, the classification type of the rule is adopted.

- **duration**: This condition requires the rogue AP to be detected for a minimum period of time.

  If you check this check box, in the **Time Duration** field, enter a value for the minimum detection period in seconds. The valid range is 0 to 86400. The default value is 0.

- **encryption**: This condition requires that WLAN uses the specified encryption.

  If you check this check box, you can optionally use the check boxes to choose the corresponding encryption type.

- **infrastructure**: This condition requires that the SSID of the rogue AP must be known to the wireless controller.

  If you check this check box, you can optionally check the **Manage SSID** check box to check if the SSID of the rogue AP matches a managed SSID.

- **rssi**: This condition requires that the rogue AP has a minimum received signal strength indication (RSSI) value.

  If you check this check box, in the **Maximum RSSI** field, enter the maximum RSSI value in dBm. The valid range is 0 to –128.

- **channel-width**: This condition requires that the rogue AP uses the channel width for the specified radio band.

  If you check this check box, choose the required option from these drop-down lists:

  - **Band**: Choose the rogue AP radio band.
  - **Maximum Channel Width**: Choose the maximum channel width for the radio band.

- **ssid**: This condition requires that the rogue AP has a specific user-configured SSID.

  If you check this check box, in the **User Configured SSID** field, enter the SSIDs. You can enter one SSID per line.

- **substring-ssid**: This condition requires that the rogue AP has a substring of the specific user-configured SSID. The wireless controller analyzes the occurrence pattern and identifies a match if the substring is found in the SSID string.

  If you check this check box, in the **User Configured Substring-SSID** field, enter the substring of SSIDs. You can enter one substring of the SSID per line.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure client exclusion policies for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure client exclusion policies for a wireless controller and provision.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **Wireless Protection Policies**.

**Step 4** Click the **Client Exclusion Policies** tab.

**Step 5** (Optional) Check the required check boxes to exclude clients for the corresponding events.

- **Select All Events**: choose all the events for client exclusion.
- **Excessive 802.11 Association Failures**: exclude clients when there are repeated 802.11 association failures.
- **Excessive 802.1X Authentication Failures**: exclude clients when there are repeated 802.1X authentication failures.
- **Excessive 802.11 Authentication Timeout**: exclude clients when there are repeated 802.11 authentication timeouts.
- **IP Theft or IP Reuse**: exclude clients when they reuse an IP address indicating a possible IP theft.
- **Excessive Web Authentication Failures**: exclude clients when there are repeated web authentication failures.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Configure LSC provision parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the parameters for AP Locally Significant Certificate (LSC) provisioning for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **LSC**.

**Step 4** Go to the **LSC Provision** tab and under **Provisioning Configuration**, configure the AP join attempts with LSC:

- From the **Status** drop-down list, choose a status for LSC provisioning.

  When you enable the status, APs can use LSC provisioning. When you disable the status, APs fall back to Manufacturer Installed Certificate (MIC) or Self-Signed Certificate (SSC).

- (Optional) In the **Trustpoint Name** field, enter the trustpoint for the Certificate Authority (CA) server that provides certificates to APs and wireless controller for LSC provisioning.

- (Optional) In the **Number of Join Attempts** field, enter the number of join attempts an AP makes using LSC before falling back to MIC.

  The valid range is from 0 to 255.

- From the **Key Size** drop-down list, choose the size of the keys used for LSC provisioning.

**Step 5** (Optional) Under **Subject Name Parameters**, enter the required parameters that are included in the certificate-signing request sent from APs.

Configure the required country, state, city, department, organization, and email address.

**Step 6** (Optional) Under **LSC Renewal Configuration**, use the **LSC Auto-Renewal** check box, to enable or disable renewal of LSC during AP join.

If you enable LSC renewal during AP join, complete these configurations:

- In the **Due Time (Days)** field, enter the number of days before the LSC expires to initiate renewal.

  The valid range is from 5 to 365.

- (Optional) From the **Renewal Schedule** drop-down list, choose a calendar profile.

  To create a calendar profile, see Create a calendar profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 142.

- Use the **Syslog** toggle button to enable or disable periodic syslog messages for LSC renewal.

- From the **Renewal Mode** drop-down list, choose a renewal mode.

  - **One Shot**: renew certificates for all applicable APs at once.

  - **Staggered**: renew certificates for applicable APs in batches.

If you choose staggered renewal, complete these configurations under **Staggered Renewal Configuration**:



**Note** To configure AP upgrade settings, see Configure AP upgrade settings for a Cisco Catalyst 9800 Series Wireless Controller, on page 349.

- From the **Accounting Action** drop-down list, choose an action to be taken when APs are missing during accounting.
- (Optional) In the **Accounting Percent** field, enter the percentage of APs that must join back during accounting.

  The valid range is from 0 to 100.
- In the **Iteration Expiry (Minutes)** field, enter the time in minutes after which the staggered iteration expires for LSC provisioning on the AP.

  The valid range is from 0 to 255.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create an LSC provisioning entry for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a Locally Significant Certificate (LSC) provisioning entry for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **LSC**.

**Step 4** Click the **LSC Provisioning Entries** tab.

**Step 5** Hover your cursor over **Add** and choose the required option:

- **Add Single AP MAC**: Configure a single MAC address for LSC provisioning entry.
- **Add Multiple AP MACs(Upload CSV)**: Upload a comma-separated value (CSV) file to configure multiple MAC addresses for LSC provisioning entries.

| If you choose... | Then... |
|---|---|
| **Add Single AP MAC** | in the **AP MAC Address** field of the **Create LSC Provisioning Entries** slide-in pane, enter the AP Ethernet MAC address to which the LSC will be provisioned.<br>Enter the MAC address in xxxx.xxxx.xxxx, xx-xx-xx-xx-xx-xx, xxxx-xxxx-xxxx, or xxxx:xxxx:xxxx format. |
| **Add Multiple AP MACs(Upload CSV)** | **a.** Click **sample CSV** to download the sample CSV file.<br>**b.** Enter the MAC addresses to which the LSC will be provisioned in the CSV file.<br>Enter MAC addresses in xxxx.xxxx.xxxx, xx-xx-xx-xx-xx-xx, xxxx-xxxx-xxxx, or xxxx:xxxx:xxxx format.<br>**c.** Either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**.<br>**d.** Click **Upload**.<br>Catalyst Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message is displayed. |

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Create a key chain for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a key chain for a wireless controller running Cisco IOS XE Release 26.1.1 or later and provision it.

Key chains are used to group authentication keys for secure communication protocols such as routing authentication.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **MACsec Key Chain**.

**Step 4** Click **Add**.

**Step 5** In the **Create Key Chain Configuration** slide-in pane, complete these configurations.

a) In the **Key Chain Name** field, enter a unique name for the key chain.

b) Configure key chains.

| If you want to... | Then... |
|---|---|
| add a key chain | **1.** Click **Add**.<br>**2.** In the **Key ID** field of the **Add Key Chain** dialog box, enter a key identifier.<br>For a regular key chain, enter a number from 0 to 2147483674. For a Media Access Control security (MACsec) key chain, enter a hexadecimal number that contains an even number of digits.<br>**3.** (Optional) From the **MACsec Cryptographic Algorithm** drop-down list, choose an algorithm for MACsec.<br>**4.** (Optional) In the **Key String** field, enter the hexadecimal key string for authentication or encryption.<br>For AES 128-bit Cipher-based Message Authentication Code (CMAC), enter a 32-character string in this field. For AES 256-bit CMAC, enter a 64-character string in this field.<br>**5.** (Optional) From the **Key String Encryption Type** drop-down list, choose an encryption method for storing the key string.<br>**6.** Click **Save**. |
| edit a key chain | **1.** Check the check box for the key chain that you want to edit.<br>**2.** Hover your cursor over **Actions** and choose **Edit**.<br>**3.** Edit the required configurations.<br>**4.** Click **Save**. |
| delete a key chain | **1.** Check the check box for the key chain that you want to delete.<br>**2.** Hover your cursor over **Actions** and choose **Delete**.<br>**3.** In the dialog box, click **Yes**. |

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Configure AP certificate policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure AP certificate policy for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AP Certificate Policy**.

**Step 4** Use the **Allow MIC APs** toggle button to enable or disable the usage of Manufacturer Installed Certificates (MIC) for APs to join the wireless controller.

**Step 5** (Optional) From the **Trustpoint Name for MIC APs** drop-down list, select a trustpoint to specify the certificate authority and secure communication for the wireless management interface.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Create an AP certificate policy using MAC address for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AP certificate policy for a wireless controller using MAC address and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AP Certificate Policy**.

**Step 4** Hover your cursor over **MAC/Serial Number** and choose **MAC**.

**Step 5** Hover your cursor over **Add** and choose the required method.

- **Add Single Entry**: Creates AP certificate policy using a single MAC address.
- **Upload CSV**: Creates AP certificate policy using MAC addresses listed in a comma-separated value (CSV) file.

| If you choose... | Then... |
|---|---|
| **Add Single Entry** | In the **AP Ethernet MAC Address** field of the **Create AP Certificate Policy MAC** slide-in pane, enter the Ethernet MAC address of the AP to which this policy applies.<br>Enter the MAC address in the format xxxx.xxxx.xxxx, xx-xx-xx-xx-xx-xx, or xx:xx:xx:xx:xx:xx. |
| **Upload CSV** | In the **Upload CSV** slide-in pane, complete these configurations:<br>**a.** Click **sample CSV** to download the sample CSV file.<br>**b.** Enter the Ethernet MAC addresses of the AP to which this policy applies.<br>Enter the MAC addresses in the format xxxx.xxxx.xxxx, xx-xx-xx-xx-xx-xx, or xx:xx:xx:xx:xx:xx.<br>**c.** Either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**.<br>**d.** Click **Upload**.<br>Catalyst Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message is displayed. |

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Create an AP certificate policy using serial number for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AP certificate policy for a wireless controller using serial number and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Security** and click **AP Certificate Policy**.

**Step 4** Hover your cursor over **MAC/Serial Number** and choose **Serial Number**.

**Step 5** Hover your cursor over **Add** and choose the required method.

- **Add Single Entry**: Creates AP certificate policy using a single serial number.
- **Upload CSV**: Creates AP certificate policy using serial numbers listed in a comma-separated value (CSV) file.

| If you choose... | Then... |
|---|---|
| **Add Single Entry** | In the **Trust Anchor Serial Number** field of the **Create AP Certificate Policy Serial Number** slide-in pane, enter the serial number of the trust anchor certificate associated with the AP.<br>The serial number must contain 11 numeric characters.<br>**Note**<br>Ensure that the serial number matches the serial number issued by the certificate authority. |

| If you choose... | Then... |
|---|---|
| **Upload CSV** | In the **Upload CSV** slide-in pane, complete these configurations:<br>**a.** Click **sample CSV** to download the sample CSV file.<br>**b.** Enter the serial numbers of the trust anchor certificate associated with the AP.<br>The serial number must contain 11 numeric characters.<br>**Note** Ensure that the serial number matches the serial number issued by the certificate authority.<br>**c.** Either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**.<br>**d.** Click **Upload**.<br>Catalyst Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message is displayed. |

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

# Global wireless configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device global wireless configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Configure CleanAir for a Cisco Catalyst 9800 Series Wireless Controller

Cisco CleanAir technology uses silicon-level intelligence to create a spectrum-aware, self-healing, and self-optimizing wireless network that mitigates the impact of wireless interference.

Use this procedure to configure the CleanAir parameters for a wireless controller and provision.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **CleanAir**.

**Step 4** In the **6 GHz** tab, complete these configurations.

a) Use the **Enable CleanAir** toggle button to enable or disable CleanAir on the 6-GHz band.
b) Use the **Report Interferers** check box to enable or disable the reporting of interferers.
c) Under **Trap Configuration**, complete these configurations.

- (Optional) Check the **Enable Air Quality Index (AQI) Trap** check box to enable air quality notification on this band.
- In the **AQI Alarm Threshold** field, enter the threshold value for the AQI trap.

  The valid range is from 1 to 100. The default value is 10.
- Check the **Enable Interference for Security Alarm** check box to enable Interference Device Reports (IDR) notification on this band.

d) Under **Advanced CleanAir Configuration**, complete these configurations:

- Use the **Air Quality Alarm for Unclassified category** toggle button to enable or disable the air quality alarm for the unclassified category.
- (Optional) In the **Air Quality Alarm Threshold for Unclassified category** field, enter the threshold value for air quality alarm for unclassified category.

  The valid range is from 1 to 100.

e) Under **Interference Types to Detect** and **Interference Types to Trap**, check the required check boxes to choose the corresponding interference types.
f) Complete Step 7, on page 219 to Step 10, on page 220 to provision the configuration.

**Step 5** In the **5 GHz** tab, complete these configurations.

a) Use the **Enable CleanAir** toggle button to enable or disable CleanAir on the 5-GHz band.
b) (Optional) Check the **Enable Spectrum Intelligence (SI)** check box to enable spectrum intelligence (SI) on this band.
c) (Optional) Check the **Report Interferers** check box to enable the reporting of interferers.
d) Under **Trap Configuration**, complete these configurations.

- (Optional) Check the **Enable Air Quality Index (AQI) Trap** check box to enable air quality notification on this band.
- In the **AQI Alarm Threshold** field, enter the threshold value for the AQI trap.

The valid range is from 1 to 100. The default value is 10.

- Check the **Enable Interference for Security Alarm** check box to enable IDR notification on this band.

e) Under **Advanced CleanAir Configuration**, complete these configurations:

- Use the **Air Quality Alarm for Unclassified category** toggle button to enable or disable the air quality alarm for the unclassified category.
- (Optional) In the **Air Quality Alarm Threshold for Unclassified category** field, enter the threshold value for air quality alarm for unclassified category.

  The valid range is from 1 to 100.

f) Under **Interference Types to Detect** and **Interference Types to Trap**, check the required check boxes to choose the corresponding interference types.

g) Complete Step 7, on page 219 to Step 10, on page 220 to provision the configuration.

**Step 6** In the **2.4 GHz** tab, complete these configurations.

a) Use the **Enable CleanAir** toggle button to enable or disable CleanAir on the 2.4-GHz band.

b) (Optional) Check the **Enable Spectrum Intelligence (SI)** check box to enable spectrum intelligence (SI) on this band.

c) Check the **Report Interferers** check box to enable the reporting of interferers.

d) Under **Trap Configuration**, complete these configurations.

- Check the **Enable Air Quality Index (AQI) Trap** check box to enable air quality notification on this band.
- In the **AQI Alarm Threshold** field, enter the threshold value for the AQI trap.

  The valid range is from 1 to 100. The default value is 10.

- Check the **Enable Interference for Security Alarm** check box to enable IDR notification on this band.

e) Under **Advanced CleanAir Configuration**, complete these configurations:

- Use the **Air Quality Alarm for Unclassified category** toggle button to enable or disable the air quality alarm for the unclassified category.
- (Optional) In the **Air Quality Alarm Threshold for Unclassified category** field, enter the threshold value for air quality alarm for the unclassified category.

  The valid range is from 1 to 100.

f) Under **Interference Types to Detect** and **Interference Types to Trap**, check the required check boxes to choose the corresponding interference types.

g) Complete Step 7, on page 219 to Step 10, on page 220 to provision the configuration.

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Configure high throughput parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the high throughput parameters for a wireless controller and provision the configuration.

**Important** Configuring high throughput on operational bands results in loss of client connectivity.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **High Throughput**.

**Step 4** In the **6 GHz** tab, configure the high throughput parameters for the 6-GHz band.

a) (Optional) Under **11ax**, complete these configurations:

- Under **SS/MCS**, check the required check boxes to choose the corresponding Spatial Streams (SS) or modulation and coding scheme (MCS) configurations.
- From the **Beamforming Support** drop-down list, choose a status to enable or disable beamforming for the WLAN.

  Beamforming improves signal quality and range by directing signals towards connected clients.
- Use the **HE Dynamic Fragmentation** toggle button to enable or disable dynamic fragmentation for high efficiency (HE) 802.11ax transmissions.

b) (Optional) Under **11be**, complete these configurations.

- Use the **Enable 11be** toggle button to enable or disable the wireless controller to manage the 802.11be networks.
- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.

c) Complete Step 7, on page 222 to Step 10, on page 223 to provision the configuration.

**Step 5** In the **5 GHz** tab, configure the high throughput parameters for the 5-GHz band.

a) (Optional) Under **11n**, complete these configurations.

- Use the **Enable 11n** toggle button to enable or disable the wireless controller to manage the 802.11n networks.
- Use the **Dot11n Short Guard Enabled** toggle button to enable or disable the support for 802.11n guard interval on this band.
- Under **MCS/(Data Rate)**, check the required check boxes to choose the corresponding MCS or data rate configurations.

b) (Optional) Under **11ac**, complete these configurations.

- Use the **Enable 11ac** toggle button to enable or disable the wireless controller to manage the 802.11ac networks.
- Under **SS/MCS/(Data Rate)**, check the required check boxes to choose the corresponding SS or MCS or data rate configurations.

c) (Optional) Under **11ax**, complete these configurations.

- Use the **Enable 11ax** toggle button to enable or disable the wireless controller to manage the 802.11ax networks.
- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.
- From the **Beamforming Support** drop-down list, choose a status to enable or disable beamforming for the WLAN.

  Beamforming improves signal quality and range by directing signals towards connected clients.
- Use the **RIFS Transmission Status** toggle button to enable or disable the usage of Reduced Interframe Spacing (RIFS) for transmissions.
- Use the **HE Dynamic Fragmentation** toggle button to enable or disable dynamic fragmentation for high efficiency (HE) 802.11ax transmissions.

d) (Optional) Under **11be**, complete these configurations.

- Use the **Enable 11be** toggle button to enable or disable the wireless controller to manage the 802.11be networks.
- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.

e) Complete Step 7, on page 222 to Step 10, on page 223 to provision the configuration.

**Step 6** In the **2.4 GHz** tab, configure the high throughput parameters for the 2.4-GHz band.

a) (Optional) Under **11n**, complete these configurations.

- Use the **Enable 11n** toggle button to enable or disable the wireless controller to manage the 802.11n networks.
- Use the **Dot11n Short Guard Enabled** toggle button to enable or disable the support for 802.11n guard interval on this band.
- Under **MCS/(Data Rate)**, check the required check boxes to choose the corresponding MCS or data rate configurations.

b) (Optional) Under **11ax**, complete these configurations.

- Use the **Enable 11ax** toggle button to enable or disable the wireless controller to manage the 802.11ax networks.
- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.
- From the **Beamforming Support** drop-down list, choose a status to enable or disable beamforming for the WLAN.

  Beamforming improves signal quality and range by directing signals towards connected clients.
- Use the **RIFS Transmission Status** toggle button to enable or disable the usage of Reduced Interframe Spacing (RIFS) for transmissions.
- Use the **HE Dynamic Fragmentation** toggle button to enable or disable dynamic fragmentation for high efficiency (HE) 802.11ax transmissions.

c) (Optional) Under **11be**, complete these configurations.

- Use the **Enable 11be** toggle button to enable or disable the wireless controller to manage the 802.11be networks.
- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.

d) Complete Step 7, on page 222 to Step 10, on page 223 to provision the configuration.

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Configure media parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the video and voice media parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Media Parameters**.

**Step 4** Hover your cursor over **6 GHz**, **5 GHz**, or **2.4 GHz**, click **Media**, and configure the required parameters.

a) (Optional) Under **Media**, check the **Unicast Video Redirect** check box to redirect a unicast or multicast only video stream on a best-effort basis.
b) (Optional) Under **Multicast Direct Admission Control**, complete these configurations.
   - Check the **Media Stream Admission Control (ACM)** check box to enable admission control for the video access category.
   - Enter data in these fields.
     - **Maximum Media Streams RF Bandwidth (%)**: enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band.

       The valid range is from 5 to 85. The default value is 5.
     - **Maximum Media Bandwidth (%)**: enter the percentage of the maximum allowed bandwidth for media traffic.

       The valid range is from 5 to 85. The default value is 85.
   - From the **Client Minimum Phy Rate (kbps)** drop-down list, choose a minimum client rate for multicast direct streams.
   - In the **Maximum Retry Percentage (%)** field, enter the maximum retry percentage for multicast direct streams.

The valid range is from 0 to 100. The default value is 80.

c) (Optional) Under **Media Stream - Multicast Direct**, configure the required parameters.

- Check the required check boxes to configure the corresponding settings.
  - **Enable Multicast Direct**: allow multicast direct stream on radio
  - **Best Effort QoS Admission**: admit a media stream in a best-effort queue
- Enter data in these fields.
  - **Maximum Stream Per Radio**: choose the maximum number of allowed media streams per radio.
  - **Maximum Stream Per Client**: choose a maximum number of allowed media streams per client.

d) (Optional) Under **Call Admission Control (CAC) Advanced**, complete these configurations:

- For the 5-GHz band, in **Default 802.11a/n QoS Packet Maximum (bytes)** field, enter the maximum allowed packet size in bytes for QoS on 802.11a/n networks.

  The valid range is from 15000 to 400000000.
- In the **CAC Maximum Concurrent Calls** field, enter the maximum number of simultaneous voice or video calls allowed on the AP or radio band.

  The valid range is from 0 to 4294967295. If you do not want to configure a limit, leave this field blank.

e) Complete Step 6, on page 225 to Step 9, on page 225 to provision the configuration.

**Step 5** Hover your cursor over **6 GHz**, **5 GHz**, or **2.4 GHz**, click **Voice**, and configure the required voice parameters.

a) (Optional) Under **Voice**, check the **Call Admission Control (ACM)** check box to enable admission control on the voice access category.

If you check this check box, complete these configurations.

- Check the **Load-Based CAC** check box to enable load-based Channel Availability Check (CAC).
- Enter data in these fields.
  - **Maximum RF bandwidth (%)**: enter the percentage of maximum bandwidth allocated to the 802.11e clients.

    The valid range is from 5 to 85. The default value is 75.
  - **Reserved Roaming Bandwidth (%)**: enter the percentage of maximum bandwidth allocated to roaming clients for voice traffic.

    The valid range is from 0 to 25. The default value is 6.
- Check the **Expedited Bandwidth** check box to enable the expedited bandwidth request support.
- Under **SIP CAC and Bandwidth**, check the **SIP CAC Support** check box to enable SIP CAC support.

  If you enable SIP CAC support, complete the required configurations.
  - In the **SIP Bandwidth (kbps)** field, enter the bandwidth in kbps for the SIP CAC configuration of the dot11 band for the APs associated with this controller.

    The valid range is from 8 to 64. The default value is 64.

- From the **SIP Voice Sample Interval (ms)** drop-down list, choose a voice sample interval in milliseconds for the SIP CAC configuration of the dot11 band for the APs associated with this controller.

b) (Optional) Under **Traffic Stream Metrics**, complete the required configurations.

- Check the required check boxes to enable the corresponding configurations.
  - **Metrics Collection**: enable the 802.11a traffic stream metrics support.

    When you enable the metrics, the associated APs send the controller statistical data on the traffic on their 802.11a interfaces every 90 seconds.
  - **Inactivity Timeout**: enable the Traffic Specification (TSPEC) inactivity timeout processing mode.
- Enter data in these fields.
  - **Stream Size**: enter the maximum acceptable data rate of the media stream.

    The valid range is from 84000 to 92100.
  - **Maximum Streams**: enter the maximum number of media streams per TSPEC.

    The valid range is from 1 to 5.

c) Complete Step 6, on page 225 to Step 9, on page 225 to provision the configuration.

**Step 6** Click **Review and Provision**.

**Step 7** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

# Configure Air Time Fairness for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the Air Time Fairness (ATF) parameters for a wireless controller.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand c and click **Airtime Fairness**.

**Step 4** Click either the **5 GHz** or **2.4 GHz** tab and complete these configurations.

a) Use the **Status** toggle button to enable or disable ATF on the band.

b) From the **Mode** drop-down list, choose an ATF operating mode.

If you chose the **Enforced** mode, you can optionally check the **Optimization** check box to enable the ATF optimization.

c) Check the **Bridge Client Access** check box to enable the air time allocation mode on the default RF policy.

If you check the **Bridge Client Access** check box, in the **Airtime Allocation** field, you can optionally enter an air time allocation weight percentage.

The valid range is from 5 to 90. The default value is 5.

**Step 5** Click **Review and Provision**.

**Step 6** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Create an Air Time Fairness policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an Air Time Fairness (ATF) policy for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Airtime Fairness**.

**Step 4** Click the **Policy** tab.

**Step 5** Click **Add**.

**Step 6** In the **ATF Policy Name** field of the **Create ATF Policy** slide-in pane, enter a unique name for the ATF policy.

**Step 7** In the **ID** field, enter a unique ID for the ATF policy.

The valid range is from 0 to 511.

**Step 8** In the **Weight** field, enter a policy weight for the ATF policy.

The valid range is from 5 to 100. The default value is 10.

**Step 9** (Optional) Check the **Client Sharing** check box to enable fair client sharing for an ATF policy.

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |

| Option | Description |
|---|---|
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Configure network parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the network parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Network Parameters**.

**Step 4** In the **6 GHz** tab, configure the required parameters for the 6-GHz band.

a) Under **General**, complete these configurations.

- (Optional) Check the **6 GHz Network Status** check box to enable the 6-GHz band.

**Note** When this band is operational, configuring **Beacon Interval (msec)**, **Fragmentation Threshold (bytes)**, or **DTPC Support** results in loss of connectivity for clients.

- Enter data in these fields.

- **Beacon Interval (msec)**: enter the time in milliseconds that an AP radio can use for scheduling beacon transmissions.

  The valid range is from 20 to 1000. The default value is 100.

- **Fragmentation Threshold (bytes)**: enter the size in bytes at which the packets are fragmented.

  The valid range is from 256 to 2346. The default value is 2346.

- (Optional) Check the **DTPC Support** check box to enable Dynamic Transmit Power Control (DTPC) on all 802.11b/g bands.

  When DTPC is enabled, the radios advertise their transmit power levels in beacons and probe responses.

**Note** If you enable DTPC, you can't configure a power constraint value for the 5-GHz band. For more information, see Configure global radio parameters for a Cisco Catalyst 9800 Series Wireless Controller, on page 233.

b) (Optional) Under **CCX Location Measurement**, check the **Mode** check box to enable the support for 802.11 Cisco Client Extensions (CCX) client location measurements.

   If you enable this measurement, in the **Interval** field, enter the 802.11 CCX client location measurement interval.

   The valid range for this interval is from 10 to 32400. The default value is 60.

c) (Optional) Under **A-MPDU Tx** and **A-MSDU Tx**, choose the required priority levels for which you want to enable the Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU) transmission priority.

d) Under **General 802.11 Parameters**, use the **Enable World Mode (IE)** toggle button to enable or disable the inclusion of world mode information element (IE) in beacon frames for APs.

   Enable this option if you network serves clients from different regulatory domains or to ensure compliance with international wireless standards.

e) Complete Step 7, on page 232 to Step 10, on page 233 to provision the configuration.

**Step 5** In the **5 GHz** tab, configure the required parameters for the 5-GHz band.

a) Under **General**, complete these configurations.

- (Optional) Check the **5 GHz Network Status** check box to enable the 5-GHz band.

**Note** When this band is operational, configuring **Beacon Interval (msec)**, **Fragmentation Threshold (bytes)**, **DTPC Support**, or data rates results in loss of connectivity for clients.

- Enter data in these fields.

  - **Beacon Interval (msec)**: enter the time in milliseconds that an AP radio can use for scheduling beacon transmissions.

    The valid range is from 20 to 1000. The default value is 100.

- **Fragmentation Threshold (bytes)**: enter the size in bytes at which the packets are fragmented.

  The valid range is from 256 to 2346. The default value is 2346.

- **RSSI Threshold (dBm)**: enter the minimum RSSI threshold for optimized roaming to occur.

  The valid range is from -127 to 0. The default value is -127.

- (Optional) Check the required check boxes to configure the required settings.
  - **DTPC Support**: enable DTPC on all 802.11b/g bands.

    When DTPC is enabled, the radios advertise their transmit power levels in beacons and probe responses.

**Note** If you enable DTPC, you can't configure a power constraint value for the 5-GHz band. For more information, see Configure global radio parameters for a Cisco Catalyst 9800 Series Wireless Controller, on page 233.

  - **Tri Radio Mode**: enable the tri-radio mode.
  - **RSSI Low Check**: check if the RSSI threshold is enabled before optimized roaming occurs.

b) (Optional) Under **CCX Location Measurement**, check the **Mode** check box to enable the support for 802.11 CCX client location measurements.

If you enable this measurement, in the **Interval** field, enter the 802.11 CCX client location measurement interval.

The valid range for this interval is from 10 to 32400. The default value is 60.

c) Under **Data Rates**, from the data rate drop-down lists, choose the required options for the corresponding data rates.

| Option | Description |
|---|---|
| **Mandatory** | Clients must support this data rate to associate to an AP with the wireless controller. |
| **Supported** | Any associated clients that support this data rate may communicate with the AP using that rate. |
| **Disabled** | Clients specify the data rates used for communication. |

d) (Optional) Under **A-MPDU Tx**, complete these configurations:

- In the **Ampdu Window Size** field, enter the window size for A-MPDU.

  The valid range is from 1 to 255.

- Use the **Aggregation Scheduler** toggle button to enable or disable the 802.11n A-MPDU scheduler.
- From the **Frame Burst** drop-down list, choose the required settings for bursting of 802.11n A-MPDUs.
- In the **Realtime Traffic Timeout** field, enter the A-MPDU transmit aggregation scheduler real-time traffic timeout in milli seconds.

  The valid range is from 1 to 1000.

- Choose the required priority levels for which you want to enable the A-MSDU transmission priority.

e) (Optional) Under **A-MSDU Tx**, choose the required priority levels for which you want to enable the A-MSDU transmission priority.

f) Under **General 802.11 Parameters**, use the **Enable World Mode (IE)** toggle button to enable or disable the inclusion of world mode information element (IE) in beacon frames for APs.

Enable this option if you network serves clients from different regulatory domains or to ensure compliance with international wireless standards.

g) Complete Step 7, on page 232 to Step 10, on page 233 to provision the configuration.

**Step 6** In the **2.4 GHz** tab, configure the required parameters for the 2.4-GHz band.

a) Under **General**, complete these configurations.

- (Optional) Check the **2.4 GHz Network Status** check box to enable the 2.4-GHz band.

**Note** When this band is operational, configuring **802.11g Network Status**, **Beacon Interval (msec)**, **Short Preamble**, **Fragmentation Threshold (bytes)**, **DTPC Support**, or data rates results in loss of connectivity for clients.

- Use the **802.11g Network Status** toggle button to enable or disable 802.11g support on the 802.11b network.
- Enter data in these fields.
  - **Beacon Interval (msec)**: enter the time in milliseconds that an AP radio can use for scheduling beacon transmissions.

    The valid range is from 20 to 1000. The default value is 100.
  - **Fragmentation Threshold (bytes)**: enter the size in bytes at which the packets are fragmented.

    The valid range is from 256 to 2346. The default value is 2346.
  - **RSSI Threshold (dBm)**: enter the minimum RSSI threshold for optimized roaming.

    The valid range is from -127 to 0. The default value is -127.
- Check the required check boxes to configure the corresponding settings.
  - **Short Preamble**: enable transmission of the short version of the radio preamble.
  - **DTPC Support**: enable DTPC on all 802.11b/g bands.

    When DTPC is enabled, the radios advertise their transmit power levels in beacons and probe responses.

**Note** If you enable DTPC, you can't configure a power constraint value for the 5-GHz band. For more information, see Configure global radio parameters for a Cisco Catalyst 9800 Series Wireless Controller, on page 233.

- **RSSI Low Check**: check if the RSSI threshold is enabled before optimized roaming occurs.

b) (Optional) Under **CCX Location Measurement**, check the **Mode** check box to enable the support for 802.11 CCX client location measurements.

If you enable this measurement, in the **Interval** field, enter the 802.11 CCX client location measurement interval.

The valid range for this interval is from 10 to 32400. The default value is 60.

c) Under **Data Rates**, from the data rate drop-down lists, choose the required options for the corresponding data rates.

| Option | Description |
|---|---|
| **Mandatory** | Clients must support this data rate to associate to an AP with the wireless controller. |
| **Supported** | Any associated clients that support this data rate may communicate with the AP using that rate. |
| **Disabled** | Clients specify the data rates used for communication. |

d) (Optional) Under **A-MPDU Tx**, complete these configurations:

- In the **Ampdu Window Size** field, enter the window size for A-MPDU.

  The valid range is from 1 to 255.

- Use the **Aggregation Scheduler** toggle button to enable or disable the 802.11n A-MPDU scheduler.
- In the **Realtime Traffic Timeout** field, enter the A-MPDU transmit aggregation scheduler real-time traffic timeout in milli seconds.

  The valid range is from 1 to 1000.

- Choose the required priority levels for which you want to enable the A-MSDU transmission priority.

e) (Optional) Under **A-MSDU Tx**, choose the required priority levels for which you want to enable the A-MSDU transmission priority.

f) Under **General 802.11 Parameters**, use the **Enable World Mode (IE)** toggle button to enable or disable the inclusion of world mode information element (IE) in beacon frames for APs.

Enable this option if you network serves clients from different regulatory domains or to ensure compliance with international wireless standards.

g) Complete Step 7, on page 232 to Step 10, on page 233 to provision the configuration.

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |

| Option | Description |
|---|---|
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Configure global radio parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global radio parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Global Parameters**.

**Step 4** In the **6 GHz** tab, configure the required parameters for the 6-GHz band.

a) Under **EDCA**, complete these configurations.

**Note** When this band is operational, configuring an Enhanced Distributed Channel Access (EDCA) profile or DFS channel switch announcement mode results in loss of connectivity for clients.

- From the **EDCA Profile** drop-down list, choose an EDCA profile for usage in the EDCA parameter set element.

EDCA parameters provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

- (Optional) Check the **Client Load Based Configuration** check box to enable the client load-based EDCA and reduce collisions by dynamically changing EDCA parameters of clients based on the active client and load.

b) Under **802.11ax**, check the required check boxes to enable the required configurations.

- **Target Wake Up Time**: enable an AP to manage activity in the Wi-Fi network.

  The AP manages activity by

  - minimizing medium contention between Stations (STAs), and
  - reducing the required amount of time that an STA in the power-save mode needs to be awake.

- **Multiple BSSID**: enable 802.11ax the multiple basic service set identifier (BSSID) functionality.
- **Target Wake up time broadcast**: enable broadcasting of 802.11ax target wake-up time.
- **BSS Color**: enable 802.11ax BSS color functionality.

c) Complete Step 7, on page 236 to Step 10, on page 237 to provision the configuration.

**Step 5** In the **5 GHz** tab, configure the required parameters for the 5-GHz band.

a) Under **EDCA**, complete these configurations.

**Note** When this band is operational, configuring the EDCA profile, DFS channel switch announcement mode, or Overlapping BSS Packet Detect (OBSS-PD) results in loss of connectivity for clients.

- From the **EDCA Profile** drop-down list, choose an EDCA profile for usage in the EDCA parameter set element.

  EDCA parameters provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

- (Optional) Check the **Client Load Based Configuration** check box to enable the client load-based EDCA and reduce collisions by dynamically changing EDCA parameters of clients based on the active client and load.

b) Under **802.11ax**, complete these configurations.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Target Wake Up Time**: enable an AP to manage activity in the Wi-Fi network.

    The AP manages activity by

    - minimizing medium contention between Stations (STAs), and
    - reducing the required amount of time that an STA in the power-save mode needs to be awake.

  - **BSS Color**: enable 802.11ax BSS color functionality.
  - **Target Wake up time broadcast**: enable broadcasting of 802.11ax target wake-up time.

- **OBSS PD**: enable OBSS-PD spatial reuse.

- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter the non-Spatial Reuse Group (SRG) OBSS PD maximum threshold in dBm.

  The valid range is from -82 to -62.

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

- Enter data in these fields.

  - **SRG OBSS PD Min Threshold (dBm)**: enter the SRG OBSS-PD minimum threshold in dBm.

    The valid range is from -82 to -62.

  - **SRG OBSS PD Max Threshold (dBm)**: enter the SRG OBSS-PD maximum threshold in dBm.

    The valid range is from -82 to -62.

c) Under **DFS (802.11h)**, complete these configurations.

- Check the **Channel Switch Status** check box to enable the channel switch functionality.
- Check the **Smart DFS** check box to enable Dynamic Frequency Selection (DFS) and avoid interference with the radar signals.
- From the **Channel Switch Announcement Mode** drop-down list, choose a mode.
- In the **Power Constraint** field, enter the power constraint value.

  The valid range is from 0 to 30.

d) Complete Step 7, on page 236 to Step 10, on page 237 to provision the configuration.

**Step 6** In the **2.4 GHz** tab, configure the required parameters for the 2.4-GHz band.

a) Under **EDCA**, complete these configurations.



**Note** When this band is operational, configuring the EDCA profile or OBSS-PD results in loss of connectivity for clients.

- From the **EDCA Profile** drop-down list, choose an EDCA profile for usage in the EDCA parameter set element.

  EDCA parameters provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

- (Optional) Check the **Client Load Based Configuration** check box to enable the client load-based EDCA and reduce collisions by dynamically changing EDCA parameters of clients based on the active client and load.

b) Under **802.11ax**, complete these configurations.

- (Optional) Check the required check boxes to enable the corresponding configurations.

  - **Target Wake Up Time**: enable an AP to manage activity in the Wi-Fi network.

    The AP manages activity by

- minimizing medium contention between Stations (STAs), and
- reducing the required amount of time that an STA in the power-save mode needs to be awake.

- **BSS Color**: enable 802.11ax BSS color functionality.
- **Target Wake up time broadcast**: enable broadcasting of 802.11ax target wake-up time.
- **OBSS PD**: enable OBSS-PD spatial reuse.

- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter the non-SRG OBSS PD maximum threshold in dBm.

  The valid range is from -82 to -62.

- (Optional) Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.
- Enter data in these fields.
  - **SRG OBSS PD Min Threshold (dBm)**: enter the SRG OBSS-PD minimum threshold in dBm.

    The valid range is from -82 to -62.
  - **SRG OBSS PD Max Threshold (dBm)**: enter the SRG OBSS-PD maximum threshold in dBm.

    The valid range is from -82 to -62.

c) Complete Step 7, on page 236 to Step 10, on page 237 to provision the configuration.

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Configure RRM on the 6-GHz band for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the Radio Resource Management (RRM) parameters on the 6-GHz band for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **RRM**.

**Step 4** Hover your cursor over **6 GHz**, choose **General**, and complete these configurations.

a) Under **Profile Threshold for Traps**, complete these configurations.

- In the **Throughput (Bps)** field, enter the 802.11a throughput threshold.

  The valid range is from 1000 to 10000000. The default value is 1000000.

- (Optional) Check the **Automatic CFG** check box to enable the performance profile mode.

b) Under **Noise/Interference/Rogue/CleanAir/SI Monitoring Channels**, from the drop-down lists, choose the required options.

**Note** CleanAir and SI monitoring is performed only when the AP is in monitor mode.

- **Channel List**: choose the channel for monitoring.
- **RRM Neighbor Discover Type**: choose a mode for the Neighbor Discovery Protocol (NDP).

c) Under **Monitor Intervals**, complete these configurations.

- Enter data in these fields.
  - **Neighbor Packet Frequency (sec)**: enter the interval in seconds to specify the frequency of receiving new signal strength, noise, and interference measurements at each AP.

    The valid range is from 60 to 3600. The default value is 180.

  - **Reporting Interval (sec)**: enter the interval in seconds between each measurement report.

    The valid range is from 60 to 3600. The default value is 180.

- **Neighbor Timeout Factor**: enter the neighbor timeout factor to specify the duration after which the neighbor expires if it doesn't receive its neighbor packets.

  The valid range is from 5 to 60. The default value is 20.

- **Monitor Coverage Interval**: enter the interval in seconds to receive the new coverage measurements at each AP.

  The valid range is from 60 to 3600.

- **Monitor Load Interval**: enter the interval in seconds to receive the new load measurements at each AP.

  The valid range is from 60 to 3600.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Channel Monitor Status**: enable the neighbor monitoring mode
  - **Monitor RSSI Normalization**: enable 802.11 neighbor discovery RSSI normalization
  - **Sys Log Load**: enable the logging mode for the load profile
  - **Sys Log Channel**: enable logging mode for the dynamic channel change
  - **Sys Log Performance**: enable logging mode for the performance profile
  - **Sys Log Coverage**: enable logging mode for the coverage profile
  - **Sys Log Foreign**: enable logging mode for the foreign profile

- Use the **Log Noise Events** toggle button to log noise-related events detected by the RRM system.

  Logging noise events helps in monitoring and troubleshooting wireless interference issues.

d) Complete Step 10, on page 241 to Step 13, on page 241 to provision the configuration.

**Step 5** Hover your cursor over **6 GHz**, choose **Coverage**, and complete these configurations.

a) Use the **Enable Coverage Hole Detection** toggle button to enable or disable Coverage Hole Detection (CHD).

b) Enter data in these fields.

- **Data Packet Count**: enter the minimum threshold for the data packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255.

- **Voice Packet Count**: enter the minimum threshold for the voice packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255.

- **Data Packet Percentage**: enter the threshold for the percentage of the data packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100.

- **Voice Packet Percentage**: enter the threshold for the percentage of the voice packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100.

c) Complete Step 10, on page 241 to Step 13, on page 241 to provision the configuration.

**Step 6** Hover your cursor over **6 GHz**, choose **DCA**, and complete these configurations.

a) From the **Channel Assignment Mode** drop-down list, choose a mode.

If you chose **Automatic**, choose the required options from the corresponding drop-down lists.

- **Interval**: choose a DCA interval.
- **Anchortime**: choose an anchor time for DCA.

b) From the **DCA Channel Sensitivity** drop-down list, choose a DCA sensitivity level.

c) From the **Dynamic Bandwidth Selection Max Channel Width** drop-down list, choose the maximum best channel width for DBS.

d) (Optional) Check the **Notification Channel Enable** check box to enable the channel change notification mode.

e) (Optional) Check the **DCA Aggr Startup** check box to enable the aggressive DCA algorithm.

f) In the **DCA Update Interval Sec** field, enter the interval in seconds to specify how often the channel assignment updates are attempted on the AP.

The valid range is from 0 to 4294967295.

g) From the **Optimized Roaming Data Rate Threshold (mbps)** drop-down list, choose a data rate threshold for 802.11 optimized roaming.

h) Use the **Include Interference in DCA** toggle button to configure the DCA algorithm to consider detected interference when selecting channels for APs.

This option allows optimization of channel assignments and reduction of co-channel interference.

i) (Optional) In the **Notification Channel Threshold** field, enter the threshold value for triggering channel change notifications.

The valid range is from 1 to 1000.

j) (Optional) Under **Event Driven RRM**, check the **Enable Event Driven RRM** check box to enable event-driven RRM on this band.

If you check this check box, complete these configurations.

- From the **Sensitivity Threshold** drop-down list, choose a threshold level for the event-driven RRM.

  If you chose **Custom**, in the **Custom Threshold** field, enter a custom threshold value for event-driven RRM.

  The valid range is from 1 to 99.

- (Optional) Check the **Rogue contribution** check box to enable event-driven RRM rogue contribution on this band.

  If you check this check box, in the **Rogue Duty-Cycle** field, enter the duty cycle threshold value for event-driven RRM rogue contribution.

  The valid range is from 1 to 99. The default value is 80.

k) Complete Step 10, on page 241 to Step 13, on page 241 to provision the configuration.

**Step 7** Hover your cursor over **6 GHz**, choose **TPC**, and complete these configurations.

a) From the **Power Assignment Method** drop-down list, choose a power assignment method.

If you chose **Fixed**, from the **Default Tx Power Level** drop-down list, choose the power level used to transmit data.

b) (Optional) Check the **TPC Channel Aware** check box to indicate that the Transmit Power Control (TPC) algorithm is channel aware.

c) Enter data in these fields.

- **Notification Max Tx Power Threshold**: enter the maximum threshold that the TPC algorithm assigns to each radio.

  The valid range is from 3 to 30.

- **Notification Min Tx Power Threshold**: enter the maximum threshold that the TPC algorithm assigns to each radio.

  The valid range is from 3 to 30.

d) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Sys Log Tx Power**: enable logging mode for transmission power change
- **Notification Tx Power Enable**: enable transmission power change notification mode

e) Complete Step 10, on page 241 to Step 13, on page 241 to provision the configuration.

**Step 8** Hover your cursor over **6 GHz**, choose **RF Grouping**, and complete these configurations.

a) From the **Grouping Mode** drop-down list, choose an RF grouping mode.

b) If you chose the **Leader** grouping mode, under **Static Members**, complete these configurations:

| If you want to... | Then... |
|---|---|
| add a static member | 1. Click **Add**.<br>2. In the **IPv4/IPv6 Address** field, enter a valid IPv4 address or IPv6 address.<br>3. In the **Controller Name** field, enter the name of the static member.<br>4. Click **Save**. |
| delete static members | 1. Check the check box for the static member that you want to delete.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

c) (Optional) In the **RRM Group Update Interval (seconds)** field, enter the interval, in seconds, at which RRM group information is updated

Based on this interval, the wireless controller recalculates and applies RRM settings across AP groups. Short intervals provide quick adaption but may increase the system overhead.

d) Complete Step 10, on page 241 to Step 13, on page 241 to provision the configuration.

**Step 9** Hover your cursor over **6 GHz**, choose **Spatial Reuse**, and complete these configurations.

a) From the **BSS Color Assignment Mode** drop-down list, choose a BSS color optimization (BCO) mode.

- **Off**: BSS color is not selected dynamically and must be configured manually.
- **Automatic**: BSS color is periodically updated for all APs that permit this operation.

**Note** For this mode, the DCA channel assignment mode must be automatic in Step 6, on page 238.

b) Complete Step 10, on page 241 to Step 13, on page 241 to provision the configuration.

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Configure RRM on the 5-GHz band for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the RRM parameters on the 5-GHz band for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **RRM**.

**Step 4** Hover your cursor over **5 GHz**, choose **General**, and complete these configurations.

a) Under **Profile Threshold for Traps**, complete these configurations.

- Enter data in these fields.
  - **Interference Percentage**: enter the interference threshold in percentage.

    The valid range is from 0 to 100. The default value is 10.

    When the interference exceeds this value, traps are generated.
  - **Clients**: enter the threshold number of clients per AP radio to trigger a trap.

    The valid range is from 1 to 200. The default value is 12.
  - **Noise**: enter the noise threshold value.

    The valid range is from -127 to 0. The default value is -70.
  - **Utilization Percentage**, enter the threshold for the bandwidth used by an AP in percentage.

    The valid range is from 0 to 100. The default value is 80.
  - **Throughput (Bps)**: enter the 802.11a throughput threshold.

    The valid range is from 1000 to 10000000. The default value is 1000000.
- (Optional) Check the **Automatic CFG** check box to enable the performance profile mode.

b) Under **Noise/Interference/Rogue/CleanAir/SI Monitoring Channels**, from the drop-down lists, choose the required options.

- **Channel List**: choose a channel option.
- **RRM Neighbor Discover Type**: choose a mode for the NDP.
- **RRM Neighbor Discover Mode**: choose an operating mode for the NDP.

c) Under **Monitor Intervals**, complete these configurations.

- Enter data in these fields.
  - **Neighbor Packet Frequency (sec)**: enter the interval in seconds to specify the frequency of receiving new signal strength, noise, and interference measurements at each AP.

    The valid range is from 60 to 3600. The default value is 180.
  - **Reporting Interval (sec)**: enter the interval in seconds between each measurement report.

    The valid range is from 60 to 3600. The default value is 180.
  - **Neighbor Timeout Factor**: enter the neighbor timeout factor to specify the duration after which the neighbor expires if it doesn't receive its neighbor packets.

    The valid range is from 5 to 60. The default value is 20.

- **Monitor Coverage Interval**: enter the interval in seconds to receive the new coverage measurements at each AP.

  The valid range is from 60 to 3600.

- **Monitor Load Interval**: enter the interval in seconds to receive the new load measurements at each AP.

  The valid range is from 60 to 3600.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Channel Monitor Status**: enable the neighbor monitoring mode.
  - **Monitor RSSI Normalization**: enable 802.11 neighbor discovery RSSI normalization.
  - **Sys Log Load**: enable the logging mode for the load profile.
  - **Sys Log Channel**: enable logging mode for the dynamic channel change.
  - **Sys Log Performance**: enable logging mode for the performance profile.
  - **Sys Log Coverage**: enable logging mode for the coverage profile.
  - **Sys Log Foreign**: enable logging mode for the foreign profile.

- Use the **Log Noise Events** toggle button to log noise-related events detected by the RRM system.

  Logging noise events helps in monitoring and troubleshooting wireless interference issues.

d) Under **UNII-3**, use the **Unii3 Lp Channels** check box to enable or disable UNII-3 low power channels for the 5-GHz band.
e) Complete Step 10, on page 247 to Step 13, on page 247 to provision the configuration.

**Step 5** Hover your cursor over **5 GHz**, choose **Coverage**, and complete these configurations.

a) Use the **Enable Coverage Hole Detection** toggle button to enable or disable Coverage Hole Detection (CHD).
b) Enter data in these fields.

- **Data RSSI Threshold**: enter the RSSI threshold for the data packets to trigger the CHD algorithm on the wireless controller.

  The valid range is from -90 to -60. The default value is -80.

- **Voice RSSI Threshold**: enter the RSSI threshold for the voice packets to trigger the CHD algorithm on the wireless controller.

  The valid range is from -90 to -60. The default value is -80.

- **Minimum Failed Client per AP**: enter the minimum number of clients to trigger the CHD algorithm.

  The valid range is from 1 to 200. The default value is 3.

- **Percent Coverage Exception Level per AP**: enter the minimum percentage of clients in the coverage hole region of the AP to trigger a coverage hole exception.

  The valid range is from 1 to 100. The default value is 25.

- **Data Packet Count**: enter the minimum threshold for the data packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255. The default value is 50.

- **Voice Packet Count**: enter the minimum threshold for the voice packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255. The default value is 100.

- **Data Packet Percentage**: enter the threshold for the percentage of the data packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100. The default value is 50.

- **Voice Packet Percentage**: enter the threshold for the percentage of the voice packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100. The default value is 50.

c) Complete Step 10, on page 247 to Step 13, on page 247 to provision the configuration.

**Step 6** Hover your cursor over **5 GHz**, choose **DCA**, and complete these configurations.

a) Under **Dynamic Channel Assignment Algorithm**, complete these configurations.

- From these drop-down lists, choose the required options.
  - **Channel Assignment Mode**: choose a mode.

    If you chose **Automatic**, from the drop-down lists, choose the required options.
    - **Interval**: choose a DCA interval.
    - **Anchortime**: choose an anchor time for DCA.

  - **DCA Channel Sensitivity**: choose a DCA sensitivity level.
  - **Channel Width**: choose a channel width.
  - **Dynamic Bandwidth Selection Max Channel Width**: choose the maximum best channel width for DBS.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Avoid Foreign AP Interference**: enable the interference detection on the wireless controller
  - **Avoid Persistent Non-Wi-Fi Interference**: enable device detection on the wireless controller.
  - **Avoid Cisco AP load**: enable load detection on the wireless controller.
  - **Zero Wait DFS**: enable the Zero Wait DFS feature.
  - **Avoid Non 5 GHz Noise**: enable the noise detection on the wireless controller.
  - **Notification Channel Enable**: enable the channel change notification mode.
  - **DCA Aggr Startup**: enable the aggressive DCA algorithm.

- In the **DCA Min Metric RSSI** field, enter the minimum RSSI energy metric required for DCA to change the channel.

  The valid range is from -100 to -60.

- (Optional) In the **DCA Update Interval Sec** field, enter the interval in seconds to specify how often the channel assignment updates are attempted on the AP.

  The valid range is from 0 to 4294967295.

- From the **Optimized Roaming Data Rate Threshold (mbps)** drop-down list, choose a data rate threshold for 802.11 optimized roaming.

b) Use the **Include Interference in DCA** toggle button to configure the DCA algorithm to consider detected interference when selecting channels for APs.

This option allows optimization of channel assignments and reduction of co-channel interference.

c) (Optional) In the **Notification Channel Threshold** field, enter the threshold value for triggering channel change notifications.

The valid range is from 1 to 1000.

d) (Optional) Under **Auto-RF Channel List**, check the required check boxes to choose the corresponding RF channels.

e) (Optional) Under **Event Driven RRM**, check the **Enable Event Driven RRM** check box to enable event-driven RRM on the band.

If you enable event-driven RRM, complete these configurations.

- From the **Sensitivity Threshold** drop-down list, choose a sensitivity level for the event-driven RRM.

  If you chose the **Custom** sensitivity threshold, in the **Custom Threshold** field, enter the event-driven RRM custom threshold value.

  The valid range is from 1 to 99. The default value is 1.

- (Optional) Check the **Rogue contribution** check box to enable rogue contribution on the band.

  If you enable rogue contribution, in the **Rogue Duty-Cycle** field, enter the rogue contribution duty cycle threshold.

  The valid range is from 1 to 99. The default value is 80.

f) Complete Step 10, on page 247 to Step 13, on page 247 to provision the configuration.

**Step 7** Hover your cursor over **5 GHz**, choose **TPC**, and complete these configurations.

a) From the **Power Assignment Method** drop-down list, choose a power assignment method.

If you chose **Fixed**, from the **Default Tx Power Level** field, choose a power level used to transmit data.

b) Enter data in these fields.

- **Maximum Power Level Assignment (dBm)**: enter the upper limit of the transmit power in dBm.

  The valid range is from -10 to 30. The default value is 30.

- **Minimum Power Level Assignment (dBm)**: enter the lower limit of the transmit power in dBm.

  The valid range is from -10 to 30. The default value is -10.

- **Power Control Threshold (dBm)**: enter the TPC threshold for the RRM algorithm.

  The valid range is from -80 to -50. The default value is -70.

c) (Optional) Check the **TPC Channel Aware** check box to indicate that the TPC algorithm is channel aware.

d) Enter data in these fields.

- **Notification Max Tx Power Threshold**: enter the maximum threshold that the TPC algorithm assigns to each radio.

  The valid range is from 3 to 30.

- **Notification Min Tx Power Threshold**: enter the minimum threshold that the TPC algorithm assigns to each radio.

  The valid range is from 3 to 30.

e) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Sys Log Tx Power**: enable logging mode for transmission power change.
- **Notification Tx Power Enable**: enable transmission power change notification mode.

f) Complete Step 10, on page 247 to Step 13, on page 247 to provision the configuration.

**Step 8** Hover your cursor over **5 GHz**, choose **RF Grouping**, and complete these configurations.

a) From the **Grouping Mode** drop-down list, choose an RF grouping mode.

b) If you chose the **Leader** grouping mode, under **Static Members**, complete these configurations:

| If you want to... | Then... |
|---|---|
| add a static member | 1. Click **Add**.<br>2. In the **IPv4/IPv6 Address** field, enter a valid IPv4 address or IPv6 address.<br>3. In the **Controller Name** field, enter the name of the static member.<br>4. Click **Save**. |
| delete static members | 1. Check the check box for the static member that you want to delete.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

c) (Optional) In the **RRM Group Update Interval (seconds)** field, enter the interval, in seconds, at which RRM group information is updated

Based on this interval, the wireless controller recalculates and applies RRM settings across AP groups. Short intervals provide quick adaption but may increase the system overhead.

d) Complete Step 10, on page 247 to Step 13, on page 247 to provision the configuration.

**Step 9** Hover your cursor over **5 GHz**, choose **Spatial Reuse**, and complete these configurations.

a) From the **BSS Color Assignment Mode** drop-down list, choose a BSS color optimization mode.

- **Off**: BSS color is not selected dynamically and must be configured manually.
- **Automatic**: BSS color is periodically updated for all APs that permit this operation.

**Note** For this mode, the DCA channel assignment mode must be automatic in Step 6, on page 244.

b) Complete Step 10, on page 247 to Step 13, on page 247 to provision the configuration.

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Configure RRM on the 2.4-GHz band for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the RRM parameters on the 2.4-GHz band for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **RRM**.

**Step 4** Hover your cursor over **2.4 GHz**, choose **General**, and complete these configurations.

a) Under **Profile Threshold for Traps**, complete these configurations.

- Enter data in these fields.
  - **Interference Percentage**: enter the interference threshold in percentage.

    The valid range is from 0 to 100. The default value is 10.

    When the interference exceeds this value, traps are generated.
  - **Clients**: enter the threshold number of clients per AP radio to trigger a trap.

    The valid range is from 1 to 200. The default value is 12.
  - **Noise**: enter the noise threshold value.

    The valid range is from -127 to 0. The default value is -70.
  - **Utilization Percentage**: enter the threshold for the bandwidth used by an AP in percentage.

    The valid range is from 0 to 100. The default value is 80.
  - **Throughput (Bps)**: enter the 802.11a throughput threshold.

    The valid range is from 1000 to 10000000. The default value is 1000000.
- (Optional) Check the **Automatic CFG** check box to enable the performance profile mode.

b) Under **Noise/Interference/Rogue/CleanAir/SI Monitoring Channels**, complete these configurations.
- From the **Channel List** drop-down list, choose a channel option.
- From the **RRM Neighbor Discover Type** drop-down list, choose a mode for the NDP.
- From the **RRM Neighbor Discover Mode** drop-down list, choose an operating mode for the NDP.

c) Under **Monitor Intervals**, complete these configurations.
- Enter data in these fields.
  - **Neighbor Packet Frequency (sec)**: enter the interval in seconds to specify the frequency of receiving new signal strength, noise, and interference measurements at each AP.

    The valid range is from 60 to 3600. The default value is 180.
  - **Reporting Interval (sec)**: enter the interval in seconds between each measurement report.

    The valid range is from 60 to 3600. The default value is 180.
  - **Neighbor Timeout Factor**: enter the neighbor timeout factor to specify the duration after which the neighbor expires if it doesn't receive its neighbor packets.

    The valid range is from 5 to 60. The default value is 20.
  - **Monitor Coverage Interval**: enter the interval in seconds to receive the new coverage measurements at each AP.

    The valid range is from 60 to 3600.
  - **Monitor Load Interval**: enter the interval in seconds to receive the new load measurements at each AP.

    The valid range is from 60 to 3600. The default value is 360.
- (Optional) Check the required check boxes to enable the corresponding configurations.

- **Channel Monitor Status**: enable the neighbor monitoring mode.
- **Monitor RSSI Normalization**: enable 802.11 neighbor discovery RSSI normalization.
- **Sys Log Load**: enable the logging mode for the load profile.
- **Sys Log Channel**: enable logging mode for the dynamic channel change.
- **Sys Log Performance**: enable logging mode for the performance profile.
- **Sys Log Coverage**: enable logging mode for the coverage profile.
- **Sys Log Foreign**: enable logging mode for the foreign profile.

- Use the **Log Noise Events** toggle button to log noise-related events detected by the RRM system.

  Logging noise events helps in monitoring and troubleshooting wireless interference issues.

d) Complete Step 10, on page 252 to Step 13, on page 253 to provision the configuration.

**Step 5** Hover your cursor over **2.4 GHz**, choose **Coverage** and complete these configurations.

a) Use the **Enable Coverage Hole Detection** toggle button to enable or disable Coverage Hole Detection (CHD).

b) Enter data in these fields.

- **Data RSSI Threshold**: enter the RSSI threshold for the data packets to trigger the CHD algorithm on the wireless controller.

  The valid range is from -90 to -60. The default value is -80.

- **Voice RSSI Threshold**: enter the RSSI threshold for the voice packets to trigger the CHD algorithm on the wireless controller.

  The valid range is from -90 to -60. The default value is -80.

- **Minimum Failed Client per AP**: enter the minimum number of clients to trigger the CHD algorithm.

  The valid range is from 1 to 200. The default value is 3.

- **Percent Coverage Exception Level per AP**: enter the minimum percentage of clients in the coverage hole region of the AP to trigger a coverage hole exception.

  The valid range is from 1 to 100. The default value is 25.

- **Data Packet Count**: enter the minimum threshold for the data packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255. The default value is 50.

- **Voice Packet Count**: enter the minimum threshold for the voice packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255. The default value is 100.

- **Data Packet Percentage**: enter the threshold for the percentage of the data packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100. The default value is 50.

- **Voice Packet Percentage**: enter the threshold for the percentage of the voice packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100. The default value is 50.

c) Complete Step 10, on page 252 to Step 13, on page 253 to provision the configuration.

**Step 6** Hover your cursor over **2.4 GHz**, choose **DCA**, and complete these configurations.

a) Under **Dynamic Channel Assignment Algorithm**, complete these configurations.

- From the drop-down lists, choose the required options.
  - **Channel Assignment Mode**: choose a mode.

    If you chose **Automatic**, from the drop-down lists, choose the required options.
    - **Interval**: choose a DCA interval.
    - **Anchortime**: choose an anchor time for DCA.
  - **DCA Channel Sensitivity**: choose a DCA sensitivity level.
  - **Dynamic Bandwidth Selection Max Channel Width**: choose the maximum best channel width for DBS.
- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Avoid Foreign AP Interference**: enable the interference detection on the wireless controller.
  - **Avoid Persistent Non-Wi-Fi Interference**: enable device detection on the wireless controller.
  - **Avoid Cisco AP load**: enable load detection on the wireless controller.
  - **Avoid Non 5 GHz Noise**: enable the noise detection on the wireless controller.
  - **Notification Channel Enable**: enable the channel change notification mode.
  - **DCA Aggr Startup**: enable the aggressive DCA algorithm.
- In the **DCA Min Metric RSSI** field, enter the minimum RSSI energy metric required for DCA to change the channel.

  The valid range is from -100 to -60.
- (Optional) In the **DCA Update Interval Sec** field, enter the interval in seconds to specify how often the channel assignment updates are attempted on the AP.

  The valid range is from 0 to 4294967295.
- From the **Optimized Roaming Data Rate Threshold (mbps)** drop-down list, choose a data rate threshold for 802.11 optimized roaming.

b) Use the **Include Interference in DCA** toggle button to configure the DCA algorithm to consider detected interference when selecting channels for APs.

This option allows optimization of channel assignments and reduction of co-channel interference.

c) (Optional) In the **Notification Channel Threshold** field, enter the threshold value for triggering channel change notifications.

The valid range is from 1 to 1000.

d) (Optional) Under **Auto-RF Channel List**, check the required check boxes to choose the corresponding RF channels.

e) Under **Event Driven RRM**, check the **Enable Event Driven RRM** check box to enable event-driven RRM on the band.

If you enable event-driven RRM, complete these configurations.

- From the **Sensitivity Threshold** drop-down list, choose a sensitivity level for the event-driven RRM.

  If you chose the **Custom** sensitivity threshold, in the **Custom Threshold** field, enter the event-driven RRM custom threshold value.

  The valid range is from 1 to 99. The default value is 1.

- (Optional) Check the **Rogue contribution** check box to enable rogue contribution on the band.

  If you enable rogue contribution, in the **Rogue Duty-Cycle** field, enter the rogue contribution duty cycle threshold.

  The valid range is from 1 to 99. The default value is 80.

f) Complete Step 10, on page 252 to Step 13, on page 253 to provision the configuration.

**Step 7** Hover your cursor over **2.4 GHz**, choose **TPC**, and complete these configurations.

a) From the **Power Assignment Method** drop-down list, choose a power assignment method.

If you chose **Fixed**, from the **Default Tx Power Level** drop-down list, choose a power level to transmit data.

b) Enter data in these fields.

- **Maximum Power Level Assignment (dBm)**: enter the upper limit of the transmit power in dBm.

  The valid range is from -10 to 30. The default value is 30.

- **Minimum Power Level Assignment (dBm)**: enter the lower limit of the transmit power in dBm.

  The valid range is from -10 to 30. The default value is -10.

- **Power Control Threshold (dBm)**: enter the TPC threshold for the RRM algorithm.

  The valid range is from -80 to -50. The default value is -70.

c) (Optional) Check the **TPC Channel Aware** check box to indicate that the TPC algorithm is channel aware.

d) In the **Notification Max Tx Power Threshold** field, enter the maximum threshold that the TPC algorithm assigns to each radio.

The valid range is from 3 to 30.

e) In the **Notification Min Tx Power Threshold** field, enter the maximum threshold that the TPC algorithm assigns to each radio.

The valid range is from 3 to 30.

f) (Optional) Check the **Sys Log Tx Power** check box to enable logging mode for transmission power change.

g) (Optional) Check the **Notification Tx Power Enable** check box to enable transmission power change notification mode.

h) Complete Step 10, on page 252 to Step 13, on page 253 to provision the configuration.

**Step 8** Hover your cursor over **2.4 GHz**, choose **RF Grouping**, and complete these configurations.

a) From the **Grouping Mode** drop-down list, choose an RF grouping mode.

b) If you chose the **Leader** grouping mode, under **Static Members**, complete these configurations:

| If you want to... | Then... |
|---|---|
| add a static member | 1. Click **Add**.<br>2. In the **IPv4/IPv6 Address** field, enter a valid IPv4 address or IPv6 address.<br>3. In the **Controller Name** field, enter the name of the static member.<br>4. Click **Save**. |
| delete static members | 1. Check the check box for the static member that you want to delete.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

c) (Optional) In the **RRM Group Update Interval (seconds)** field, enter the interval, in seconds, at which RRM group information is updated

Based on this interval, the wireless controller recalculates and applies RRM settings across AP groups. Short intervals provide quick adaption but may increase the system overhead.

d) Complete Step 10, on page 252 to Step 13, on page 253 to provision the configuration.

**Step 9** Hover your cursor over **2.4 GHz**, choose **Spatial Reuse** and complete these configurations.

a) From the **BSS Color Assignment Mode** drop-down list, choose a BSS color optimization mode.

- **Off**: BSS color is not selected dynamically and must be configured manually.
- **Automatic**: BSS color is periodically updated for all APs that permit this operation.

**Note** For this mode, the DCA channel assignment mode must be automatic in Step 6, on page 250.

b) Complete Step 10, on page 252 to Step 13, on page 253 to provision the configuration.

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |

| Option | Description |
|---|---|
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Configure RRM FRA parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the RRM FRA parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **RRM**.

**Step 4** Click the **FRA** tab.

**Step 5** Under **5/6 GHz Flexible Radio Assignment**, complete these configurations.

a) Use the **FRA Status** toggle button to enable or disable Flexible Radio Assignment (FRA) on all APs for 5/6-GHz dual-band (XOR) models.
b) (Optional) Check the **FRA Freeze** check box to enable FRA freeze on all APs for the 5/6-GHz dual-band (XOR) models.
c) From the **FRA Interval** drop-down list, choose an FRA interval for the 5/6-GHz dual-band (XOR) models.

**Step 6** Under **2.4/5 GHz Flexible Radio Assignment**, complete these configurations.

a) Use the **FRA Status** toggle button to enable or disable FRA on all APs.
b) (Optional) Check the **FRA Freeze** check box to enable FRA freeze on all APs.
c) From the **FRA Interval** drop-down list, choose an FRA interval.
d) From the **FRA Sensitivity** drop-down list, choose an FRA coverage overlap sensitivity.
e) (Optional) Check the **Client Aware** check box to allow the dual-band to operate in 5-GHz or monitor mode based on the load on the 5-GHz band.
f) From the **FRA Action** drop-down list, choose an FRA action for the dual-band radio.

g) In the **Client Select Threshold** field, enter the FRA utilization threshold value for moving the dual-band radio from the monitor mode to the client-serving mode.

The valid range is from 0 to 100.

**Note** The client select threshold value must be greater than the client reset threshold value.

h) In the **Client Reset Threshold** field, enter the FRA utilization threshold value for moving the dual-band radio from the client-serving mode to the monitor mode.

The valid range is from 0 to 100.

**Note** The client reset threshold value must be less than the client select threshold value.

i) From the **FRA Sensor Threshold** drop-down list, choose an FRA sensor threshold value.

j) From the **FRA Service Priority** drop-down list, choose an FRA service priority.

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

# Configure global wireless parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global wireless parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

**Step 4** In the **Global** tab, enter data in these fields.

- **Secure Network Name Encryption Type**: choose an encryption type to store or transmit the secure network name.

  **Note** For the clear-text encryption type, the secure network name can contain up to 19 characters. For the AES encryption type, the secure network name must contain 12 to 64 characters.

- **Secure Network Name**: click the edit icon and enter a unique name for the secure network that is used for AP authentication or encryption.

  The name can contain up to 64 characters.

- **Maximum Login Sessions Per User**: enter the maximum number of concurrent logins that are allowed for a single user.

  The valid range is from 0 to 8.

**Step 5** Check the required check boxes to enable the corresponding configurations.

- **Wireless Password Policy**: enable wireless password policy for AP join profile (management user password) and flex profile (local auth user password).
- **Management via Wireless**: enable management access from wireless clients
- **AP Lag Mode**: enable the global lag
- **Dot15 Radio**: enable the global 802.15 radio switch
- **Device Classifier**: enable classification of attached devices.

**Step 6** Under **Assisted Roaming**, enter data in these fields.

- **Denial Maximum**: enter the maximum number times for association denial.

  The valid range is from 1 to 10.

- **Floor Bias (dBm)**: enter the RSSI bias default value in dBm for APs that are on the same floor.

  The valid range is from 5 to 25.

- **Prediction Minimum**: enter the minimum number of optimized APs for the assisted roaming prediction to work.

  The valid range is from 2 to 6.

- **RSSI Threshold for XOR to Dedicated Mode**: enter the minimum RSSI value in dBm at which an AP switches from dual-band (XOR) mode to dedicated mode.

  The valid range is from -128 to 0. Lower values make the AP mode transition less sensitive to weak signals.

**Step 7** (Optional) Under **AP Image Upgrade**, complete these configurations:

- Use the **HTTPS Method** toggle button to enable or disable HTTPS.
- In the **HTTPS Port** field, enter the custom port number for HTTPS file transfer.

  The valid range is from 0 to 65535.

**Step 8** (Optional) Under **AP Geolocation**, use the **Geolocation Derivation Using Ranging** toggle button to enable or disable geolocation derivation using ranging to improve AP location accuracy.

**Step 9** (Optional) Under **Client Events & Logging**, use these toggle buttons to enable or disable the corresponding configurations:

- **Enable Client Onboarding Event**: enables or disables the generation of events when a new client device joins the wireless network.
- **Enable Detailed Client Syslog**: enables or disables detailed syslog messages for client events.

**Step 10** (Optional) Under **Probe Request Management**, complete these configurations:

- **Probe Request Limit**: enter the maximum number of probe requests allowed from a client before taking action.

  The valid range is from 1 to 100.

- **Probe Request Interval (ms)**: enter the minimum interval in milliseconds between probe requests from the same client.

  The valid range is from 100 to 64000.

- **Enable Probe Request Filtering**: enables or disables filtering of probe requests from clients.

  When you enable filtering, wireless controller filters unnecessary probe requests to improve performance and reduce interference.

**Step 11** (Optional) Under **Web Authentication**, in the **Web Authentication Max Retries** field, enter the maximum number of times a client can retry web authentication after a failure.

The valid range is from 0 to 20.

**Step 12** (Optional) Under **XOR Roaming & Load Balancing**, complete the required configurations:

- **Dedicated to XOR RSSI Threshold (dBm)**: enter the RSSI threshold in dBm for dedicated dual-ban (XOR) operations.

  The valid range is from -128 to 0.

- **Minimum Clients for XOR Roaming**: enter the minimum number of clients required before XOR roaming features are activated.

  The valid range is from 0 to 200.

- **Load Balancing Window**: enter the time in seconds used for load balancing calculations.

  The valid range is from 0 to 200.

- **XOR Roam Probe Suppression Mode**: choose the operational mode for probe suppression during XOR roaming.

- **Probe Suppression Aggressiveness**: enter a number to indicate the aggressiveness level for probe suppression during XOR roaming.

  The valid range is from 0 to 255. A higher value increases suppression to reduce probe traffic.

- **Optimized Roaming Hysteresis**: enter the RSSI in dBm to configure probe cycles to be suppressed.

  The valid range is from -6 to -3.

**Step 13** (Optional) Under **Access Point Features**, complete these configurations:

- **LED Brightness Level**: enter a number to indicate the brightness level of AP LEDs.

  The valid range is from 1 to 8. A higher number indicates higher brightness.

- **Use Locally Administered MAC Address**: enables or disables the use of locally administered MAC address for the AP.

  To override the default hardware MAC address for network policies or privacy, enable this option.

**Step 14** (Optional) Under **AP Audit & VLAN**, complete these configurations:

- **Enable AP Audit Report**: enables or disables periodic audit reports from APs.

- **AP Audit Report Interval (seconds)**: enter time in seconds to indicate how often APs send audit report to wireless controller.

  The valid range is from 10 to 43200.

- **Persistent VLAN Assignment**: enables or disables persistent VLAN assignment for clients.

  When enabled, clients retain the VLAN assignments across reassociations.

**Step 15** Under **AP HTTPS File Transfer**, complete these configurations:

- Use the **File Download** toggle button to enable or disable the HTTPS file download operations for APs.

- Use the **File Upload** toggle button to enable or disable the HTTPS file upload operations for APs.

**Step 16** Click **Review and Provision**.

**Step 17** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 18** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 19** On the **Tasks** window, monitor the task deployment.

## Configure load balancing for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the load-balancing parameters on the 5-GHz and 2.4-GHz bands for a wireless controller and provision the configuration.

For the 6-GHz band, global parameters like **Aggressive Load Balancing Window** and **Aggressive Load Balancing Denial Count** are configured in the RF profile.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

**Step 4** Click the **Load Balancing** tab.

**Step 5** Under **5 GHz** and **2.4 GHz**, enter data in these fields.

- **Aggressive Load Balancing Window (clients)**: enter the number of clients for the aggressive load-balancing window.

  The valid range is from 0 to 20.

- **Aggressive Load Balancing Denial Count**: enter the denial count for the aggressive load-balancing window.

  The valid range is from 1 to 10.

**Step 6** Click **Review and Provision**.

**Step 7** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure band selection for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the band selection parameters per WLAN for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

**Step 4** Click the **Band Select** tab.

**Step 5** (Optional) Enter data in these fields.

- **Cycle Count**: enter the maximum number of suppression cycles for a client.

  The valid range is from 1 to 10.

- **Cycle Threshold (msec)**: enter a value for the cycle threshold for band selection.

  The valid range is from 1 to 1000.

- **Age Out Suppression (sec)**: enter the expiry time for suppression in seconds.

  The valid range is from 10 to 200.

- **Age Out Dual Band (sec)**: enter the expiry time for dual-band.

  The valid range is from 10 to 300.

- **Client RSSI (dBm)**: enter a minimum value for the mobile station RSSI threshold.

  The valid range is from -90 to -20.

- **Client Mid RSSI (dBm)**: enter the medium mobile station RSSI threshold.

  The valid range is from -90 to -20.

**Step 6** Click **Review and Provision**.

**Step 7** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure optimized roaming for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the optimized roaming parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

**Step 4** Click the **Optimized Roaming** tab.

**Step 5** Under **6 Ghz**, **5 Ghz**, and **2.4 Ghz**, complete these configurations.

a) Use the **Optimized Roaming Mode** toggle button to enable or disable optimized roaming on the corresponding band.
b) From the **Optimized Roaming Data Rate Threshold (mbps)** drop-down list, choose a data rate threshold for 802.11 optimized roaming.

This threshold sets the minimum data rate required for a client to stay connected, encouraging clients to move to better coverage areas.

**Note** Misconfiguration of data rate threshold may result in client connectivity issues. If you have issues with clients being unintentionally disconnected after enabling this feature, lower or disable the data rate threshold.

c) In the **Optimized Roaming Hysteresis** field, enter the signal strength margin required for client roaming.

The valid range is from 0 to 10.

**Step 6** Click **Review and Provision**.

**Step 7** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure high-density parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the high-density parameters on the 5-GHz and 2.4-GHz bands for a wireless controller and provision the configuration.

For the 6-GHz band, the global high-density parameters like **Rx SOP Threshold** and **Multicast Data Rate** are configured in the RF profile.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

**Step 4** Click the **High Density** tab.

**Step 5** Under **Rx SOP Threshold**, from these drop-down lists, choose the required options.

- **5 GHz (dBm)**: choose a threshold value for the 5-GHz band.

If you chose **Custom**, in the **Custom 5 GHz (dBm)** field, enter a custom value for the Rx SOP threshold in dBm.

The valid range is from -85 to -60. The default value is -85.

- **2.4 GHz (dBm)**: choose a threshold value for the 2.4-GHz band.

  If you choose **Custom**, in the **Custom 2.4 GHz (dBm)** field, enter a custom value for the Rx SOP threshold in dBm.

  The valid range is from -85 to -60. The default value is -85.

**Step 6** Under **Multicast Data Rate**, from these drop-down lists, choose the required options.

- **5 GHz (dBm)**: choose a minimum data rate at which multicast clients can associate with APs for the 5-GHz band.
- **2.4 GHz (dBm)**: choose a minimum data rate at which multicast clients can associate with APs for the 2.4-GHz band.

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Add a preferred call for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to add a preferred call for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

**Step 4** Click the **Preferred Calls** tab.

**Step 5** Click **Add**.

**Step 6** In the **Call Index** field of the **Create Preferred Calls** slide-in pane, enter the SIP index for the call.

The valid range is from 1 to 6.

**Step 7** In the **Call Number** field, enter the SIP preferred call number.

The SIP preferred call number can contain up to 28 characters. Catalyst Center does not support ? and spaces in the call number.

**Step 8** Click **Review and Provision**.

**Step 9** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Configure RFID for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the radio frequency identification (RFID) parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

**Step 4** Click the **RFID** tab.

**Step 5** Use the **RFID State** toggle button to enable or disable the RFID tag tracking.

**Step 6** In the **RFID Timeout (sec)** field, enter the timeout value in seconds to clean up the stale RFID entries.

The valid range is from 60 to 7200.

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Configure cellular steering for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the cellular steering parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

**Step 4** Click the **Cellular Steering** tab.

**Step 5** Enter the RSSI threshold value in dBm to trigger the Wi-Fi to cellular steering for the

- 6-GHz band,
- 5-GHz band, and
- 2.4-GHz band.

The valid range is from -90 to -80 dBm.

**Step 6** Click **Review and Provision**.

**Step 7** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure 6-GHz client steering for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the 6-GHz client steering parameters per WLAN for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

**Step 4** Click the **6 GHz Client Steering** tab.

**Step 5** (Optional) Enter data in these fields.

- **6 GHz Transition Minimum Client Count**: enter the minimum number of clients for 6-GHz client steering.

  The valid range is from 0 to 200.

- **6 GHz Transition Minimum Window Size**: enter a value to set the minimum window size of the client steering.

  The valid range is from 0 to 200.

- **6 GHz Transition Max Utilization Difference (%)**: enter a value in percentage to set the maximum channel utilization difference to steer the clients.

  The valid range is from 0 to 100.

- **6 GHz Transition Min 2.4 GHz RSSI Threshold (dBm)**: enter the minimum received 2.4-GHz RSSI threshold to steer the clients.

  The valid range is from -70 to -20.

- **6 GHz Transition Min 5 GHz RSSI Threshold (dBm)**: enter the minimum received 5-GHz RSSI threshold to steer the clients.

  The valid range is from -75 to -20.

**Step 6** Click **Review and Provision**.

**Step 7** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure mDNS for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure a multicast Domain Name System (mDNS) gateway for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

**Step 4** In the **Global** tab, use the **mDNS Gateway** toggle button to enable or disable the mDNS gateway.

**Step 5** If you enable the mDNS gateway, complete these configurations.

- From the **Transport** drop-down list, choose a transport method for mDNS message processing.
- In the **Active-Query Timer (Minutes)** field, enter a time value in minutes.

  The valid range is from 1 to 120. The default value is 30.
- (Optional) From the **mDNS-AP Service Policy** drop-down list, choose an mDNS service policy.

  To create an mDNS service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 272.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Create an mDNS service definition for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an mDNS service definition for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

**Step 4** Hover your cursor over **Service Policy** and choose **Service Definition**.

**Step 5** Click **Add**.

**Step 6** In the **Service Definition Name** field of the **Create Service Definition** slide-in pane, enter a name for the service definition.

The service definition can contain up to 164 characters. It must start with an alphanumeric character.

**Step 7** (Optional) In the **Description** field, enter a description.

The description can contain up to 164 characters.

**Step 8** Under **Service Types**, configure service types.

| If you want to... | Then... |
|---|---|
| add a service type | **a.** Click **Add**.<br>**b.** In the **Service Type** field of the **Add Service Type** dialog box, enter a string for the service type. You can enter up to 164 characters.<br>Catalyst Center does not allow the special characters ?, <, >, & in the service type.<br>**c.** Click **Save**. |
| delete service types | **a.** Check the check box next to the service types that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 9** Click **Review and Provision**.

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Create an mDNS service list for a Cisco Catalyst 9800 Series Wireless Controller

You can create mDNS service lists for the ingress and egress directions. Use this procedure to create an mDNS service list for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

**Step 4** Hover your cursor over **Service Policy** and choose **Service List**.

**Step 5** Hover your cursor over **Add** and choose one of the directions.

- **Direction - IN**: creates service list for the ingress direction.
- **Direction - OUT**: creates service list for the egress direction.

**Step 6** In the **Service List Name** field of the **Create Service List** slide-in pane, enter a name for the service list.

The name can contain up to 164 characters.

For the **IN** direction, Catalyst Center does not allow the default-mdns-in-service-list name. For the **OUT** direction, Catalyst Center does not allow the default-mdns-out-service-list name.

**Step 7** (Optional) Click the **Assign All Services** toggle button to assign all services to the service list.

| If you chose... | Then... |
|---|---|
| **Direction - IN** | from the **Message Type** drop-down list, choose a message type. |
| **Direction - OUT** | from the **Wired Filter** drop-down list, choose a wired filter.<br>To create a wired filter, see Create an mDNS wired filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 273. |

**Step 8** (Optional) If the **Assign All Services** toggle button isn't enabled, under **Assigned Services**, configure the services.

| If you want to... | Then... |
|---|---|
| add an available service | **a.** Click **Add**.<br>**b.** From the **Services** drop-down list on the **Add Available Service**, choose a service definition.<br>Catalyst Center automatically populates the string based on the service definition in the **Service String** field.<br>**c.** Based on the chosen direction, complete these configurations.<br>• If you chose **Direction - IN**, from the **Message Type** drop-down list, choose a message type.<br>• If you chose **Direction - OUT**, from the **Wired Filter** drop-down list, choose a wired filter.<br>To create a wired filter, see Create an mDNS wired filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 273.<br>**d.** Click **Save**. |
| edit an available service | **a.** Check the check box next to the service that you want to edit.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Edit the required configuration.<br>**d.** Click **Save**. |

| If you want to... | Then... |
|---|---|
| delete available services | **a.** Check the check box next to the services that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 9** Click **Review and Provision**.

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an mDNS service policy for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

**Step 4** Hover your cursor over **Service Policy** and choose **Service Policy**.

**Step 5** Click **Add**.

**Step 6** In the **Service Policy Name** field of the **Create Service Policy** slide-in pane, enter a unique name for the service policy.

The service policy name can contain up to 164 characters.

**Step 7** (Optional) From these drop-down lists, choose the required options.

- **Service List Input**: choose an ingress service list.

  To create an ingress service list, see Create an mDNS service list for a Cisco Catalyst 9800 Series Wireless Controller, on page 270.

- **Service List Output**: choose an egress service list.

To create an egress service list, see Create an mDNS service list for a Cisco Catalyst 9800 Series Wireless Controller, on page 270.

- **Location**: choose an option for mDNS location-based filtering.
  - **ap-location**: Location-based filtering using the AP location.
  - **ap-name**: Location-based filtering using the AP name.
  - **location-group**: Location-based filtering using the location group.
  - **lss**: Location-based filtering using Location Specific Services (LSS).
  - **regex**: Location-based filtering using a Regular-Expression string.
  - **site-tag**: Location-based filtering using the site tag.
  - **ssid**: Location-based filtering using the SSID.

**Step 8** If you chose the **regex** option for location-based filtering using a regular-expression string, complete these configurations.

- From the **AP Regex** drop-down list, choose a corresponding location filtering option.
- In the **Regex Pattern** field, enter the regular-expression string.

  The regex pattern can contain up to 164 characters. Catalyst Center doesn't support ? in this field. If you enter %, +, or * in this field, do not enter any characters after these characters.

**Step 9** Click **Review and Provision**.

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Create an mDNS wired filter for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an mDNS wired filter for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

**Step 4** Hover your cursor over **Service Policy** and choose **Wired Filter**.

**Step 5** Click **Add**.

**Step 6** In the **Wired Filter Name** field of the **Create Wired Filter** slide-in pane, enter a unique name for the wired filter.

The wired filter name can contain up to 64 characters.

**Step 7** (Optional) In the **VLAN List** field, enter the list of VLAN IDs.

The valid range for VLAN IDs is from 1 to 4094. You can enter

- multiple VLAN IDs separated by a comma (for example, 20,30,40),
- a range of VLAN IDs (for example, 20-25), or
- up to 16 VLANs in the list separated by a comma (for example, 10-20,30,40-50).

**Step 8** Under **MAC Address**, configure the MAC addresses.

| If you want to... | Then... |
|---|---|
| add a MAC address | **a.** Click **Add**.<br>**b.** In the **MAC Address** field of the **Add MAC Address** dialog box, enter the MAC address of an mDNS service provider.<br>Enter the MAC address in the xxxx.xxxx.xxxx format.<br>**c.** Click **Save**. |
| delete MAC addresses | **a.** Check the check box for the MAC addresses that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 9** Click **Review and Provision**.

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Create an mDNS flex profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an mDNS flex profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

**Step 4** Click the **mDNS Flex Profile** tab.

**Step 5** Click **Add**.

**Step 6** In the **mDNS Flex Profile Name** field of the **Create mDNS Flex Profile** slide-in pane, enter a unique name for the mDNS flex profile.

The mDNS flex profile name can contain up to 164 characters. Catalyst Center does not allow ? and spaces in the profile name. The profile name must start with an alphanumeric character.

**Step 7** (Optional) Enter data in these fields.

- **Service Cache Update Timer**: enter a value for the mDNS service cache update timer.

  The valid range is from 1 to 100. The default value is 1.

- **Statistics Update Timer**: enter a value for the mDNS statistics update timer.

  The valid range is from 1 to 100.

- **VLAN List**: enter the list of VLAN IDs.

  The valid range for VLAN IDs is from 1 to 4094. You can enter

  - multiple VLAN IDs separated by a comma (for example, 20,30,40),
  - a range of VLAN IDs (for example, 20-25), or
  - up to 16 VLANs in the list separated by a comma (for example, 10-20,30,40-50)

**Step 8** (Optional) From the **Wired Service Policy** drop-down list, choose a service policy.

To create a service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 272.

**Step 9** Click **Review and Provision**.

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Configure multicast for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global wireless multicast parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

**Step 4** In the **General** tab, use the **Global Wireless Multicast** toggle button to enable or disable global wireless multicast.

If you enable global wireless multicast, you can optionally check the **Wireless mDNS Bridging** check box to enable mDNS bridging.

**Step 5** From the **AP CAPWAP Multicast** drop-down, choose a delivery mechanism for the multicast.

If you chose the **Multicast** option, you can optionally enter data in these fields.

- **AP CAPWAP IPv4 Multicast group Address**: enter an IPv4 multicast group address for CAPWAP used by APs.
- **AP CAPWAP IPv6 Multicast group Address**: enter an IPv6 multicast group address for CAPWAP used by APs.

**Step 6** Use the toggle buttons to enable or disable these configurations:

- **Wireless Non-IP Multicast**: allows administrators to enable or disable multicast traffic for non-IP applications.
- **Wireless Broadcast**: broadcast traffic transmission within the wireless network.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

# Configure IGMP snooping for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure Internet Group Management Protocol (IGMP) snooping for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

**Step 4** Click the **IGMP Snooping** tab.

**Step 5** (Optional) Check the **IGMP Snooping** check box to enable the IGMP snooping for VLANs.

If you enable IGMP snooping, complete these configurations:

- In the **Last Member Query Interval (msec)** field, enter the last member query interval in milliseconds.

  The valid range is from 100 to 32767.

- (Optional) Under **VLAN(s)**, enable or disable the required VLANs.

  To enable or disable VLANs, check the check box next to the required VLANs, hover your cursor over **Actions** and choose **Enable** or **Disable**.

**Step 6** (Optional) Check the **IGMP Snooping Querier** check box to enable the querier when there is no multicast router available in a VLAN to send IGMP membership queries.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

# Configure MLD snooping for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure global Multicast Listener Discovery (MLD) snooping for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

**Step 4** Click the **MLD Snooping** tab.

**Step 5** (Optional) Check the **Snooping** check box to enable global MLD snooping for VLANs.

If you enable MLD snooping, complete these configurations:

- In the **MLD Query Interval (msec)** field, enter the last listener query interval in milliseconds.

  The valid range is either 0 or 100 to 32768.

- (Optional) Under **VLAN(s)**, enable or disable the required VLANs.

  To enable or disable VLANs, check the check box next to the required VLANs, hover your cursor over **Actions** and choose **Enable** or **Disable**.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Configure PIM and multicast-routing for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure Protocol Independent Multicast (PIM) and multicast routing globally for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

**Step 4** Click the **PIM and Multicast-Routing** tab.

**Step 5** In the **PIM Configuration** section, configure these parameters:

- **PIM RP-Address**: Enter the Rendezvous Point (RP) address to statically configure the RP Address. This configuration is required so that receivers can find the multicast source in the network.
- **Auto RP Listener**: Enable Auto RP Listener to dynamically discover RP in a PIM-SM network.

**Step 6** In the **Multicast Routing Configuration** section, configure these settings:

- **Distributed Multicast-Routing**: Toggle this button to enable or disable the multicast configuration globally.
- **VRF with Distributed Multicast-Routing**: From the list of available VRFs, add or remove the VRFs to be used for distributed multicast-routing. This option enables the segmentation of multicast traffic across multiple virtual networks. To create an VRF interface, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 320.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create a VRF to RP address map for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a VRF to Rendezvous Point (RP) address map for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

**Step 4** Click the **VRF - RP Address Map** tab.

**Step 5** Click **Add**.

**Step 6** In the **Create VRF - RP Address Map** slide-in pane, complete these configurations:

- From the **VRF** drop-down list, choose a VRF.

  To create a VRF, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 320.

- In the **RP Address** field, enter the IP address of the RP for the group.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create wireless broadcast and non-IP multicast for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create VLAN broadcast and non-IP multicast for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

**Step 4** Click the **Wireless Broadcast and Wireless Non-IP Multicast** tab.

If the **More** drop-down list is displayed, hover your cursor over **More** and choose **Wireless Broadcast and Wireless Non-IP Multicast**.

**Step 5** In the **VLAN ID** field of the **Create VLAN Broadcast and Non-IP Multicast** slide-in pane, enter the VLAN ID.

The valid range is from 1 to 4094.

**Step 6** Use these toggle buttons to enable or disable the corresponding configurations:

- **Non-IP Multicast**: enable non-IP muticast for VLANs.
- **Broadcast**: allow broadcast packets for wireless clients.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure location for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the location parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Location**.

**Step 4** From the **Algorithm** drop-down list, choose an algorithm used for averaging the RSSI and SNR values.

- **Average**: sets the probe RSSI measurement updates to a more accurate algorithm with more CPU overhead.
- **Simple**: sets the probe RSSI measurement updates to a faster algorithm with smaller CPU overhead, but less accuracy.

**Step 5** Enter data in these fields.

- **Expiry Calibrating Client Threshold (sec)**: enter the timeout in seconds for calibrating the clients.

  The valid range is from 1 to 3600.

- **Expiry Client Threshold (sec)**: enter the timeout in seconds for RSSI values.

  The valid range is from 5 to 3600.

- **Notify Client Threshold (dB)**: enter the Network Mobility Services Protocol (NMSP) notification RSSI threshold for clients in dB.

The valid range is from 0 to 10.

This threshold defines the change in client RSSI that triggers a notification. For example, if you enter 5 in this field, NMSP sends a notification when the RSSI of a client changes by 5 dB.

- **Expiry Tags (sec)**: enter the RFID RSSI expiry time in seconds.

  The valid range is from 5 to 300.

  After the RSSI value expires, the RFID RSSI is cleaned up.

- **Notify Threshold Tags (dB)**: enter the Location Control Protocol (LOCP) notification threshold for RSSI measurements.

  The valid range is from 1 to 10.

**Step 6** From these drop-down lists, choose the required options.

- **RSSI Half Life Calibrating Client Threshold (sec)**: choose an RSSI half-life threshold for calibrating the clients.
- **RSSI Half Life Client Threshold (sec)**: choose an NMSP notification threshold for the clients.
- **RSSI Half Life Rogue AP Threshold (sec)**: choose an RSSI half-life threshold for rogue APs.
- **RSSI Half Life Tags (sec)**: choose an RSSI half-life threshold for RFID tags.

  RFID RSSI half-life represents the half life when averaging two RSSI readings for RFID tags.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure country codes for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure country codes for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Country**.

**Step 4** Configure the country codes.

Use these options to manage country codes:

| If you want to... | Then... |
|---|---|
| search for country codes | in the **Search** field, enter either the partial or full name of the country and press **Enter**. |
| add country codes | use one of these options:<br>• Click the plus icon next to the required country code.<br>• Click the country code and click **Add Selected**.<br>**Note** To select and add multiple country codes, press **Shift**, click the country code, and click **Add Selected**. |
| remove country codes | use one of these options:<br>• Click the **X** icon next to the required country code.<br>• Click the country code and click **Remove Selected**.<br>**Note** To select and remove multiple country codes, press **Shift**, click the country code, and click **Remove Selected**.<br>• Click **Remove All** to remove all the country codes. |

**Step 5** Click **Review and Provision**.

**Step 6** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 7** On the **Tasks** window, monitor the task deployment.

## Configure Cisco DNA integration settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure Cisco DNA integration settings for a wireless controller and provision the configuration.

Cisco DNA gRPC and Network Assurance gRPC can operate simultaneously. Cisco Spaces IoT Services and Catalyst Center gRPC can also run simultaneously.

**Note** The clear-text token configuration is available only when **wsaCfgIcapPort** is enabled.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Cisco DNA Integration Settings**.

**Step 4** In the **Clear Text Token** field, enter the AP join token in clear-text format.

Use this field when the token type is **Clear** or when you are migrating from unencrypted to encrypted tokens.

**Note** Clear-text tokens are less secure.

**Step 5** Click **Review and Provision**.

**Step 6** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 7** On the **Tasks** window, monitor the task deployment.

## Configure AP policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the AP policy for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **AP Policy**.

**Step 4** Click the **AP Policy** tab.

**Step 5** (Optional) Check the required check boxes to configure the corresponding policies.

- **Authorize APs against MAC**: configure the AP authorization policy with the MAC address
- **Authorize APs against Serial Number**: configure the AP authorization policy with the serial number

**Step 6** From the **Authorization Method List** drop-down list, choose an authorization method list.

To create an authorization method list for **Type - Credential-download**, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create a device authentication serial number for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a device authentication serial number for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **AP Policy**.

**Step 4** Hover your cursor over **Device Authentication** and choose **Serial Numbers**.

**Step 5** Click **Add**.

**Step 6** In the **Serial Number** field of the **Create Device Authentication Serial Number** slide-in pane, enter the device authentication serial number.

It can contain up to 255 characters. Catalyst Center does not support ? and spaces in the serial number.

**Step 7** (Optional) From the **Attribute List Name** drop-down list, choose an attribute list.

To create an attribute list, see Create an attribute list for a Cisco Catalyst 9800 Series Wireless Controller, on page 166.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create a device authentication MAC Address for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a device authentication MAC address for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **AP Policy**.

**Step 4** Hover your cursor over **Device Authentication** and choose **MAC Addresses**.

**Step 5** Click **Add**.

**Step 6** In the **MAC Address** field of the **Create Device Authentication MAC Address** slide-in pane, enter the device authentication MAC address.

It can contain up to 64 characters. You can enter the MAC address in the *xx:xx:xx:xx:xx:xx*, *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xxxxxxxxxxxx* format.

**Step 7** (Optional) From the **Attribute List Name** drop-down list, choose an attribute list.

To create an attribute list, see Create an attribute list for a Cisco Catalyst 9800 Series Wireless Controller, on page 166.

**Step 8** (Optional) In the **Description** field, enter a description.

You can enter up to 128 characters. Catalyst Center does not support ? in the description.

**Step 9** (Optional) From the **WLAN Profile Name** drop-down list, choose a WLAN profile.

To create a WLAN profile, see Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 66.

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Configure wireless geolocation settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure wireless geolocation settings for APs associated with a wireless controller to enable location-based services and tracking capabilities, and then provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Global Wireless** and click **Wireless Geolocation Settings**.

**Step 4** Use the **Enable Geolocation Derivation** toggle button to enable or disable the automatic update and derivation of geographic location of APs.

When you enable this option, the wireless controller automatically derives and updates the geographic location of APs using available network data. This option improves location-based services and reporting. If you disable this option, you must manually configure geolocation settings for each AP.

**Step 5** Click **Review and Provision**.

**Step 6** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 7** On the **Tasks** window, monitor the task deployment.

# Service configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device service configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Create a service template for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a service template for a local policy for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Local Policy**.

**Step 4** In the **Service Template** tab, click **Add**.

**Step 5** Enter data in these fields of the **Create Service Template** slide-in pane.

- **Service Template Name**: enter a unique name for the service template.

  The name can contain up to 48 characters.

- (Optional) **VLAN ID**: enter a VLAN ID.

  The valid range is from 1 to 4094.

- (Optional) **Session Timeout (sec)**: enter the session timeout in seconds.

  The valid range is from 1 to 1073741823.

**Step 6** (Optional) From these drop-down lists, choose the required options.

- **Access Control List** (to create an ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168)
- **Ingress QoS** (to create a QoS, see Create a QoS policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 291)
- **Egress QoS** (to create a QoS, see Create a QoS policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 291)
- **mDNS Service Policy** (to create an mDNS service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 272)

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create a policy map for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a policy map and map it to a service template for a local policy for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Local Policy**.

**Step 4** Click the **Policy Map** tab.

**Step 5** Click **Add**.

**Step 6** In the **Policy Map Name** field of the **Create Policy Map** slide-in pane, enter a unique name for the policy map.

**Step 7** (Optional) Under **Match Criteria List**, configure the required match criteria list.



**Note** Configure at least one match criteria list. You can configure up to 254 match criteria lists.

| If you want to... | Then... |
|---|---|
| add a match criteria list | **a.** Click **Add**.<br>**b.** From the **Service Template** drop-down list of the **Add Match Criteria List** dialog box, choose a service template for the local policy.<br>To create a service template, see Create a service template for a Cisco Catalyst 9800 Series Wireless Controller, on page 288.<br>**c.** (Optional) Check the required check boxes to include the corresponding filters in the match criteria list.<br>• **Device Type**<br>• **User Role**<br>• **User Name**<br>• **OUI**<br>• **MAC Address**<br>**d.** If you checked the check box for any filter, complete these configurations.<br>• From the corresponding **Condition** drop-down list, choose a condition for the filter: **equals**, **does not equal**, or **regex**<br>• Enter data in the corresponding field for the filter:<br>• **Device Type**: enter the device name.<br>• **User Role**: enter the user role.<br>• **User Name**: enter the user name.<br>• **OUI**: enter an Organizationally Unique Identifier (OUI) in hexadecimal format separated by a period. For example, *xx.xx.xx*.<br>• **MAC Address**: enter a MAC address in the *xxxx.xxxx.xxxx* format.<br>**e.** Click **Save**. |
| edit a match criteria list | **a.** Check the check box next to the sequence that you want to edit.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Edit the required configurations.<br>**d.** Click **Save**. |

| If you want to... | Then... |
|---|---|
| delete match criteria lists | **a.** Check the check box next to the sequences that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create a QoS policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a QoS policy for a wireless controller and provision it.

**Note** You must add at least one class map or configure class default for a QoS policy.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **QoS**.

**Step 4** Click **Add**.

**Step 5** In the **Policy Name** field of the **Create QoS Policy** slide-in pane, enter a unique name for the QoS policy.

Catalyst Center does not allow ? and spaces in the policy name.

**Step 6** (Optional) In the **Description** field, enter a description.

The description can contain up to 200 characters.

**Step 7** Under **Class Default**, complete these configurations.

a) From the **Mark Type** drop-down list, choose the required option: **None**, **DSCP**, or **User Priority**.

Marking can be used to either

- set certain fields or bits in the packet headers, or
- set certain fields in the packet structure that is internal to the device.

| If you chose... | Then... |
|---|---|
| **DSCP** | from the **Mark Value** drop-down list, choose the required option to set DSCP in IPv4 and IPv6 packets. |
| **User Priority** | from the **Mark Value** drop-down list, choose the required option to set the WLAN user priority. |

b) (Optional) In the **Police (kbps)** field, enter the committed information rate.

The valid range is from 8 to 10000000.

**Step 8** (Optional) Under **Class Maps**, configure class maps.

a) Click **Add** to add a class map.

In the **Add Class Map** dialog box, complete these configurations.

1. From the **Class Type** drop-down list, choose a class map type: **AVC** or **User Defined**.
2. From the **Match** drop-down list, choose a match type: **Any** or **All**.
3. From the **Drop** drop-down list, choose the required option to drop traffic from specific sources: **Disabled** or **Enabled**.

   If you chose **Disabled**, complete these configurations.

   - From the **Mark Type** drop-down list, choose the required option: **None**, **DSCP**, or **User Priority**.

| If you chose... | Then... |
|---|---|
| **DSCP** | from the **Mark Value** drop-down list, choose the required option to set DSCP in IPv4 and IPv6 packets. |
| **User Priority** | from the **Mark Value** drop-down list, choose the required option to set the WLAN user priority. |

   - (Optional) In the **Police (kbps)** field, enter the committed information rate.

     The valid range is from 8 to 10000000.

4. From the **Match Type** drop-down list, choose the required matching parameter.

| If you chose... | Then... |
|---|---|
| the **AVC** class type | add a matching parameter based on the match type using one of these methods:<br>• Click the plus icon next to the required matching parameter.<br>• Click the required matching parameter and click **Add Selected**.<br>To choose multiple matching parameters, press **Shift**, click the matching parameter, and click **Add Selected**.<br>• To add all the matching parameters, click **Add All**.<br>You can use the **Search** field to filter the matching parameter.<br>Add at least one matching parameter. You can add up to 256 matching parameters.<br>For example, if you chose the **Protocol** match type, choose at least one protocol. |
| the **User Defined** class type | from the **Match Value** drop-down list, choose the required matching parameter. |

5. Click **Save**.

b) To delete a class map, complete these steps.

1. Check the check box next to the required class map.
2. Hover your cursor over **Actions** and choose **Delete**.
3. In the dialog box, click **Yes**.

**Step 9** Click **Review and Provision**.

**Step 10** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create a custom application for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a custom application for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Application Visibility**.

**Step 4** In the **Custom Applications** tab, click **Add**.

**Step 5** In the **Application Name** field of the **Create Custom Application** slide-in pane, enter a unique name for the application.

The application name length must be between 3 and 24 characters. Catalyst Center allows alphanumeric characters, - and _ in the application name. Catalyst Center does not allow spaces and other special characters in the application name.

**Step 6** From the **Type** drop-down list, choose an application type: **URL**, **Server Name**, **Protocol**, or **DSCP**.

**Step 7** Based on the application type, complete these configurations.

a) If you choose **URL**, in the **URL** field, enter the URL.

Catalyst Center does not allow spaces in the URL.

b) If you choose **Server Name**, in the **Server Name** field, enter the server name.

You can enter up to 30 characters.

c) If you choose **Protocol**, complete these configurations:

- In the **IP Address** field, enter a valid IP address of the custom application in the *x.x.x.x* format.
- (Optional) In the **Subnet (0-32)** field, enter the subnet mask of the custom application.

  The valid range is from 0 to 32.
- Under **Protocol Type**, check the check box next to the required protocols: **TCP** and **UDP**
- Under **Port Values**, choose the required option.

- If you choose **Individual Values**, complete these configurations:

| If you want to... | Then... |
|---|---|
| add a port number | 1. Click **Add**.<br>2. In the **Port Number** field of the **Add Port Number** dialog box, enter a port number.<br>The valid range is from 1 to 65535.<br>3. Click **Save**. |
| delete port numbers | 1. Check the check box next to the port numbers that you want to delete.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

- If you choose **Range**, enter the start and end range for the port number in the corresponding fields.

  The valid range is from 1 to 65535.

d) If you choose **DSCP**, use one of these methods to add DSCP.

**Note** Add at least one DSCP.

- Click the plus icon next to the required DSCP.
- Click the required DSCP and click **Add Selected**.

  To choose multiple DSCP, press **Shift**, click the DSCP, and click **Add Selected**.
- To add all the DSCP, click **Add All**.

  You can use the **Search** field to filter the DSCP.

**Step 8** Choose either **Traffic Class** or **Similar To**.

| If you chose... | Then... |
|---|---|
| **Traffic Class** | from the **Traffic Class** drop-down list, choose a class. |
| **Similar To** | from the **Similar To** drop-down list, choose the required option. |

**Step 9** From the **Business Relevance** drop-down list, choose an option: **Relevant**, **Irrelevant**, or **Default**.

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create an exporter for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a flow exporter for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Application Visibility**.

**Step 4** Hover your cursor over **Flow Monitors** and click **Exporter**.

**Step 5** In the **Exporter** window, click **Add**.

**Step 6** In the **Create Exporter** slide-in pane, complete these configurations:

a) In the **Exporter Name** field, enter a unique name for the flow exporter.

You can enter up to 60 characters. Catalyst Center allows alphanumeric characters, - and _ in the exporter name. Catalyst Center does not allow spaces and other special characters in the exporter name.

b) (Optional) In the **Description** field, enter a description for the flow exporter.

You can enter up to 80 characters. Catalyst Center does not allow the special characters ?, <, >, and & in the exporter name.

c) From the **Exporter Type** drop-down list, select an exporter type: **External Collector** or **Local**.

If you select **External Collector**, complete these configurations:

- **Destination IP**: Enter the IP address of the destination and the flow records are sent to this destination device. Enter the IP address in the *xxx.xxx.xxx.xxx* format.
- **VRF**: Select a VRF from the drop-down list. The flow monitor is associated with the selected VRF.
- **Port**: Enter the UDP port number.

  The valid range is from 1 to 65535. The default value is 9995.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create a flow monitor for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a flow monitor for a wireless controller and provision it.

### Before you begin

Ensure that you have created flow exporters to be bound to the flow monitor.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Application Visibility**.

**Step 4** Hover your cursor over **Flow Monitors** and click **Monitor**.

**Step 5** In the **Monitor** window, click **Add**.

**Step 6** In the **Create Monitor** slide-in pane, enter the configuration settings:

- **Flow Monitor Name**: Enter a unique name for the flow monitor.

  You can enter up to 40 characters. Catalyst Center allows the special characters -, _, @, [, ], {, }, (, ), and . in the flow monitor name.

- (Optional) **Description**: Enter a description for the flow monitor.

  You can enter up to 80 characters. Catalyst Center does not allow ? in the flow monitor name.

- **Flow Exporters**: Use one of these methods to add the required flow exporters from the available list.
  - Click the plus icon next to the required flow exporter.
  - Click the required flow exporter and click **Add Selected**.

    To choose multiple flow exporter, press **Shift**, click the flow exporter, and click **Add Selected**.
  - To add all the flow exporter, click **Add All**.

    You can use the **Search** field to filter the flow exporter.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure EoGRE global parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the EoGRE global parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **EoGRE**.

**Step 4** In the **Global** tab, enter data in these fields.

- **Heartbeat Interval(sec)**: enter the heartbeat interval in seconds for keepalive to the tunnel gateway.

  The valid range is from 60 to 600.

- **Max Heartbeat Skip Count**: enter the maximum heartbeat skip count for keepalive to the tunnel gateway.

  The valid range is from 3 to 10.

**Step 5** From the **Interface Name** drop-down list, choose an interface.

To manage physical interfaces, Configure an Ethernet port for a Cisco Catalyst 9800 Series Wireless Controller, on page 319

To create an SVI profile, see Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 311.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Create an EoGRE gateway for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an EoGRE tunnel gateway for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **EoGRE**.

**Step 4** Click the **Gateways** tab.

**Step 5** Click **Add**.

**Step 6** In the **Tunnel ID** field of the **Create Gateway** slide-in pane, enter the tunnel ID.

**Step 7** Under **Destination IP Address**, choose an IP address option.

**Step 8** (Optional) From the **Source Interface** drop-down list, choose an interface.

To manage physical interfaces, see Configure an Ethernet port for a Cisco Catalyst 9800 Series Wireless Controller, on page 319.

To create an SVI profile, see Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 311.

**Step 9** (Optional) Based on the destination IP address option that you chose, complete these configurations.

| If you chose... | Then... |
|---|---|
| **Ipv4** | in the **Destination IP Address(IPv4)** field, enter the destination IPv4 address or host name. |
| **Ipv6** | in the **Destination IP Address(IPv6)** field, enter the destination IPv6 address or host name. |

**Step 10** (Optional) Click the **AAA Proxy** toggle button to enable AAA proxy and complete these configurations.

- From the **Encryption Type** drop-down list, choose an encryption type.
- Enter data in these fields.

- **Key Phrase**: enter the AAA key phrase.

  You can enter up to 128 characters.

- **Auth Port**: enter the AAA authentication or authorization port.

  The valid range is from 0 to 65535.

- **Acct Port**: enter the AAA accounting port.

  The valid range is from 0 to 65535.

**Step 11** Click **Review and Provision**.

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Create an EoGRE domain for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an EoGRE tunnel domain for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **EoGRE**.

**Step 4** Click the **Domains** tab.

**Step 5** Click **Add**.

**Step 6** In the **Domain Name** field of the **Create Domain** slide-in pane, enter a name for the tunnel domain.

**Step 7** (Optional) Click the **Status** toggle button to enable the tunnel domain.

**Step 8** (Optional) Choose a primary and secondary tunnel gateway from the corresponding drop-down lists.

**Step 9** (Optional) Check the **Revertive Redundancy** check box to enable the revertive redundancy model.

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create an EoGRE tunnel profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an EoGRE wireless tunnel profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **EoGRE**.

**Step 4** Click the **Tunnel Profiles** tab.

**Step 5** Click **Add**.

**Step 6** In the **General** tab of the **Create Tunnel Profile** slide-in pane, complete these configurations.

a) In the **Tunnel Profile Name** field, enter a name for the tunnel profile.

The tunnel profile name can contain up to 128 characters.

b) (Optional) Click the **Status** toggle button to enable the tunnel profile.
c) Use the **Centralized Forwarding** toggle button to indicate whether all wireless client traffic is routed through the central controller or forwarded locally to the AP.
d) Under **DHCP Option-82**, complete these configurations.

- (Optional) Click the **DHCP Option-82 Status** toggle button to enable the DHCP Option 82.
- (Optional) Click the **ASCII** toggle button to enable the DHCP Option 82 in ASCII format.

  If the ASCII format isn't used, the binary format is used.
- (Optional) In the **Delimiter** field, enter the DHCP Option 82 delimiter character.

  You can enter a single delimiter character.
- From these drop-down lists, choose the required options.
  - **MAC Format**: choose a DHCP Option 82 MAC format.
  - (Optional) **Circuit ID**: choose a DHCP Option 82 circuit ID.

- (Optional) **Remote ID**: choose a DHCP Option 82 remote ID.

e) (Optional) Under **AAA**, check the required check boxes to enable the corresponding configurations.

- **RADIUS Proxy**: enable AAA proxy.

  If you enable AAA proxy, you can optionally check the **Accounting Proxy** check box to enable AAA accounting proxy.

- **Override**: enable AAA override.

**Step 7** (Optional) Click the **Rules** tab and configure the required rules.

| If you want to... | Then... |
|---|---|
| add a rule | **a.** Click **Add**.<br>**b.** In the **Priority** field of the **Add Rule** dialog box, enter a number for the rule priority.<br>The valid range is from 1 to 100.<br>**c.** In the **Realm** field, enter the rule realm to match with.<br>The rule realm can contain up to 128 characters. Catalyst Center does not support leading or trailing spaces in the realm.<br>**d.** From the **Domain Name** drop-down list, choose a destination domain for the rule.<br>**e.** In the **VLAN ID** field, enter the rule VLAN ID.<br>The valid range is from 1 to 4094.<br>**f.** Click **Save**. |
| edit a rule | **a.** Check the check box next to the rule that you want to edit.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Edit the required configurations.<br>**d.** Click **Save**. |
| delete rules | **a.** Check the check box next to the rules that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Configure media stream for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the media stream parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Media Stream**.

**Step 4** In the **General** tab, use the **Enable Multicast Direct** toggle button to enable or disable the multicast-direct configuration.

**Step 5** (Optional) Under **Session Message Configuration**, complete these configurations.

a) Check the **Session Announcement State** check box to enable the media stream Session Description Protocol (SDP) message.
b) Enter data in these fields.

- **Session Announcement URL**: enter the media stream SDP URL.

  The URL can contain up to 128 characters.

- **Session Announcement Email**: enter the media stream SDP email ID.

  The email ID can contain up to 64 characters.

- **Session Announcement Phone**: enter the media stream SDP phone number.

  The phone number can contain up to 30 numbers and hyphens.

- **Session Announcement Note**: enter the media stream SDP announcement note.

  The announcement note can contain up to 128 characters.

**Step 6** Click **Review and Provision**.

**Step 7** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |

| Option | Description |
|---|---|
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create a media stream profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a media stream profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Media Stream**.

**Step 4** Click the **Streams** tab.

**Step 5** Click **Add**.

**Step 6** In the **Media Stream Name** field of the **Create Media Stream Profile** slide-in pane, enter a name for the media stream group.

The media stream group name can contain up to 64 characters.

**Step 7** In the **Maximum Expected Bandwidth (Kbps)**, enter the expected bandwidth for the media stream.

The valid range is from 1 to 35000. The default value is 1000.

**Step 8** Under **Multicast Destination**, enter valid IPv4 address or IPv6 address in these fields.

- **Start IPv4/IPv6 Address**: enter the media stream group starting IP address.
- **End IPv4/IPv6 Address**: enter the media stream group ending IP address.

  The starting and ending IP addresses must be of the same type.

**Step 9** Under **Resource Reservation Control (RRC) Parameters**, from the drop-down lists, complete these configurations.

a) In the **Average Packet Size (bytes)** field, enter the expected packet size for the stream.

The valid range is from 100 to 1500. The default value is 1200.

b) From these drop-down lists, choose the required options.

- **Policy**: choose an action for the stream: **Admit** or **Deny**
- **Priority**: choose a priority for the stream. You can choose a value from 1 to 8.
- **QoS**: choose a QoS value for the stream.
- **RRC re-evaluation**: choose an option for the RRC evaluation: **Periodical** or **Initial**
- **Violation**: choose an action for RRC violation: **Fallback** or **Drop**

**Step 10** Click **Review and Provision**.

**Step 11** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

# Create a guest LAN profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a guest LAN profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Guest LAN**.

**Step 4** In the **Guest LAN Profiles** tab, click **Add**.

**Step 5** In the **General** tab of the **Create Guest LAN Profile** slide-in pane, complete these configurations.

a) In the **Guest LAN Profile Name** field, enter a unique name for the guest LAN profile.

The profile name can contain up to 32 characters.

b) In the **ID** field, enter an ID for the guest LAN profile.

The valid range is from 1 to 5.

c) In the **Client Association Limit** field, enter the maximum number of client connections per a guest LAN.

The valid range is from 1 to 2000. The default value is 2000.

d) From the **mDNS Mode** drop-down list, choose an mDNS mode for the guest LAN: **Bridging**, **Drop**, or **Gateway**
e) Use the **Wired VLAN Status** toggle button to enable or disable a wired-VLAN ID for the guest LAN.

**Note** The wired-VLAN ID must be configured on the guest foreign controller.

If you enable the wired-VLAN ID, in the **Wired VLAN ID** field, enter the VLAN ID for the guest LAN on the guest foreign controller.

The valid range is from 0 to 4094. The default value is 0.

f) Use the **Status** toggle button to enable or disable the guest LAN.

**Step 6** (Optional) Click the **Security** tab and complete these configurations.

a) Check the **Web Auth** check box to configure security web authentication.
b) From these drop-down lists, choose the required options.

- **Web Auth Parameter Map** (to create a web authentication profile, see Create a web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 192)
- **Authentication List** (to create an authentication list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 158)

- **Authorization List** (to create an authorization list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159)

**Step 7** Click **Review and Provision**.

**Step 8** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create a guest LAN map for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a guest LAN map for a wireless controller and provision it.

**Note** You can create a single guest LAN map for a wireless controller.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Guest LAN**.

**Step 4** Click the **Guest LAN Map** tab.

**Step 5** Click **Add**.

**Step 6** In the **Map Name** field of the **Create Guest LAN Map** slide-in pane, enter a unique name for the guest LAN map.

The map name can contain up to 32 characters.

**Step 7** (Optional) Under **Guest LAN - Policy Map**, configure guest LAN and policy map profile.

**Note** You can configure up to five guest LAN and policy profile maps.

| If you want to... | Then... |
|---|---|
| add a guest LAN and policy profile map | **a.** Click **Add**.<br>**b.** From the **Guest LAN Profile Name** drop-down list on the **Add Guest LAN - Policy Map** dialog box, choose a guest LAN profile.<br>**c.** From the **Policy Profile Name** drop-down list, choose a policy profile.<br>**d.** Click **Save**. |
| edit a guest LAN and policy profile map | **a.** Check the check box next to the required profile name.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Edit the required configurations.<br>**d.** Click **Save**. |
| delete guest LAN and policy profile maps | **a.** Check the check box next to the required profile names.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** Click **Review and Provision**.

**Step 9** If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

| Option | Description |
|---|---|
| **License Manager** | Open the **License Manager** window and enable the corresponding licenses.<br>To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*. |

| Option | Description |
|---|---|
| **Continue to device provision** | Continue with the device provisioning.<br>**Note**<br>APs that don't meet the license requirements are in worldwide safe mode (WWSM). |
| **Cancel** | Close the dialog box. |

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Add an excluded client for a Cisco Catalyst 9800 Series Wireless Controller

Excluded clients can be used for troubleshooting or security purposes. By excluding the required clients, you can ensure that certain devices aren't able to access the network.

Use this procedure to add an excluded client for a wireless controller and provision it.

**Note** If you modify the list of clients from the Assurance window, the **Excluded Clients** table displays them only after the wireless controller is resynchronized.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **Excluded Clients**.

**Step 4** Click **Add**.

**Step 5** In the **Create Client Exclusion** slide-in pane, enter data in these fields.

- **Client device MAC Address**: enter the MAC address of the client that you want to exclude.

Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, *xxxx-xxxx-xxxx*, *xxxx:xxxx:xxxx*, or *xx:xx:xx:xx:xx:xx* format. Ensure that the client is not already on the exclusion list.

- **Description**: enter a description for the MAC address or a reason for exclusion.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Configure ThousandEyes for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to enable ThousandEyes wireless active testing and provision the configuration on a wireless controller.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Services** and click **ThousandEyes**.

**Step 4** In the **ThousandEyes Configuration** window, complete these configurations:

a) Use the **Wireless Active Testing Status** toggle button to enable or disable wireless active testing on the wireless controller.

When enabled, compatible APs can act as synthetic wireless clients to run ThousandEyes tests. ThousandEyes provides visibility from the AP to the cloud for proactive network assurance.

b) (Optional) In the **TE Connection String** field, enter the unique token that identifies the ThousandEyes account group for Endpoint Agent registration.

Obtain the token from the ThousandEyes Enterprise Agent application under **Endpoint Experience** > **Agent Settings** by clicking **Download** or **Add New Endpoint Agent**.

c) (Optional) Review the **TE Download URL** field and update it only if necessary.

By default, this field contains the URL for downloading and installing the ThousandEyes Endpoint Agent package on compatible APs.

### What to do next

Active testing APs require specific tag configurations to operate as synthetic wireless clients. Review and configure the required profiles and tags for your active testing APs:

- Configure a dedicated RF tag using a radio profile with the **Wireless Active Testing Radio Selection** enabled. This configuration allows the active testing AP radio to operate in synthetic client mode. Refer to Create a radio profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 103 and Create an RF tag for a Cisco Catalyst 9800 Series Wireless Controller, on page 105.
- Use an existing policy tag for the active testing AP. The active testing AP does not broadcast SSIDs from the policy tag. The SSID names in the policy tag are sent to ThousandEyes to support test configuration. Refer to Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 66, Create a policy profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 80, and Create a policy tag for a Cisco Catalyst 9800 Series Wireless Controller, on page 93.
- Use a site tag with an AP join profile that has Application Hosting enabled. This setting allows the ThousandEyes Endpoint Agent container to run on the AP. Refer to Create a site tag for a Cisco Catalyst 9800 Series Wireless Controller, on page 141 and Create an AP join profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 111.
- Assign the RF tag, policy tag, and site tag to the active testing AP through tag mapping. This step ties the required configurations together and places the AP into active testing operation. Refer to Tag mapping configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 144.
- Validate the operational state from the ThousandEyes Enterprise Agent application dashboard and the Catalyst Center Assurance or telemetry workflow.

# Layer 2 configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device Layer 2 configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a Switched VLAN Interface (SVI) profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 2** and click **VLAN**.

**Step 4** In the **SVI** tab, click **Add**.

**Step 5** In the **General** tab of the **Create SVI** slide-in pane, complete these configurations.

a) In the **VLAN Number** field, enter a VLAN ID for SVI.

The valid range is from 1 to 4094.

b) (Optional) In the **Description** field, enter a description.
c) Use the **Admin Status** toggle button to enable or disable the VLAN.
d) (Optional) From the **VRF** drop-down list, choose a VRF.

**Important** VRF modification results in the removal of IPv4 and IPv6 addresses.

e) (Optional) In the **MTU (bytes)** field, enter the value for IP MTU.

The valid range is from 68 to 18000. The default value is 1500.

f) (Optional) Check the **PIM Sparse Mode** check box to enable Protocol Independent Multicast (PIM) sparse mode for efficient multicast routing.

We recommend this mode for networks with sparse receiver distribution.

g) (Optional) From the **IGMP Version** drop-down list, choose an IGMP version.
h) (Optional) Check the **Autostate** check box to enable automatic state determination for VLAN.
i) (Optional) Check the **IPv4** check box to enable IPv4 addresses on the VLAN interfaces and complete these configurations.

- From the **Type** drop-down list, choose the method through which VLAN interfaces receive their IP configuration.
- If you choose **Static**,
  - In the **IP Address** field, enter an IPv4 address.
  - In the **Subnet Mask** field, enter a subnet mask.
  - Check the **Secondary** check box to add a secondary IP address.

    If you check this check box, enter the secondary IP address and subnet mask in the corresponding fields.
- If you choose **DHCP**, in the **Host Name** field, enter the host name.
- Under **OSPF**, complete these configurations.
  - From the **Process ID** drop-down list, choose an Open Shortest Path First (OSPF) process ID.
  - Check the **BFD** check box to enable Bidirectional Forwarding Detection (BFD).
  - Check the **Message Digest Authentication** check box to use message-digest authentication.
  - Under **Message Digest Authentication - Key Map(s)**, configure message digest authentication key map.

| If you want to... | Then... |
|---|---|
| add a message digest authentication key map | 1. Click **Add**.<br>2. In the **Key** field, enter the key.<br>3. In the **Password Type** field, enter the encryption type.<br>4. In the **Password** field, enter the OSPF key.<br>5. Click **Save**. |
| delete message digest authentication key map | 1. Check the check box next to the keys that you want to delete.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

j) (Optional) Check the **IPv6** check box to enable IPv6 addresses on the VLAN interfaces and complete these configurations.

- Configure IPv6 static.

| If you want to... | Then... |
|---|---|
| add an IPv6 static | 1. Click **Add**.<br>2. From the **Type** drop-down list in the **Add IPv6 Static** dialog box, choose a type.<br>3. In the **Address** field, enter the address for the VLAN interface.<br>4. Click **Save**. |
| delete IPv6 static | 1. Check the check box next to the IPv6 addresses that you want to delete.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Link Local**: use link-local address.

    If you check this check box, in the **Address** field, enter the link-local address.
  - **DHCP**: enable DHCP to allow SVI to dynamically obtain an IPv6 address.

    If you enable DHCP, you can optionally check the **Rapid Commit** check box to enable rapid commit for prefix delegation.
  - **Autoconfig**: enable automatic address assignment on VLAN interfaces.

    If you check this check box, you can optionally check the **Default** check box to insert the default route.
  - **Act as an IPv6 DHCP client**: enable automatic IPv6 address assignment from DHCP servers.

If you check this check box, in the **Prefix Name** field, you can optionally enter the prefix name.

You can enter up to 200 characters for the prefix name.

**Step 6** (Optional) Click the **Advanced** tab and complete these configurations.

a) Under **Access Lists**, choose an inbound and outbound IPv4 and IPv6 ACL from the corresponding drop-down lists.

To create an ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168 and Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 175.

b) Under **DHCP Relay**, complete these configurations.

- Check the **Relay Information Option** check box to enable the relay information option in the received DHCP.
- In the **Subscriber ID** field, enter the subscriber ID suboption.
- From the **Source-Interface VLAN** drop-down list, choose an SVI.

  To create an SVI profile, see Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 311.
- Check the **Server Id Override** check box to insert server-id-override and link-selection suboption.
- Check the **Option Insert** check box to allow insertion of DHCP options in outbound packets.

c) Under **Helper Address(es)**, configure the IPv4 helper addresses.

| If you want to... | Then... |
|---|---|
| add a helper address | 1. Click **Add**.<br>2. In the **IPv4 Helper Address** field of the **Add Helper Address** dialog box, enter the DHCP server IP address.<br>3. Click **Save**. |
| delete a helper address | 1. Check the check box next to the helper addresses that you want to delete.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

d) Check the **mDNS Gateway** check box to enable mDNS gateway.

Ensure that the mDNS gateway is configured in the global configuration mode. For more information, see Configure mDNS for a Cisco Catalyst 9800 Series Wireless Controller, on page 268.

(Optional) If you check this check box, from the **mDNS Service Policy** drop-down list, choose an mDNS service policy. To create an mDNS service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 272.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create a VLAN profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a VLAN profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 2** and click **VLAN**.

**Step 4** Click the **VLAN** tab.

**Step 5** Click **Add**.

**Step 6** In the **VLAN ID** field of the **Create VLAN** slide-in pane, enter a VLAN ID.

The valid range is from 1 to 4094.

**Step 7** In the **Vlan Name** field, enter a VLAN name.

**Step 8** From the **State** drop-down list, choose an operational state for the VLAN.

**Step 9** Click **Review and Provision**.

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Create a VLAN group profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a VLAN group profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 2** and click **VLAN**.

**Step 4** Click the **VLAN Group** tab.

**Step 5** Click **Add**.

**Step 6** In the **VLAN Group Name** field of the **Create VLAN Group** slide-in pane, enter a VLAN group name.

**Step 7** In the **VLAN List** field, enter a value for the VLAN list.

You can enter either

- a VLAN ID (the valid range for VLAN ID is from 1 to 4094) or
- a range of comma-separated VLAN IDs (for example 1-20,30,40-50).

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create a port channel interface for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a port channel interface for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

**Step 4** Hover your cursor over **Logical** and choose **Port Channel**.

**Step 5** Click **Add**.

**Step 6** In the **Create Port Channel** slide-in pane, complete the required configurations.

a) In the **Port Channel Number** field, enter the port channel number.

The valid range is from 1 to 64.

b) (Optional) In the **Description** field, enter a description.

You can enter up to 200 characters. Catalyst Center does not allow ? in the description.

c) Use the **Admin Status** toggle button to enable or disable the interface.
d) Use the **Layer 3 Address** toggle button to change the port channel type from Layer 2 to Layer 3 or Layer 3 to Layer 2.

**Note** Changing the port channel type removes the port members. You must reselect the port members.

e) Under **Port Members**, configure port members for the port channel type.

| If you want to... | Then... |
|---|---|
| search for port members | in the **Search** field, enter either the partial or full name of the port member and press **Enter**. |
| add port members | use one of these options:<br>• Click the plus icon next to the required port member.<br>• Click the port member and click **Add Selected**.<br>**Note**<br>To select and add multiple port members, press **Shift**, click the port member, and click **Add Selected**. |
| remove port members | use one of these options:<br>• Click the **X** icon next to the required port member.<br>• Click the port member and click **Remove Selected**.<br>**Note**<br>To select and remove multiple port members, press **Shift**, click the port member, and click **Remove Selected**.<br>• Click **Remove All** to remove all port members. |

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Create loopback interface for a Cisco Catalyst 9800 Series Wireless Controller

The loopback interface is used for management and routing purposes in a wireless controller.

Use this procedure to create loopback interface for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

**Step 4** Hover your cursor over the **Logical** tab, click **Loopback**.

**Step 5** Click **Add**.

**Step 6** In the **Create Loopback** slide-in pane, complete these configurations.

a) Enter a unique number as **Loopback Number**, which is used to identify the loopback interface.
b) (Optional) In the **Description** field, enter a description.
c) (Optional) Use the **Admin Status** toggle button to enable or disable the selected interface.
d) (Optional) From the **VRF** drop-down list, choose a VRF so that the loopback interface is associated with the selected VRF table. This ensures that the traffic on the loopback interface is routed according to the routing table of the VRF.
e) Enable the **Relay Information Option**, so that the received DHCP packets do not set the gateway IP address (giaddr) field. This configuration is used in networks where the relay agent needs to provide additional information to the DHCP server without specifying a gateway IP address. The DHCP server can then use the information in the relay agent information option to assign IP addresses and other configuration parameters.
f) Under **IP Options**, choose the required options.
g) If you choose **IPv4**, configure these settings:

- From the **IPv4 Type** drop-down list, choose the type of the IP address.
- In the **IP address** field, enter the IPv4 address to be assigned to the loopback interface.
- In the **Subnet Mask** field, enter the subnet mask.

- (Optional) Check the **Secondary IP** check box to assign a secondary IP address to the loopback interface. Enter the **Secondary IP** address and **Secondary IP Mask**.

h) If you choose **IPv6**, configure these settings:

- Select at least one of these IPv6 configurations:
  - **DHCP**: Enables DHCPv6 for the loopback interface. If chosen, then you can optionally enable the **Rapid Commit**, for delegation of the prefix.
  - **Autoconfig**: Configures the loopback interface automatically. If selected, then select the auto configuration to be inserted from the **Autoconfig** drop-down list.
  - **Act as an IPv6 DHCP client**: Enables automatic assignment of the IPv6 address. If chosen, then enter the prefix name in the **Act as an IPv6 DHCP client** field.
- Under **Static lists**, configure the static list.

| If you want to... | Then... |
|---|---|
| add a static list | 1. Click **Add**.<br>2. From the **Static** drop-down list in the **Add Static List** dialog box, choose a static list.<br>3. Based on the static list, enter a valid IPv6 address in the corresponding field.<br>4. Click **Save**. |
| delete static lists | 1. Check the check box next to the static lists that you want to delete.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure an Ethernet port for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure an Ethernet port for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

**Step 4** In the **Ethernet** tab, click the radio button next to the Ethernet port that you want to configure.

**Step 5** Hover your cursor over **Actions** and choose **Edit**.

**Step 6** (Optional) In the **General** tab of the **Edit Ethernet Ports** slide-in pane, in the **Description** field, enter a description for the port.

**Step 7** (Optional) In the **Advanced** tab, choose the inbound and outbound IPv4 and IPv6 ACLs from the corresponding drop-down lists.

To create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168.

To create an IPv6 ACL, see Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 175.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller

The Virtual Routing and Forwarding (VRF) interface is used for segmenting multiple routing table instances in a wireless controller.

Use this procedure to create VRF interface for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

**Step 4** In the **VRF** tab, click **Add**.

**Step 5** In the **Create VRF** slide-in pane, complete these configurations.

- Choose the protocols from these options: **IPv4**, **IPv6**, or **IPv4/IPv6**. The routing table is created based on the selected protocol.
- In the **VRF name** field, enter a name for the VRF.
- In the **Route Distinguisher** field, enter the route distinguisher details in the **ASN:nn** format. This is a unique ID that is used to distinguish between routes in different VRFs
- For the **Route-Target Import**, click **Add** to specify the route-target extended community attributes that the VRF should import. This allows the VRF to accept routes from other VRFs that have matching route-target attributes.
- For the **Route-Target Export**, click **Add** to specify the route-target extended community attributes that the VRF should export. This allows the VRF to advertise its routes to other VRFs with matching route-target attributes.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Configure the wireless management interface for a Cisco Catalyst 9800 Series Wireless Controller

The wireless management interface is used for all communications between the wireless controller and APs. A wireless controller has a single wireless management interface.

Use this procedure to configure the wireless management interface for a wireless controller and provision it.

**Note** Changing the interface or trustpoint causes APs to disconnect and disrupt clients.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

**Step 4** Click the **Wireless** tab.

**Step 5** (Optional) Complete these configurations.

a) From the **Interface Name** drop-down list, choose an interface.

To create an SVI interface, refer to Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 311. To create an Ethernet port, refer to Configure an Ethernet port for a Cisco Catalyst 9800 Series Wireless Controller, on page 319.

b) In the **Trustpoint** field, enter the wireless management trustpoint name.
c) In the **NAT IPv4/IPv6 Server Address** field, enter the NAT IP address.
d) Use the toggle buttons to enable or disable these configurations:

- **Enable NAT on L3 Interface Cache**: Enable or disable Network Address Translation (NAT) for Layer 3 interface cache data.
- **Private IP Discovery**: Enable or disable the option to allow the wireless controller to detect and log private IP addresses associated with client devices.
- **Public IP Discovery**: Enable or disable the option to allow the wireless controller to detect and log public IP addresses associated with client devices.

**Step 6** Under **Controller Management Security**, complete these configurations:

- In the **SSC Authentication Token** field, enter the Secure Socket Communications (SSC) token used for secure management communication with the wireless controller.

**Note** Ensure that this token is kept confidential and matches the expected value on peer devices or management systems.

- From the **SSC Auth Token Type** drop-down list, choose the encryption or hashing method used to store and transmit the SSC authentication token.

**Note** If you change the token type, you may need to update tokens on all connected systems.

**Step 7** Under **SSC Trust Hashes**, configure SSC trust hashes.

| If you want to... | Then... |
|---|---|
| Add an SSC trust hash | **a.** Click **Add**.<br>**b.** In the **SSC Certificate Fingerprint** field of the **Add SSC Trust Hash** dialog box, enter the fingerprint or hash of the SSC used by an AP for secure communication with the wireless controller.<br>**c.** Click **Save**. |
| Edit an SSC trust hash | **a.** Check the check box next the SSC trust hash that you want to edit.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Edit the configuration.<br>**d.** Click **Save**. |
| Delete SSC trust hashes | **a.** Check the check box for the SSC trust hashes that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Configure discovery protocols for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure discovery protocols for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 2** and click **Discovery Protocols**.

**Step 4** Under **CDP**, complete these configurations.

a) Use the **CDP Status** toggle button to enable or disable Cisco Discovery Protocol (CDP).

If you enable CDP, enter data in these fields.

- **Hold Time**: enter the hold time, in seconds, to be sent in CDP packets.

  The valid range is from 10 to 255.

- **Timer**: enter the rate, in seconds, at which CDP packets are sent.

  The valid range is from 5 to 254.

b) From the **CDP Advertisement Version** drop-down list, choose the required version.

**Step 5** Under **LLDP**, complete these configurations.

a) Use the **LLDP Status** toggle button to enable or disable the Link Layer Discovery Protocol (LLDP).
b) (Optional) Add the type, length, and value (TLV) using one of these methods.

- Click the plus icon next to the required TLV.
- Click the required TLV and click **Add Selected**.

  To choose multiple TLVs, press **Shift**, click the TLV, and click **Add Selected**.

- To add all the TLVs, click **Add All**.

  You can use the **Search** field to filter the TLVs.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

# Network settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device network settings for a Cisco Catalyst 9800 Series Wireless Controller.

## Configure DNS loopback for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure DNS-based hostname-to-address translation for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **DNS**.

**Step 4** Use the **DNS Loopback** toggle button to enable or disable DNS-based address to hostname translation

**Step 5** Click **Review and Provision**.

**Step 6** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 7** On the **Tasks** window, monitor the task deployment.

#### What to do next

If you enable DNS loopback, in the **DNS** table, you can add, edit, or delete DNS servers. To add a DNS server, see Add a DNS server for DNS loopback, on page 325.

## Add a DNS server for DNS loopback

Use this procedure to add a DNS server for DNS-based hostname to address translation for a Cisco Catalyst 9800 Series Wireless Controller.

If you enable DNS loopback for a Cisco Catalyst 9800 Series Wireless Controller, you must add at least one DNS server. To configure DNS loopback, see Configure DNS loopback for a Cisco Catalyst 9800 Series Wireless Controller, on page 324.



**Note** A DNS IPv6 server address created in the long format is converted to the short format after device resync.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **DNS**.

**Step 4** In the **DNS** table, click **Add**.

**Step 5** In the **Create DNS** slide-in pane, complete these configurations:

a) (Optional) To enable VRF, check the **VRF** check box.
b) If you enable VRF, from the **VRF Name** drop-down list, choose a VRF.

**Note** When VRF is enabled, Catalyst Center does not support the VRF **None**.

To create a VRF interface, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 320.

c) Configure DNS servers.

| If you want to... | Then... |
|---|---|
| add a DNS server | 1. Click **Add**.<br>2. In the **DNS Server(IPv4 / IPv6)** field of the **Add DNS Server(IPv4 / IPv6)** dialog box, enter a valid IPv4 or IPv6 address of the DNS server.<br>3. Click **Save**. |
| delete DNS servers | 1. Check the check box next to the DNS servers that you want to delete.<br>2. Hover your cursor over **Actions** and select **Delete**.<br>3. In the dialog box, click **Yes**. |

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

# Create an IPv4 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv4 DHCP pool for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **DHCP Pools**.

**Step 4** Hover your cursor over **DHCP Pools** and choose **IPv4**.

**Step 5** Click **Add**.

**Step 6** In the **General** tab of the **Create DHCP Pools** slide-in pane, complete these configurations.

a) In the **DHCP Pool Name** field, enter a unique name for the DHCP pool.

The DHCP pool name can contain up to 236 characters. Catalyst Center does not support ? or spaces in the DHCP pool name.

b) (Optional) Check the **VRF** check box to enable VRF.

If you enable VRF, from the **VRF Name** drop-down list, choose a VRF to associate with the DHCP pool.

c) In the **Network** field, enter a valid network IP address.
d) From the **Subnet Mask** drop-down list, choose a subnet mask.
e) From the **Lease** drop-down list, choose an option for lease expiry.

If you chose the **User Defined** option, enter data in these fields.

- **Days** (the valid range is from 0 to 365)
- **Hours** (the valid range is from 0 to 23)
- **Minutes** (the valid range is from 0 to 59)

**Step 7** (Optional) In the **Advanced** tab, complete these configurations.

a) In the **Domain** field, enter a domain name.

Domain names can contain up to 255 characters for wireless controllers running Cisco IOS XE Release 17.15.1 or later. Catalyst Center does not support ? or spaces in the domain name.

b) (Optional) Under **Default Router**, configure default routers.

| If you want to... | Then... |
|---|---|
| add a default router | 1. Click **Add**.<br>2. In the **Default routers** field of the **Add Default Router(s)** dialog box, enter the default router IP address.<br>3. Click **Save**.<br>**Note** The default router must be in the same subnet as the DHCP pool. |
| delete default routers | 1. Check the check box next to the default routers that you want to delete.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

c) (Optional) Under **DNS Server**, configure DNS servers.

| If you want to... | Then... |
|---|---|
| add a DNS server | 1. Click **Add**.<br>2. In the **DNS Server List** field of the **Add DNS Server** dialog box, enter the DNS server IPv4 address.<br>3. Click **Save**. |
| delete DNS servers | 1. Check the check box next to the DNS servers that you want to delete.<br>2. Hover your cursor over **Actions** and click **Delete**.<br>3. In the dialog box, click **Yes**. |

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create an IPv6 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv6 DHCP pool for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **DHCP Pools**.

**Step 4** Hover your cursor over **DHCP Pools** and choose **IPv6**.

**Step 5** Click **Add**.

**Step 6** In the **DHCP Pool Name** field of the **Create DHCP Pools** slide-in pane, enter a unique name for the DHCP pool.

The DHCP pool name can contain up to 232 characters. Catalyst Center does not support ? or spaces in the DHCP pool name.

**Step 7** (Optional) Under **Domain Names**, configure domain names.

| If you want to... | Then... |
|---|---|
| add a domain name | **a.** Click **Add**.<br>**b.** In the **Domain Name** field of the **Add Domain Names** dialog box, enter the domain name.<br>The domain name can contain up to 225 characters.<br>**c.** Click **Save**. |
| delete domain names | **a.** Check the check box next to the domain names that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** Under **DNS Server**, configure DNS servers.

| If you want to... | Then... |
|---|---|
| add a DNS server | **a.** Click **Add**.<br>**b.** In the **DNS Server List** field of the **Add Domain Names** dialog box, enter the DNS server IPv6 address.<br>**c.** Click **Save**. |

| If you want to... | Then... |
|---|---|
| delete DNS servers | **a.** Check the check box next to the DNS servers that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 9** Under **IPV6 Address Allocation**, configure IPv6 address allocation.

| If you want to... | Then... |
|---|---|
| add an IPv6 address | **a.** Click **Add**.<br>**b.** In the **IPv6 Address** field of the **Add IPV6 Address Allocation** dialog box, enter the IPv6 address.<br>**c.** Click **Save**. |
| delete IPv6 addresses | **a.** Check the check box next to the IPv6 addresses that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Configure DHCP persistence for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure DHCP persistence for a Cisco Catalyst 9800 Series Wireless Controller and provision the configuration.

### Before you begin

Ensure that you have already created the DHCP pools.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **DHCP Pools**.

**Step 4** Click the **DHCP Persistence** tab. Select the interface to configure DHCP persistence.

**Step 5** Hover your cursor over **Action** and click **Edit**.

Alternatively, click the interface name.

**Step 6** In the **Edit DHCP Persistence** slide-in pane, configure these parameters:

- **Interface**: Displays the client interface for which the IP address should be assigned.
- **Pool Name**: Choose the DHCP pool name from the drop-down list. By default, the DHCP pool **None** is selected.

  To create a DHCP pool, see Create an IPv4 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller, on page 327 and Create an IPv6 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller, on page 328.

  **Note** To change the DHCP pool name, first choose the DHCP pool **None** and provision the configuration. After the provisioning is completed, choose the required DHCP pool.

- **Reserved IP Address**: Enter the reserved IP address.

  This IP address ensures that these IP addresses are not dynamically assigned to other devices.

  **Note** This field is disabled when the DHCP pool **None** is selected.

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

## Configure HTTP and HTTPS for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure HTTP and HTTPS for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **HTTP/HTTPS**.

**Step 4** Check the required check boxes to enable the corresponding configurations.

- **HTTP Access**: enable the HTTP server.

  If you check this check box, in the **HTTP Port** field, enter the HTTP port number.

  The valid values are either 80 or any number from 1024 to 65535.

  **Note** The HTTP and HTTPS port numbers must be different. To switch to a port that is already in use for HTTPS, provision a new port for HTTPS and then use the port for HTTP.

  For example, if HTTPS is configured to use port 1028 and you want HTTP to use port 1028, first change the HTTPS port to a different number and provision the configuration, and then assign port 1028 to HTTP.

- **HTTPS Access**: enable the HTTPS secure server.

  If you check this check box, in the **HTTPS Port** field, enter the HTTPS port number.

  The valid values are either 443 or any number from 1025 to 65535.

  **Note** The HTTP and HTTPS port numbers must be different. To switch to a port that is already in use for HTTP, provision a new port for HTTP and then use the port for HTTPS.

  For example, if HTTP is configured to use port 1026 and you want HTTPS to use port 1026, first change the HTTP port to a different number and provision the configuration, and then assign port 1026 to HTTPS.

- **Personal Identity Verification**: enable personal identity verification.

**Note** Configure the trustpoint, CA server certificate on the wireless controller. Ensure that the client certificate is signed by the CA server on the browser. Otherwise, access to the wireless controller UI is not available.

If you enable personal identity verification, you can optionally check the **Personal Identity Verification Authorization only** check box to set the verification for only the web UI.

**Step 5** From the **Authentication** drop-down list, choose an authentication method.

If you chose **aaa**, from these drop-down lists, you can optionally choose the required options.

- **Authorization List** (to create an authorization method list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 159)
- **Authentication List** (to create an authentication method list of the type **LOGIN**, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 158)

**Step 6** (Optional) Under **HTTP Proxy Configuration**, enter data in both these fields.

- **Client Proxy Server**: enter the client proxy server.

  You can enter an IPv4 address, IPv6 address, or host name.

- **Client Proxy Port**: enter the client proxy port.

  The valid range is from 1 to 65535.

**Note** If you enter data in one of these fields, you must also enter data in the other field. Catalyst Center supports the combined length of up to 215 characters for both fields.

**Step 7** Under **HTTP Trustpoint**, use the **Enable TrustPoint** toggle button to enable or disable the HTTP trustpoint.

If you enable HTTP trustpoint, from the **Secure Trustpoint** drop-down list, choose a secure server certificate trustpoint.

**Note** Changes to the secure trustpoint settings in the HTTP interface can disrupt access to the wireless controller UI, potentially affecting the management capabilities.

**Step 8** Under **Timeout Policy**, enter data in these fields:

- **HTTP Timeout-policy (secs)**: enter the idle timeout of HTTP server connection in seconds.

  The valid range is from 1 to 600.

- **Session Idle Timeout(secs)**: enter the HTTP server session idle timeout in seconds.

  For wireless controllers running Cisco IOS XE Release 26.2.1 or later, the valid range is from 180 to 14400. For wireless controllers running versions earlier than Cisco IOS XE Release 26.2.1, the valid range is from 180 to 1200.

- **Server Life Time (secs)**: enter the lifetime of an HTTP server connection in seconds.

  The valid range is from 1 to 86400.

- **Max number of requests**: enter the maximum number of requests allowed on an HTTP server connection.

  The valid range is from 1 to 86400.

**Step 9** Click **Review and Provision**.

**Step 10** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 11** On the **Tasks** window, monitor the task deployment.

## Configure general SNMP parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the general SNMP parameters for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

**Step 4** (Optional) In the **General** tab, enter data in these fields.

- **System Location**: enter the location of the device.

  The system location can contain up to 234 characters. Catalyst Center does not support ? in the system location.

- **System Contact**: enter the contact details of the device administrator.

  The contact details can contain up to 235 characters. Catalyst Center does not support ? in the contact details.

**Step 5** Click **Review and Provision**.

**Step 6** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 7** On the **Tasks** window, monitor the task deployment.

## Configure SNMP wireless traps for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure SNMP wireless traps for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

**Step 4** Click the **Wireless Traps** tab.

**Step 5** Use the **Enable** toggle button under each area to enable or disable the corresponding traps.

- **General Controller**
- **Mesh**
- **RF**
- **Rogue**
- **RRM**
- **Wireless Client**
- **Wireless Mobility**

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Add an SNMP community string for a Cisco Catalyst 9800 Series Wireless Controller

An SNMP community string is a password that is used to authenticate access to the managed devices. It can also be used for device discovery.

**Note** If an SNMP community string used for device discovery is deleted, the device enters into an Unmanaged state on Catalyst Center.

Use this procedure to add an SNMP community string for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

**Step 4** Click the **Community Strings** tab.

**Step 5** Click **Add**.

**Step 6** In the **Community Name** field of the **Add Community String** slide-in pane, enter the SNMP community string.

SNMP community string is a password to authenticate access to the managed devices. The string can contain up to 128 characters. Catalyst Center does not support ?, backslash (\), and spaces in the string.

**Step 7** From the **Access Mode** drop-down list, choose a mode in which the SNMP management station can retrieve information from the device.

- **Read Only**: view or retrieve information from the network device.
- **Read/Write**: view information and modify device settings and configurations.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create SNMPv3 user group for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create SNMPv3 user group for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

**Step 4** Click the **V3 User Groups** tab.

**Step 5** Click **Add**.

**Step 6** In the **Group Name** field of the **Create V3 User Groups** slide-in pane, enter a unique name for the SNMPv3 user group.

The user group name can contain up to 32 characters.

**Step 7** Under **Security Level**, configure the level of the security for the user group.

| If you want to... | Then... |
|---|---|
| add a security level | **a.** Click **Add**.<br>**b.** From the **Security Level** drop-down list in the **Add Security Level** dialog box, choose a security level.<br>• **AUTH**: Messages are authenticated but not encrypted.<br>• **NOAUTH**: No security applied.<br>• **PRIV**: Messages are authenticated and encrypted.<br>**Note** Security level types must be unique in a user group.<br>**c.** (Optional) In the **Read View** field, specify the read view for the group<br>**d.** (Optional) In the **Write View** field, specify the write view for the group. |

| If you want to... | Then... |
|---|---|
| edit a security level | **a.** Check the check box for the security level.<br>**b.** Hover your cursor over **Actions** and choose **Edit**.<br>**c.** Update the required configuration.<br>**d.** Click **Save**. |
| delete security levels | **a.** Check the check box security levels that you want to delete.<br>**b.** Hover your cursor over **Actions** and choose **Delete**.<br>**c.** In the dialog box, click **Yes**. |

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Create an SNMPv3 user for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an SNMPv3 user for a wireless controller and provision it. SNMPv3 provides enhanced security for network management by supporting authentication and privacy.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

**Step 4** Click the **V3 Users** tab.

**Step 5** Click **Add**.

**Step 6** In the **Create V3 User Groups** slide-in pane, complete these configurations:

a) In the **Username** field, enter a unique name for the SNMPv3 user.

The user group name can contain up to 32 characters.

b) From the **Group Name** drop-down list, choose an SNMPv3 user group.

To create an SNMPv3 user group, see Create SNMPv3 user group for a Cisco Catalyst 9800 Series Wireless Controller, on page 337.

c) From the **Security Mode** drop-down list, choose a security level for authentication and privacy.

| If you choose... | Then... |
|---|---|
| **AuthPriv** | • From the **Privacy Protocol** drop-down list, choose a protocol for data encryption.<br>• From the **Privacy Encryption** drop-down list, choose an encryption method for the privacy password.<br>**Note**<br>To use encryption types **6** or **7**, ensure that the device is configured to accept plain-text passwords, or provide the preencrypted password. Otherwise, choose encryption type **0**.<br>• In the **Privacy Password** field, enter the privacy password. |
| **AuthPriv** or **AuthNoPriv** | • From the **Authentication Protocol** drop-down list, choose a protocol for authentication.<br>If you choose **SHA2**, from the **Authentication Algorithm** drop-down list, choose the bit length for SHA-2 authentication algorithm.<br>• From the **Authentication Encryption** drop-down list, choose an encryption method for the authentication password.<br>**Note**<br>To use encryption types **6** or **7**, ensure that the device is configured to accept plain-text passwords, or provide the preencrypted password. Otherwise, choose encryption type **0**.<br>• In the **Authentication Password** field, enter the authentication password.<br>• (Optional) From the **ACL IPv6** drop-down list, choose an IPv6 ACL.<br>To create an IPv6 ACL, see Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 175. |
| **AuthPriv**, **AuthNoPriv**, or **NoAuthNoPriv** | (Optional) From the **ACL IPv4** drop-down list, choose an IPv4 ACL.<br>To create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 168. |

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

---

The **V3 Users** table shows only the SNMPv3 users with encrypted passwords.

## Create an SNMP host for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an SNMP host for a wireless controller and provision it.

### Procedure

---

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

**Step 4** Click the **Hosts** tab.

**Step 5** Click **Add**.

**Step 6** In the **IP Address** field of the **Create SNMP Host** slide-in pane, enter the IP address of the host.

**Step 7** From the **Version** drop-down list, choose an SNMP version to send the trap.

| If you choose... | Then... |
|---|---|
| **V1** or **V2C** | from the **Community String** drop-down list, choose an SNMP community string.<br>To add a community string, refer to Add an SNMP community string for a Cisco Catalyst 9800 Series Wireless Controller, on page 336. |
| **V3** | complete these configurations:<br>• In the **V3 User** field, enter the user name for SNMPv3 authentication and encryption.<br>• From the **Security Level** drop-down list, choose a security level. |

**Step 8** (Optional) In the **UDP Port** field, enter the number for the SNMP destination port.

The valid range is from 0 to 65535. The default value is 162.

**Step 9** From the **Type** drop-down list, choose the type of SNMP notifications.

- **traps**: SNMP notifications are unacknowledged.
- **informs**: SNMP notifications are acknowledged.

**Step 10** Click **Review and Provision**.

**Step 11** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 12** On the **Tasks** window, monitor the task deployment.

## Create an NTP server profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a Network Time Protocol (NTP) server profile for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **NTP**.

**Step 4** In the **NTP** tab, click **Add**.

**Step 5** In the **Host Name** field of the **Create NTP Server Profile** slide-in pane, enter the host name.

You can enter an IPv4 address, IPv6 address, or a Fully Qualified Domain Name (FQDN).

**Step 6** (Optional) Check the **Prefer** check box to use this NTP server profile by default.

**Step 7** From the **IP for DNS Resolution** drop-down list, choose the type of IP address used for Domain Name System (DNS) resolution.

**Step 8** From the **Source Address** drop-down list, choose an interface that is used to communicate with the NTP server.

| If you chose... | Then... |
|---|---|
| **VLAN** | from the **VLAN** drop-down list, choose a VLAN to communicate with the NTP server. |
| **Interface** | from the **Interface** drop-down list, choose the interface that is used to communicate with the NTP server. |

**Step 9** (Optional) Check the **Enable Authentication** check box to enable authentication against the NTP server.

If you check this check box, from the **Key** drop-down list, choose a key index that is used for authentication.

To create an authentication key profile, see Create an authentication key profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 342.

**Step 10** (Optional) Check the **VRF** check box to configure NTP servers for each VRF to ensure accurate time synchronization within isolated routing domains, enhancing network reliability and event logging for specific segments.

If you check this check box, based on the IP address option that you choose for DNS resolution choose a VRF interface from the corresponding drop-down list. To create a VRF, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 320.

**Step 11** Click **Review and Provision**.

**Step 12** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 13** On the **Tasks** window, monitor the task deployment.

## Create an authentication key profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an authentication key profile to authenticate against an NTP server for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Network Settings** and click **NTP**.

**Step 4** Click the **Authentication Keys** tab.

**Step 5** Click **Add**.

**Step 6** In the **Authentication Key Number** field of the **Create Authentication Key** slide-in pane, enter a unique authentication key number.

The valid range is from 1 to 4294967295.

**Step 7** In the **Authentication Key** field, enter an authentication key for MD5 authentication.

The authentication key can contain up to 32 characters. Catalyst Center does not support ? and spaces in the authentication key.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

# Layer 3 configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device Layer 3 configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Create a static route for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a static route for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Layer 3** and click **Routing**.

**Step 4** In the **Static** tab, hover your cursor over **Add** and choose the required static route option.

**Step 5** If you chose **IPv4**, in the **Create Static Route** slide-in pane, complete these configurations.

a) In the **Prefix** field, enter the static route prefix.
b) In the **Prefix Mask** field, enter the static route prefix mask.

c) (Optional) Check the **VRF** check box to enable Virtual Routing and Forwarding (VRF).

If you check this check box, from the **VRF Name** drop-down list, choose a VRF. To create a VRF, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 320.

d) (Optional) Check the **DHCP** check box to obtain the default gateway from DHCP.

If you check this check box, in the **Metric** field, enter a value.

The valid range is from 1 to 255. The default value is 1.

e) (Optional) Under **Route Path List**, configure route path lists.

| If you want to... | Then... |
|---|---|
| add a route path list | **1.** Click **Add**.<br>**2.** From the **Route Path** drop-down list in the **Add Route Path List** dialog box, choose a route path.<br>If you chose **Interface**, from the **Interface** drop-down list, choose an interface.<br>**3.** In the **Next Hop IP** field, enter the next hop IP address.<br>If you chose **Interface**, this field is optional.<br>**4.** In the **Metric** field, enter a value.<br>The valid range is from 1 to 255. The default value is 1.<br>**5.** Click **Save**. |
| delete route path lists | **1.** Check the check box next to the required route paths.<br>**2.** Hover your cursor over **Actions** and choose **Delete**.<br>**3.** In the dialog box, click **Yes**. |

**Step 6** If you chose **IPv6**, in the **Create Static Route** slide-in pane, complete these configurations.

a) In the **Prefix** field, enter the static route IPv6 prefix.

b) In the **Prefix Length** field, enter the static route prefix length.

c) (Optional) Check the **VRF** check box to enable Virtual Routing and Forwarding (VRF).

If you check this check box, from the **VRF Name** drop-down list, choose a VRF. To create a VRF, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 320.

d) (Optional) Under **Route Path List**, configure route path lists.

| If you want to... | Then... |
|---|---|
| add a route path list | 1. Click **Add**.<br>2. From the **Route Path** drop-down list in the **Add Route Path List** dialog box, choose a route path.<br>If you chose **Interface**, from the **Interface** drop-down list, choose an interface.<br>3. In the **Next Hop IP** field, enter the next hop IP address.<br>If you chose **Interface**, this field is optional.<br>4. (Optional) In the **Administrative Distance** field, enter a value.<br>The valid range is from 1 through 254. The default value is 1.<br>5. Click **Save**. |
| delete route path lists | 1. Check the check box next to the required route paths.<br>2. Hover your cursor over **Actions** and choose **Delete**.<br>3. In the dialog box, click **Yes**. |

**Step 7** Click **Review and Provision**.

**Step 8** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 9** On the **Tasks** window, monitor the task deployment.

# Administrative configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device administrative configurations for a Cisco Catalyst 9800 Series Wireless Controller.

## Configure device administration settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the device administration settings for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Administration** and click **Device**.

**Step 4** In the **General** tab, complete these configurations:

- Use the **IP Routing** toggle button to enable or disable IP routing.
- In the **Host Name** field, enter the host name.

  The host name can contain uppercase and lowercase letters, numbers, hyphens (-), underscores (_), and periods (.). The host name must not contain only numbers.
- (Optional) In the **Banner** field, enter the required data.

**Step 5** Click **Review and Provision**.

**Step 6** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 7** On the **Tasks** window, monitor the task deployment.

## Configure device FTP/SFTP/TFTP settings for a Cisco Catalyst 9800 Series Wireless Controller

In a network, you can ensure secure transfer of files between devices by configuring one of these transfer protocols:

- File Transfer Protocol (FTP): Used for transferring files between a client and a server over a network.
- Secure File Transfer Protocol (SFTP): Uses Secure Shell (SSH) for encrypted file transfers.
- Trivial File Transfer Protocol (TFTP): A simpler, lightweight protocol for transferring files, often used for network booting or firmware upgrades.

Use this procedure to configure the FTP, SFTP, and TFTP settings for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Administration** and click **Device**.

**Step 4** Click the **FTP/SFTP/TFTP** tab.

**Step 5** Under **FTP Settings**, complete these configurations:

- From the **Source Interface** drop-down list, choose the source interface.
- **Username**: Enter a user name for the FTP connection.

  The user name can contain up to 237 characters. Catalyst Center does not support ? and spaces in the user name.
- **Password**: Enter a password for the FTP connection.

  The password can contain up to 25 characters. It must contain at least one alphanumeric character. Catalyst Center does not support ? in the password.

**Step 6** Under **SFTP Settings**, from **Source Interface** drop-down list, choose an interface.

**Step 7** Under **TFTP Settings**, from the **Source Interface** drop-down list, choose an interface.

**Step 8** Click **Review and Provision**.

**Step 9** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 10** On the **Tasks** window, monitor the task deployment.

## Configure user administration settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the user administration settings for a wireless controller and provision the configuration.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Administration** and click **User Administration**.

**Step 4** Click **Add**.

**Step 5** In the **Create User Administration** slide-in pane, configure the parameters to define the user role and privilege.

a) **User Name**: Enter a unique user name for the new account.

The name can contain up to 64 characters. Catalyst Center does not support ? in the user name.

b) **Policy**: Choose a password policy from the drop-down list. This policy is associated with the user.
c) **Advanced Mode**: Toggle this option to enable the privilege level to the advanced mode.
d) **Privilege**: Choose the user privilege level based on the mode. If you have not enabled the **Advanced** mode, then the privilege is set for the basic mode.
e) If you choose the basic mode, these privilege options are available:

- **Admin**: Users have access to all the sections in the GUI.
- **Read Only**: Users have access only to the dashboard and monitoring sections.
- **No Access**: Users cannot access the GUI.
- **Lobby Admin**: Users who can create only guest user accounts.

**Note** To change the privilege from Lobby Admin to another role or vice versa, delete the existing entry and add a new entry with the required privilege.

f) If you choose the advanced mode, choose the privilege level from 0 to 15.

- Privilege 15 is an admin user.
- Privileges 1 to 14 are considered as read-only users.
- Privilege 0 has no access.

g) **Password**: Enter a password for the user account and re-enter it for confirmation in the **Confirm Password** field.

The password can contain up to 127 characters. The password in the **Confirm Password** field must match the password in the **Password** field.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

## Configure AP upgrade settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the AP upgrade settings for a wireless controller and provision it.

### Procedure

**Step 1** Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

**Step 2** Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

**Step 3** In the **Configuration** tab, expand **Administration** and click **AP Upgrade Configuration**.

**Step 4** From the **AP Upgrade Percentage per Iteration** drop-down list, choose the required option for AP upgrade percentage per iteration or AP upgrade mode.

These options are available:

- Staggered upgrade: to upgrade the APs associated with the wireless controller in batches based on the selected percentage.
- One-time upgrade: to upgrade all the APs associated with the wireless controller in a single iteration.
- Serial upgrade: to upgrade one AP associated with the wireless controller at a time.

You can choose a staggered upgrade percentage, one-time upgrade, or serial upgrade of the APs associated with the wireless controller.

**Step 5** Use these check boxes to enable or disable the corresponding settings:

- **Client Steering**: Steer clients away from AP during the upgrade.
- **Client Deauthentication**: Deauthenticate clients connected to the AP during the upgrade before it reloads.

**Step 6** Click **Review and Provision**.

**Step 7** Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

**Step 8** On the **Tasks** window, monitor the task deployment.

# Inter-Release Controller Mobility introduction

Inter-Release Controller Mobility (IRCM) supports seamless mobility and wireless services across different Cisco Wireless Controllers with different software versions.

Catalyst Center supports the guest anchor feature for device combinations, including:

- Configuration of a Cisco AireOS controller as a foreign controller with a Cisco AireOS controller as an anchor controller.
- Configuration of a Cisco AireOS controller as a guest anchor controller with a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller.
- Configuration of a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller with a Cisco Catalyst 9800 Series Wireless Controller as an anchor controller.

Configuring IRCM on controller devices has limitations, including:

- Configuration of a Cisco AireOS controller as a foreign controller and Cisco Catalyst 9800 Series Wireless Controller as an anchor controller is not supported.
- Configuration of a fabric guest anchor is not supported.
- Only guest SSID is supported.
- Broadcast of a nonguest anchor SSID in guest anchor mode is not supported.

## Guest anchor configuration and provisioning process

Use this procedure to configure a guest anchor Cisco Wireless Controller.

### Procedure

**Step 1** Design a network hierarchy, with sites, buildings, floors, and so on. For more information, see Create, edit, and delete a site and Add, edit, and delete a building.

**Step 2** Configure network servers, such as AAA, DHCP, and DNS servers. For more information, see Configure global network servers and Add Cisco ISE or other AAA servers.

**Step 3** Create SSIDs for a guest wireless network with external web authentication and central web authentication along with configuring Cisco Identity Services Engine. For more information, see Create SSIDs for a guest wireless network.

**Step 4** Discover the wireless controller using the Cisco Discovery Protocol (CDP) or an IP address range, and make sure that the devices are in the **Devices** > **Inventory** window and in the **Managed** state. For more information, see Discovery overview.

**Step 5** Provision a foreign wireless controller as the active main wireless controller. See Provision a Cisco AireOS Controller, on page 4.

**Note** If you choose a site with multiple network profiles while provisioning a foreign wireless controller, ensure that the total number of anchor groups for the network profiles is three or less.

**Step 6** Choose the role for the wireless controller as guest anchor and provision the guest anchor controllers. For more information, see Provision a Cisco AireOS Controller, on page 4.

**Note**
- You must choose the same site as the managed AP location for the anchor wireless controller as specified for the SSID.
- If you modify the interface configuration for the anchor wireless controller, you must reprovision it.

**Step 7** Configure device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Add global CLI credentials, Add global SNMPv2c credentials, Add global SNMPv3 credentials, and Add global HTTPS credentials.

# Prerequisites for configuring IRCM on a Cisco controller device

- Discover the Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.

  You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete the configurations of network devices.

  For more information, see Discover your network using CDP or Discover your network using an IP address range or CIDR.

- Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

  To create a new network hierarchy, see Create, edit, and delete a site and Add, edit, and delete a building.

- Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

  For more information, see Work with APs on a floor map.

- Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network. You can add a TACACS server while adding a AAA server.

  For more information, see Network settings overview, Configure global network servers, and Add AAA server.

- Create SSIDs for a guest wireless network.

  For more information, see Create SSIDs for a guest wireless network.

- The WLAN profile name of the foreign controller and anchor controller should be the same for mobility.

# Configuring IRCM on a Cisco AireOS Controller and a Cisco Catalyst 9800 Series Wireless Controller

### Before you begin

Ensure the prerequisites for configuring IRCM are met. For more information, see Prerequisites for configuring IRCM on a Cisco controller device, on page 351.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window display with the discovered devices listed.

**Step 2** Check the check box next to the Catalyst 9800 Series Wireless Controller that you want to provision as a foreign controller.

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

**Step 4** In the **Assign Site** window, click **Choose a Site** to assign a site for the Catalyst 9800 Series Wireless Controller device.

**Step 5** In the **Add Sites** window, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.

**Step 6** Click **Save**.

**Step 7** Click **Apply**.

**Step 8** Click **Next**.

**Step 9** Select a role for the Catalyst 9800 Series Wireless Controller as **Active Main WLC**.

**Step 10** For an active main wireless controller, you need to configure interface and VLAN details.

**Step 11** Under the **Assign Interface** area, do these steps:

a) **VLAN ID**: Enter a value for the VLAN ID.
b) **IP Address**: Enter the interface IP address.
c) **Gateway IP Address**: Enter the gateway IP address.
d) **Subnet Mask (in bits)**: Enter the interface net mask details.

**Note** Assigning an IP address, gateway IP address, and subnet mask is not required for the Catalyst 9800 Series Wireless Controller.

**Step 12** Click **Next**.

**Step 13** In the **Summary** window, review the configuration settings.

**Step 14** Click **Deploy** to provision the Catalyst 9800 Series Wireless Controller as a foreign controller.

**Step 15** On the **Devices** > **Inventory** window, check the check box next to the Cisco AireOS Controller that you want to provision as a guest anchor controller.

**Step 16** Repeat Step 3 through Step 8.

**Step 17** Select a role for the Cisco AireOS Controller as **Guest Anchor**.

**Step 18** For a guest anchor wireless controller, you need to configure the interface and VLAN details.

**Step 19** Repeat Step 11 through Step 14.

# Prerequisites for provisioning a Meraki device

- Integrate the Meraki dashboard with Catalyst Center. See Integrate the Meraki dashboard.
- Create the SSID. See Create SSIDs for an enterprise wireless network.

**Note** The Meraki dashboard supports these types of SSIDs:

- Open: This SSID corresponds to Open in the Meraki dashboard.
- WPA2 Personal: This SSID corresponds to the preshared key with WAP2 in the Meraki dashboard.
- WPA2 Enterprise: This SSID corresponds to WAP-2 Encryption with Meraki authentication or My Radius server in the Meraki dashboard. If you have defined AAA or Cisco ISE servers for client and endpoint authentication at the building level in Catalyst Center, the configuration is provisioned to **my Radius server** in the Meraki dashboard. Otherwise, **Meraki Radius** is used for authentication by the Meraki devices.

For every SSID, you can choose an interface name. If you choose the **Management** interface in Catalyst Center and the VLAN ID is 0, the configuration is not supported in the Meraki dashboard and VLAN tagging is disabled in the Meraki dashboard. If you create a custom interface for the SSID in Catalyst Center, an AP tag is created with the custom interface name and VLAN ID in the Meraki dashboard.

- Create the network profile and assign it to the sites for which the SSID is provisioned.

**Note** The Network Hierarchy **Sites** > **Buildings** in Catalyst Center corresponds to **Organization** > **Network** in the Meraki dashboard. We recommend that you choose **Buildings** in the **Add Sites to Profile** window in the workflow.

**Note** Catalyst Center creates the Meraki network and provisions the SSIDs to the network. The Meraki dashboard provisions the Meraki network configuration to the Meraki devices.

# Provision a Meraki device

This procedure explains how to provision SSIDs for Cisco Meraki devices managed by a Meraki dashboard.

### Before you begin

Ensure the prerequisite is met. For more information, see Prerequisites for provisioning a Meraki device, on page 353.

### Procedure

**Step 1** From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

**Step 2** To view the Meraki dashboard, expand the **Global** site in the left pane, and choose a building.

All Meraki dashboards available in the chosen building display.

**Step 3** Check the check box next to the Meraki dashboard name that you want to provision.

**Step 4** From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window displays, which is where you can view the Meraki dashboard and the associated building.

**Step 5** To change the associated building, click **Choose a site**.

**Step 6** In the **Choose a site** window, select a building and click **Save**.

**Step 7** Click **Next**.

The **Configuration** window displays. You can view the managed building in the primary location.

**Step 8** Click **Select Secondary Managed AP Locations** to choose the secondary managed location for the Meraki dashboard.

**Step 9** In the **Managed AP Location** window, check the check box next to the building name.

**Step 10** Click **Save**.

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

**Note** Meraki deployment supports a maximum of 15 SSIDs in each network.

**Step 12** Click **Deploy**.

**Step 13** In the **Provision Devices** window, do these steps to preview the CLI configuration:

a) Click the **Generate Configuration Preview** radio button.
b) In the **Task Name** field, enter a name for the CLI preview task, and click **Apply**.
c) In the **Task Submitted** dialog box, click the **Work Items** link.

**Note** This dialog box displays for a few seconds and then disappears. To navigate to the **Tasks** window, click the menu icon and choose **Activities** > **Tasks**.

d) In the **Tasks** window, click the CLI preview task for which you submitted the configuration preview request.
e) View the CLI configuration details, and click **Deploy**.
f) To immediately deploy the device, click the **Now** radio button, and click **Apply**.

g) To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
h) In the **Information** dialog box, do these steps:
   1. Click **Yes** if you want to delete the CLI preview task from the **Tasks** window.
   2. Click **No** if you want to retain the task in the **Tasks** window.



**Note** The CLI task will be marked as completed in the **Tasks** window. You can view the CLI configuration for this task, but you cannot deploy it again.



**Note** 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).

The **Provision Status** column in the **Device Inventory** window shows `SUCCESS` after a successful deployment.

# Provision remote teleworker devices

These topics explain the components of remote teleworker sites and the procedure for provisioning remote teleworker devices.

## Remote teleworker deployment overview

### Deployment components

The Cisco remote teleworker deployment is built around three main components: Cisco wireless controllers, Cisco OfficeExtend access points (APs) and a Corporate firewall. These models are supported in this deployment:

- **Wireless Controllers**: Cisco 5520 Wireless Controller, Cisco 8540 Wireless Controller, Cisco 3504 Wireless Controller[2], Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-80 Wireless Controller, Cisco Catalyst 9800-CL Wireless Controller, and Cisco Catalyst 9800-L Wireless Controller.
- **Access Points**: Cisco Aironet 1815T (Teleworker) Access Point, Cisco Aironet 1815I Access Point, Cisco Aironet 1815W Access Point, Cisco Aironet 1840I Access Point, Cisco Aironet 2800 Series Access Points, Cisco Aironet 3800 Series Access Points, Cisco Aironet 4800 Series Access Points, Cisco Catalyst 9115 Access Point, Cisco Catalyst 9120 Access Point, and Cisco Catalyst 9130 Access Point.

[2] Supported with Cisco Aironet 1815 Teleworker Access Point only.

### Cisco Wireless Controllers

Cisco controllers are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco APs to support business-critical wireless applications for teleworkers. Controllers provide the control, scalability, security, and reliability that network managers need to build a secure, scalable teleworker environment.

To allow users to connect their corporate devices to the organization's on-site wireless network, the remote teleworking solution offers the same wireless Secure Set Identifiers (SSIDs) at a teleworker's home as those that support data and voice inside the organization.

### Cisco OfficeExtend Access Points

APs cannot act independently of controllers. As an AP communicates with the controller resources, it downloads its configuration and synchronizes its software or firmware image, if required. The AP establishes a secure Datagram Transport Layer Security (DTLS) connection to the controller, which offers remote WLAN connectivity using the same profile as at the corporate office. Secure tunneling allows all traffic to be validated against centralized security policies and minimizes the management overhead associated with home-based firewalls.

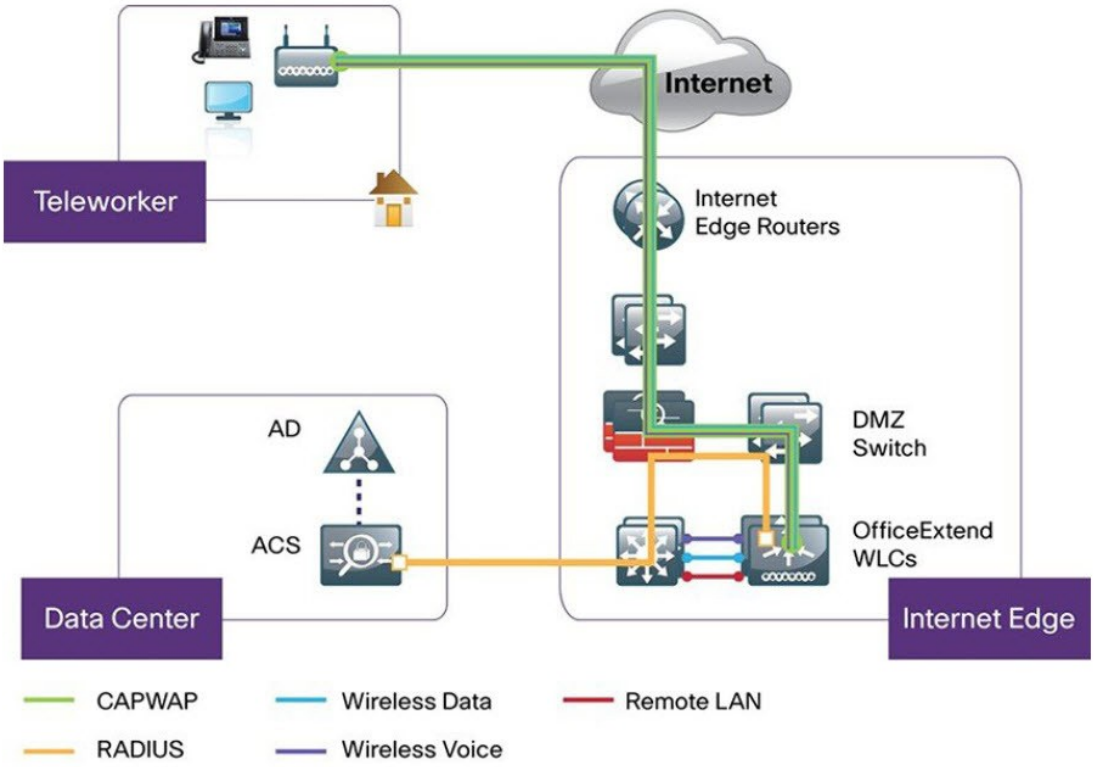
### Corporate firewall

The controller should be placed in a demilitarized zone (DMZ) and the corporate firewall must allow CAPWAP control and data traffic through the firewall to the controller. The general configuration on the firewall is to allow CAPWAP control and CAPWAP management port numbers through the firewall. The UDP 5246 and 5247 ports need to be opened on the firewall for communication between the controller and the AP.

### Deployment configuration

For the most flexible and secure remote teleworker configuration, deploy a dedicated controller pair in a dedicated to the Internet edge DMZ. Traffic from the Internet terminates in the DMZ versus in the internal network, while the remote AP is still directly connected to the internal network.

*Figure 1: Sample remote teleworker deployment scenario*




# Create a remote teleworker site

A remote teleworker site is a dedicated site that is used only to manage wireless controllers and remote teleworker access points (APs). To create a remote teleworker site, you need to enable the remote teleworker function on the site. When enabled, the remote teleworker function can't be independently disabled for a site, building, or floor within the site's hierarchy. The site can only manage remote teleworker functions.

In a teleworker site, switching is performed centrally from the controller. You can't configure the network profile for FlexConnect with local switching.

### Before you begin

- Understand the supported devices that are used in a teleworker deployment.
- Make sure that you have a Cisco Wireless Controller and Cisco APs in your inventory. If not, discover the devices or add them manually. For more information, see Discover Your Network or Add a network device.
- Configure global wireless network settings appropriate for your network. For more information, see Configure global wireless settings.
- For remote teleworker APs, we recommend that you create an AP profile with remote teleworker enabled and configure custom site tags. For more information, see Configure additional settings for an AP profile for Cisco IOS XE devices and Add AP groups, flex groups, site tags, and policy tags to a network profile.

- For Cisco AireOS devices, you must map the AP profile to the custom AP group of the site that will be used for the remote teleworker AP. For more information, see Create network profiles for wireless and Add AP groups, flex groups, site tags, and policy tags to a network profile.

### Procedure

**Step 1** Create a site to manage remote teleworker APs. See Create, edit, and delete a site.

**Step 2** Add buildings and floors. See Add, edit, and delete a building.

**Step 3** Configure the wireless network settings for the remote teleworker site.

a) From the main menu, choose **Design** > **Network Settings** > **Wireless**.
b) From the left hierarchy tree, select the remote teleworker site.
c) Click **Remote Teleworker**.
d) Check the **Enable Remote Teleworker** check box.
e) Click **Save**.

**Step 4** Assign the controller to the site. See Assign an unprovisioned device to a site.

**Step 5** Assign the APs to the site. See Assign an unprovisioned device to a site.

You can use serial numbers or MAC addresses but not a mixture of both, or you can upload a CSV file.

**Step 6** In the wireless network settings, add the APs to the authorized APs list.

a) From the left hierarchy tree, select Global.
b) From the main menu, choose **Design** > **Network Settings** > **Wireless**.
c) Click **Security Settings**.
d) Click the **AP Authorization List** tab and add the APs that are allowed to join the controller. For more information, see Create an AP authorization list.

The controller responds only to CAPWAP requests from APs that are in its authorization list.

**Step 7** Provision the controller.

a) From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

b) Locate the controller that you want to provision.
c) Check the check box next to the device name.
d) From the **Actions** drop-down list, choose **Provision** > **Provision Device**.
e) In the **Assign Site** window, verify the assigned site, and click **Save**.
f) Click **Next**.
g) (Optional) On the **Configuration** window, under **NAT Address for Remote Teleworker**, click the **Enable NAT Address** check box and enter the NAT IP address.

**Note** Note that Catalyst Center does not support these addresses:

- IPv6 Documentation addresses: 2001:db8::/322
- IPv6 Site Local addresses: fec0::/103
- IPv6 Link Local addresses: fe80::/104
- IPv6 Loopback addresses: ::1
- IPv6 Multicast addresses: FF00::/8

h) Click **Next**.
i) In the **Feature Templates** window, click **Next**.
j) In the **Advanced Configuration** window, click **Next**.
k) In the **Summary** window, review the configuration settings, and click **Deploy**.
l) In the **Provision Device** slide-in pane, choose **Now**, and click **Apply**.

**Note** 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).

**Step 8** After the Cisco Wireless Controller is provisioned, you can provision the APs.

a) From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

b) Locate the APs that you want to provision.
c) Check the check box next to the device names.
d) From the **Actions** drop-down list, choose **Provision** > **Provision Device**.
e) In the **Assign Site** window, click **Choose a floor**, and assign the APs to a floor.
f) Click **Save**.
g) Click **Next**.
h) In the **Configuration** window, click **Next**.
i) In the **Summary** window, review the configuration settings, and click **Deploy**.
j) In the **Provision Device** slide-in pane, choose **Now**, and click **Apply**.