Wireless Network Configuration Use Cases

Wireless network configuration use case

Use these use cases to learn about wireless network configuration.

For information about optimal network management using wireless automation, see *Leveraging Cisco Catalyst Center Wireless Automation for Optimal Network Management*.

Wireless controller management use cases

These topics help you understand the wireless controller management use cases for wireless networks.

WLAN profile and policy profile configuration

Catalyst Center provides flexibility and intelligence when managing SSIDs across complex site hierarchies. Catalyst Center dynamically selects the WLAN profile and policy profile names from either network settings or network profiles based on the design intent and the specific site context.

SSID defined at Global site without override

When an SSID is defined at the Global site without any overrides at the site hierarchy, the WLAN profile and policy profile names are based on the network profile for that site.

Catalyst Center automatically detects conflicts when the same SSID is associated with the same WLAN profile and policy profile names but configured with different configuration flavors across multiple network profiles. For example, the SSID `store_wifi` with WLAN profile and policy profile name `store_wifi_area1` is defined

as Flex in the network profile attached to `Site1` and non-Flex in the network profile attached to `Site2`. If `Site1` and `Site2` are managed by the same wireless controller, it is a conflicting configuration.

To resolve conflicts, update each network profile to have unique WLAN profile and policy profile names. For example, update the network profile for `Site2` with the WLAN profile and policy profile name as `store_wifi_area1_site2`.

SSID overridden at child sites

When an SSID is overridden at child sites, Catalyst Center determines the WLAN profile and policy profile names based on either the network setting or network profile, based on these conditions:

Profile name selection	Criteria
From network settings	• WLAN profile and policy profile names in the network profile are the same as the names in the Global network settings. • The same WLAN profile or policy profile name is used across all network profiles under the overridden site.
From network profile	Multiple network profiles exist, each with a unique WLAN profile and policy profile name.

Catalyst Center automatically detects conflicts when the same SSID and WLAN profile or policy profile names are used with different configurations in two or more network profiles.

For example, a wireless controller manages a network with the SSID `store_wifi` and this hierarchy:

- Area1
  - Site1 (`store_wifi_area1`)
    - Building-01
      - Floor1
      - Floor2
  - Site2 (`store_wifi_area1`)
    - Building-02
      - Floor1
      - Floor2

This table lists the conflict configuration examples and resolutions.

Example	Resolution
The WLAN profile or policy profile name is `store_wifi_profile`. The SSID is defined as: • Flex configuration in `Site1` associated with `Network Profile-1` • Nonflex configuration in `Site2` associated with `Network Profile-2` The wireless controller detects a conflict as it manages both the sites.	Update each network profile to use a unique WLAN or policy profile name (for example, `store_wifi_area1_site2` for `Site2`).
The wireless controller manages only the buildings from the hierarchy using two network profiles, one for each floor. • `Network Profile-1` for first floors in each building using WLAN profile and policy profile name `store_wifi_area1_np1`. • `Network Profile-2` for second floors in each building using WLAN profile and policy profile name `store_wifi_area1_np2`. Overrides are configured at two sites but with same WLAN profile and policy profile name `store_wifi_area1`. Catalyst Center finds granular-level profile names at `Network Profile-1` and `Network Profile-2` under each overridden site (`Site1` and `Site2`). The wireless controller detects a conflict as the SSID is overridden at `Site1` and `Site2` with different configurations using the same WLAN profile and policy profile name `store_wifi_area1_np1`.	• Use a single network profile for all managed floors if there are no configuration differences at the network profile level. • Apply common configuration at the area-level network settings. • Create a network profile for each floor with unique WLAN profile and policy profile names.

WLAN profile or policy profile name modification

Catalyst Center automatically detects the migrated SSIDs when the wireless controller is reprovisioned without any intent change. Catalyst Center reuses the WLAN profile and policy profile name based on these conditions:

- The site level override is same as before migration.
- The WLAN profile or policy profile name is same as before migration in either the network profile or network settings.

These conditions are also applicable to non-migrated SSIDs which are created in Release 2.3.7.7 and reprovisioned with a WLAN profile or policy profile name change.

If you change the WLAN profile or policy profile name of an SSID at either the site hierarchy (**Network Settings** > **Wireless** > **SSID**) or the network profile and then reprovision the wireless controller, Catalyst Center tries to reuse the provisioned WLAN profile or policy profile names for a site if the SSID is already provisioned to the wireless controller for the same site with a WLAN profile or policy profile name that matches either the WLAN profile or policy profile name defined in the network profile or network settings. Catalyst Center ignores the updated profile name and continues to use the existing profile name.

For example, a wireless controller manages a network with the SSID `store_wifi` created at the Global level using WLAN profile or policy profile name `store_wifi_profile`. The network hierarchy under Global is:

- Area1
  - Site1

- Building-01
  - Floor1
  - Floor2
- Site2
  - Building-02
    - Floor1
    - Floor2

- Example 1:
  - The network profile `Network Profile-1` is assigned to all floors of `Site1/Building-01` with the WLAN profile or policy profile name `store_wifi_area1_np1`.
  - The network profile `Network Profile-2` is assigned to all floors of `Site2/Building-02` with the WLAN profile or policy profile name `store_wifi_area1_np2`.

  When you provision the wireless controller, the WLAN profile and policy profiles `store_wifi_area1_np1` and `store_wifi_area1_np2` are created on the wireless controller.

  To use a new WLAN profile or policy profile name (for example, `store_wifi_area1_np1_1`) for the sites using `Network Profile-1`, you can update the profile name in `Network Profile-1` and then reprovision the wireless controller. The new profile name is used. Similarly, if you change the profile name in `Network Profile-2` to `store_wifi_area1_np2_1` and reprovision the wireless controller, it uses the updated profile name.
- Example 2: A single network profile `Network Profile-1` with `store_wifi_profile` as the WLAN profile and policy profile names is used for all the floors.

  When you provision the wireless controller managing all the floors, the WLAN profile and policy profile `store_wifi_profile` is applied to all the floors.

  To update the WLAN profile or policy profile name used by the wireless controller, you must update the name in `Network Profile-1` and the SSID configuration in global network settings to ensure that the new profile name is correctly applied.

Wi-Fi 7 configuration use case

This section helps you understand the Wi-Fi 7 configuration use case for wireless networks.

Enable the Wi-Fi 7 configuration

Use this procedure to enable the Wi-Fi 7 configuration on Catalyst Center.

Before you begin

- Ensure that the Wi-Fi 7 APs are available in the **Provision** > **Inventory** window.

The Wi-Fi 7 APs include:

- Cisco Wireless 9171I Series Access Points running Cisco IOS XE Release 17.18 or later,
- Cisco Catalyst 9172H Series Access Points,
- Cisco Catalyst 9172I Series Access Points,
- Cisco Catalyst 9176D1 Series Access Points running Cisco IOS XE Release 17.17.1 or later,
- Cisco Catalyst 9176I Series Access Points running Cisco IOS XE Release 17.17.1 or later, and
- Cisco Catalyst 9178I Series Access Points.

- The devices must be running Cisco IOS XE Release 17.15.2 or later.
- Wi-Fi 7 APs use CNS licenses. If these APs don't meet the license requirements, they operate in worldwide safe mode (WWSM).

  To disable WWSM and meet the license requirements, enable the CNS licenses in the **License Manager** window. For more information, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 Enable the 802.11be status for the 2.4-GHz, 5-GHz, and 6-GHz radio bands in the **Dot11be Status Configuration** feature template.

You can use the existing default profiles or create custom profiles for each radio band. For more information, see Create a feature template for Dot 11be status configuration.

Step 2 Create an RF profile with the necessary settings and configure the required Wi-Fi 7 settings.

- Enable preamble puncturing using the **Preamble Puncturing** toggle button for the 5-GHz and 6-GHz radio bands.
- Use the **DBS Channel Width** slider to set the maximum channel width of 320 MHz for the 6-GHz radio band.
- Check the corresponding check box to enable the 802.11be parameters for the 6-GHz radio band.
  - Downlink OFDMA
  - Uplink OFDMA
  - Downlink MU-MIMO
  - Uplink MU-MIMO
  - OFDMA Multi-RU

Note
Starting with Cisco IOS XE Release 17.18.2, the OFDMA uplink, OFDMA downlink, MU-MIMO uplink, and MU-MIMO downlink configurations are deprecated and ignored under the **802.11BE PARAMETERS**. To configure these settings, use the **802.11AX PARAMETERS** section.

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

Step 3 Create a 802.11be profile.

- Configure the 802.11be settings for the 2.4-GHz and 5-GHz radio bands.

  Note
  This 802.11be profile is mapped to the WLAN and applies to only the 2.4-GHz and 5-GHz radio bands. The 802.11be configuration for the 6-GHz radio band is used from the corresponding settings in the RF profile.

- Configure the MLO group settings for all radio bands.

For more information, see Create an 802.11be profile.

Step 4 In the associated wireless network profile,

- Associate the 802.11be profile with the corresponding SSID in the network profile (for more information, see Add SSIDs to a network profile) and
- Add the **Dot11be Status Configuration** feature template to the network profile (for more information, see Add feature templates to a network profile).

Step 5 (Optional) In the corresponding SSID, check the **AP Beacon Protection** check box to enable AP beacon protection.

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

Step 6 Configure the Wi-Fi 7 APs.

For more information, see Configure APs.

Step 7 Provision the Wi-Fi 7 APs with the associated network profile.

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

High availability use cases

These topics help you understand the high availability (HA) use cases for wireless networks.

Configure Cisco Wireless Controller HA

Cisco Wireless Controller HA allows you to use a wireless controller as a backup for a primary wireless controller. The active wireless controller handles all the APs, client traffic, and shares the AP and client database with the standby wireless controller. If there is a failover, the standby wireless controller takes over immediately, resulting in zero client service downtime and zero SSID outage.

Before you begin

- Ensure that both the wireless controllers are of the same form factors.
- Ensure that both the wireless controllers are running the same software version.
- Wireless controller HA supports a maximum redundancy port link latency of 80 ms round-trip time (RTT), minimum bandwidth of 60 Mbps, and minimum maximum transmission unit (MTU) of 1500.

- Ensure that you connect the redundancy ports of both the wireless controllers physically or through a Layer 2 virtual network. If you connect redundancy ports through a Layer 2 virtual network, ensure that the link latency, bandwidth, and MTU requirements are met.
- For the Cisco Catalyst 9800-CL Wireless Controllers running on ESXi, KVM, and Hyper-V, ensure that the redundancy port connects to the same vswitch.

Procedure

Step 1 Ensure that you have the wireless controller in your inventory. For more information, see About Inventory and Add a network device.

If the wireless controller isn't available in the inventory, use the Discovery feature to discover it. For more information, see Discover Your Network.

Step 2 Ensure that both the wireless controllers are in the **Managed** state in the inventory. For more information, see Display information about your inventory.

Step 3 Use the **show redundancy** command to verify that the operating redundancy mode is **Non-redundant** on both the wireless controllers.

Step 4 From the main menu, choose **Provision** > **Inventory**.

Step 5 Check the check box next to the required wireless controller, and then click **Actions** > **Provision** > **Configure WLC HA**.

Step 6 Enter the **Redundancy Management IP** and the **Peer Redundancy Management IP** addresses.

You must configure the IP addresses used for redundancy management IP and peer redundancy management IP 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 7 Enter the **Netmask**.

Step 8 From the **Select Secondary WLC** drop-down list, choose the secondary wireless controller.

Step 9 Since the Cisco Catalyst 9800-CL Wireless Controller doesn't have a dedicated redundancy port, choose the interface that will be used for the redundancy port.

Note
Appliance-based Cisco Catalyst 9800 Series Wireless Controllers have dedicated redundancy ports, and redundancy port interface selection isn't necessary for these devices.

Step 10 Click **Configure HA**.

What to do next

To verify the status of HA, use the **show redundancy** command. This is a sample output of the command:

```
  cat_9800-1 #show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 5 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
              Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 5 minutes
                 Image Version = Cisco IOS Software [Bengaluru], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.6.3, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed [redacted] 23:13 by [redacted]
        Configuration register = 0x2102
               Recovery mode   = Not Applicable

Peer Processor Information :
----------------------------
              Standby Location = slot 2
        Current Software state = STANDBY HOT
       Uptime in current state = 3 minutes
                 Image Version = Cisco IOS Software [Bengaluru], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.6.3, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed [redacted] 23:13 by [redacted]
                       BOOT =
                  CONFIG_FILE =
        Configuration register = 0x2102
```

To verify the **Priority** of the primary wireless controller, use the **show chassis** command. The **Priority** of the primary wireless controller is changed to 2 to ensure that its role is **Active**. This is a sample output of the command:

```
  cat_9800-1 #show chassis
Chassis/Stack Mac Address : 000c.2972.9b46 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
-----------------------------------------------------------------------------------------
*1       Active   000c.2972.9b46     2      V02     Ready               172.16.0.2
 2       Standby  0050.56ae.a54f     1      V02     Ready               172.16.0.3
```

Configure Cisco Wireless Controller N+1 HA

Cisco Wireless Controller N+1 HA allows you to use a wireless controller as a backup for multiple primary wireless controllers. Catalyst Center doesn't support stateful switchover for N+1 HA and each wireless controller must be managed separately.

Note

- Catalyst Center supports N+1 HA configurations for primary and secondary wireless controllers. Catalyst Center doesn't support tertiary wireless controller configurations.
- If you edit the primary wireless controller configuration, reprovision the secondary wireless controller manually with the updated configurations.

Procedure

Step 1 Ensure that you have the wireless controller in your inventory. For more information, see About Inventory and Add a network device.

If the wireless controller isn't available in the inventory, use the Discovery feature to discover it. For more information, see Discover Your Network.

Step 2 Ensure that both the wireless controllers are in the **Managed** state in the inventory. For more information, see Display information about your inventory.

Step 3 Create enterprise and guest wireless SSIDs. For more information, see Create SSIDs for an enterprise wireless network and Create SSIDs for a guest wireless network.

Step 4 If you created a wireless network profile during SSID creation, assign it to the primary wireless controller-managed site. From the main menu, choose **Design** > **Network Profiles**, and then click the corresponding **Assign Site** option for the wireless network profile.

Step 5 Provision the primary wireless controller. Choose the role as **Active Main WLC**. For more information, see Provision a Cisco AireOS Controller and Provision a Cisco Catalyst 9800 Series Wireless Controller.

Step 6 Provision the secondary wireless controller. Choose the role as **Active Main WLC** and choose the secondary managed AP location same as the managed AP location for the primary wireless controller. For more information, see Provision a Cisco AireOS Controller and Provision a Cisco Catalyst 9800 Series Wireless Controller.

Step 7 Provision the APs. For more information, see Provision Cisco APs on day 1.

Wireless mobility use cases

These topics help you understand the mobility configuration use cases for wireless networks.

Configure wireless mobility

Mobility configuration in Catalyst Center allows you to establish a tunnel between Cisco Wireless Controllers in a network allowing them to communicate with each other and dynamically share information. The mobility tunnel enables seamless roaming of clients within a wireless network. This procedure describes the steps to configure a mobility tunnel between wireless controllers for these use cases:

- Two newly added wireless controllers with the same mobility group: The two wireless controllers are newly added to Catalyst Center and are not yet provisioned.
- Two existing wireless controllers with the same mobility group: The wireless controllers are already added and provisioned on Catalyst Center and have the same mobility group name.
- Two existing wireless controllers with different mobility group: The wireless controllers are already added and provisioned on Catalyst Center and have different mobility group name.
- Two existing wireless controllers with a third wireless controller: Adding a new wireless controller to an existing mobility group between two wireless controllers.

Before you begin

- Ensure that you have the Cisco Wireless Controllers in your inventory and they are in **Managed** state. For more information, see About Inventory and Display information about your inventory.
- For more information on wireless mobility configuration, see Mobility configuration overview.

Procedure

Step 1 For newly added wireless controllers with the same mobility group, do these steps:

a) Run the **show wireless mobility summary** command to verify that there's no existing mobility tunnel between the controllers.

b) Choose one of the wireless controllers and configure the mobility group, adding the other wireless controller as the peer. For more information, see Configure mobility group.

c) Verify the configurations before provisioning.

d) Provision the wireless controller.

Note
You don't have to provision the second wireless controller. Adding it as a peer for the first wireless controller automatically provisions it with the same mobility group name and peer configurations.

Step 2 For two existing wireless controllers with same mobility group, do these steps:

a) Verify that the wireless controllers have the same mobility group name configured. For more information, see About Inventory and Display information about your inventory.

b) Choose one of the wireless controllers and configure the mobility group, adding the other wireless controller as the peer. For more information, see Configure mobility group.

c) Verify the configurations before provisioning.

d) Provision the wireless controller.

Note
You don't have to provision the second wireless controller. Adding it as a peer for the first wireless controller automatically provisions it with the same mobility group name and peer configurations.

Step 3 For two existing wireless controllers with different mobility group, do these steps:

a) Verify that the wireless controllers have the mobility group name configured. For more information, see About Inventory and Display information about your inventory.

b) Choose one of the wireless controllers and configure the mobility group, adding the other wireless controller as the peer. For more information, see Configure mobility group.

c) Verify the configurations before provisioning.

d) Provision the wireless controller.

Note
You don't have to provision the second wireless controller. Adding it as a peer for the first wireless controller automatically provisions it with the same mobility group name and peer configurations.

Step 4 For adding a new wireless controller to an existing mobility group between two wireless controllers, do these steps:

a) Verify that the existing wireless controllers have the mobility tunnel established between them by checking the mobility group name and the mobility peer information in the **Mobility** tab. For more information, see About Inventory and Display information about your inventory.

b) Choose the newly added wireless controller and configure the mobility group, adding the other two existing wireless controllers as peers. For more information, see Configure mobility group.

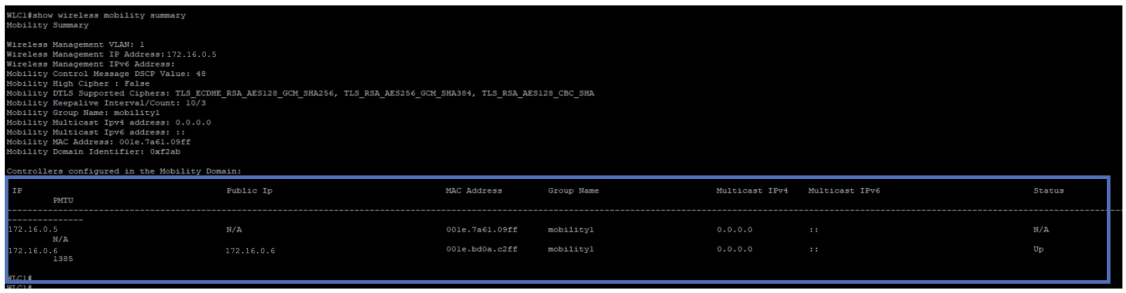
c) Verify the configurations before provisioning.

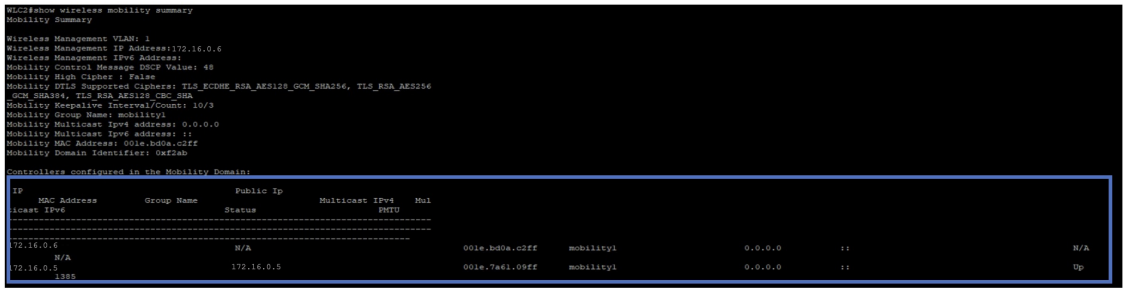
d) Provision the wireless controller.

Note
You don't have to provision the existing two wireless controllers. Adding them as a peer for the newly added wireless controller automatically provisions it with the same mobility group name and peer configurations.

What to do next

After provisioning, run the **show wireless mobility summary** command on each of the controllers to verify the mobility tunnel status. This is a sample output of the command:





Configure anchor and foreign wireless mobility

The anchor and foreign wireless configuration on Catalyst Center allows you to establish wireless mobility between Cisco Wireless Controllers on different wireless networks. In an anchor and foreign setup, the foreign wireless controller encapsulates the client L3 traffic in the mobility tunnel and forwards it to the anchor wireless controller. The anchor wireless controller decapsulates the tunnel and switches the client traffic. This procedure describes the steps to configure anchor/foreign wireless mobility for these use cases:

- Configuring two newly added wireless controllers - one anchor and one foreign wireless controller.
- Configuring three newly added wireless controllers - one anchor and two foreign wireless controllers.
- Configuring three newly added wireless controllers - one foreign and two anchor wireless controllers.
- Deleting the anchor/foreign setup.

Before you begin

- Ensure that you have the Cisco Wireless Controllers in your inventory and they are in **Managed** state. For more information, see About Inventory and Display information about your inventory.

- Use the **show wireless mobility summary** command to verify that there's no existing mobility tunnel between the wireless controllers.

Procedure

Step 1 Create an SSID for the wireless network and associate it with a new wireless network profile. For more information, see Create SSIDs for an enterprise wireless network or Create SSIDs for a guest wireless network.

In the **Associate SSID to Profile** step, choose the **Add Profile** option and complete this configuration:

- **Profile Name**: Enter a name for the profile.
- **Fabric**: Choose **No**.
- **Do you need Anchor for this SSID?**: Choose **Yes**.

Step 2 For a scenario with one anchor and one foreign wireless controller, do these steps:

a) Assign the newly created wireless profile to the site managed by the foreign wireless controller.

To assign a site:

- From the main menu, choose **Design** > **Network Profiles**
- Choose the profile and click **Assign Site**. For information on creating sites, see Create, edit, and delete a site.

b) Provision the anchor wireless controller.

- Choose the wireless controller role as **Anchor WLC** and select the anchor **Managed AP location(s)**.
- Configure the interface details.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

c) Provision the foreign wireless controller.

- Choose the wireless controller role as **Active Main WLC** and select the **Managed AP location(s)**.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

d) Provision the APs under the wireless controllers.

Ensure that APs have the correct SSID. For more information on AP provisioning, see Provision Cisco APs on day 1.

Step 3 For a scenario with one anchor and two foreign wireless controllers, do these steps:

a) Assign the newly created wireless profile to the sites managed by the foreign wireless controllers.

- From the main menu, choose **Design** > **Network Profiles**
- Choose the profile and click **Assign Site**. For information on creating sites, see Create, edit, and delete a site.

b) Provision the anchor wireless controller.

- Choose the wireless controller role as **Anchor WLC** and select the **Managed AP location(s)** (select both foreign sites).
- Configure the interface details.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

c) Provision the foreign wireless controllers.

- Choose the wireless controller role as **Active Main WLC** and select the **Managed AP location(s)**.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

d) Provision the APs under the wireless controllers.

Ensure that APs have the correct SSID. For more information on AP provisioning, see Provision Cisco APs on day 1.

Step 4 For a scenario with one foreign and two anchor wireless controllers, do these steps:

a) Assign the newly created wireless profile to the sites managed by both wireless controllers (foreign and anchor).

- From the main menu, choose **Design** > **Network Profiles**
- Choose the profile and click **Assign Site**. For information on creating sites, see Create, edit, and delete a site.

b) Provision the foreign wireless controller.

- Choose the wireless controller role as **Active Main WLC** and select the **Managed AP location(s)** (select both foreign and anchor sites).
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

c) Provision the anchor wireless controllers.

- Choose the wireless controller role as **Anchor WLC** and select the **Managed AP location(s)**.
- Configure the interface details.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

d) Provision the APs under the wireless controllers.

Ensure that APs have the correct SSID. For more information on AP provisioning, see Provision Cisco APs on day 1.

What to do next

After provisioning, Catalyst Center automatically creates a mobility tunnel between the anchor and foreign wireless controllers. Use the **show wireless mobility summary** command on each of the controllers to verify the mobility tunnel status. This is a sample output of the command:

```
WLC2#show wireless mobility summary
Mobility Summary

Wireless Management VLAN: 1
Wireless Management IP Address:172.16.0.7
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384, TLS_RSA_AES128_CBC_SHA
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.bd0a.c2ff
Mobility Domain Identifier: 0x34ac

Controllers configured in the Mobility Domain:
IP                                      Public Ip                               MAC Address       Group Name                      Multicast IPv4   Multicast IPv6                          Status
        PMTU
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
172.16.0.7                              N/A                                     001e.bd0a.c2ff    default                         0.0.0.0          ::                                      N/A
        N/A
172.16.0.8                              172.16.0.8                              001e.e657.ddff    default                         0.0.0.0          ::                                      Up
        1385
```

```
WLC3-Anchor#show wireless mobility summary
Mobility Summary

Wireless Management VLAN: 1
Wireless Management IP Address:172.16.0.8
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384, TLS_RSA_AES128_CBC_SHA
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.e657.ddff
Mobility Domain Identifier: 0x34ac

Controllers configured in the Mobility Domain:
IP                                      Public Ip                               MAC Address       Group Name                      Multicast IPv4   Multicast IPv6                          Status
        PMTU
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
172.16.0.8                              N/A                                     001e.e657.ddff    default                         0.0.0.0          ::                                      N/A
        N/A
172.16.0.7                              172.16.0.7                              001e.bd0a.c2ff    default                         0.0.0.0          ::                                      Up
        1385
```

Verify these mobility configurations on the wireless controllers:

- Both wireless controllers have the same WLAN and policy profile.
- The policy tag is created on foreign wireless controller and mapped to the AP.
- The VLAN interface is created for the anchor wireless controller and is mapped to the policy profile.

Delete the anchor/foreign setup

To delete the anchor and foreign setup, do these steps:

1. Ensure that the mobility tunnel between the anchor and foreign wireless controllers is in *up* state.
2. Delete the SSID that was created for the wireless network.
   a. From the main menu, choose **Design** > **Network Settings**
   b. Click the **Wireless** tab.
   c. From the left hierarchy tree, choose **Global**.
   d. In the **SSID** table, choose the SSID and click **Delete**.
3. Provision the foreign wireless controllers.

In the provision **Summary** window, ensure that the SSID details are removed.

After provisioning, Catalyst Center automatically deletes the mobility tunnel between the anchor and foreign wireless controllers and the WLAN and policy profile is deleted on all the wireless controllers.

AP management use cases

These topics help you understand the AP management use cases for wireless networks.

AP configuration

You can do these tasks for APs in Catalyst Center:

- Configure AP-level parameters and radio-level parameters for APs.
- Schedule recurring events for APs.
- Configure APs using existing templates.

For more information, see AP configurations in Catalyst Center.

AP refresh

You can replace old AP models with new AP models using Catalyst Center. You can replace both provisioned and unprovisioned old APs with new ones in Catalyst Center. For more information, see AP Refresh workflow.

Skip AP provision during Cisco Catalyst 9800 Series Wireless Controller provisioning

When you provision a wireless controller for the first time, Catalyst Center also provisions the associated APs. When you reprovision the wireless controller, Catalyst Center detects if there are any changes to these AP intent configurations:

- VLAN configurations: local VLAN, native VLAN, and AAA VLAN.
- Tag configurations: policy tag, site tag, AP profile name, flex profile name, and site tag load count.
- Failed AP wireless configuration parameters from the previous provisioning attempts.

If there are no changes to these AP intent configurations, Catalyst Center skips the provisioning of associated APs. If there are changes to the AP intent configurations, you can use the **Skip AP Provision** option to skip the AP provisioning during wireless controller reprovisioning. If you check the **Skip AP Provision** check box, Catalyst Center doesn't reprovision the existing APs and the APs managed by the wireless controller. However, the newly added APs are provisioned.

The selective AP group Resource Facing Service (RFS) translate feature optimizes wireless controller reprovisioning for AP-related configurations (such as AP tag mapping, RF tags, and flex or RF profiles) by translating only the AP intent that has changed. Out-of-band AP 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 tag mapping:

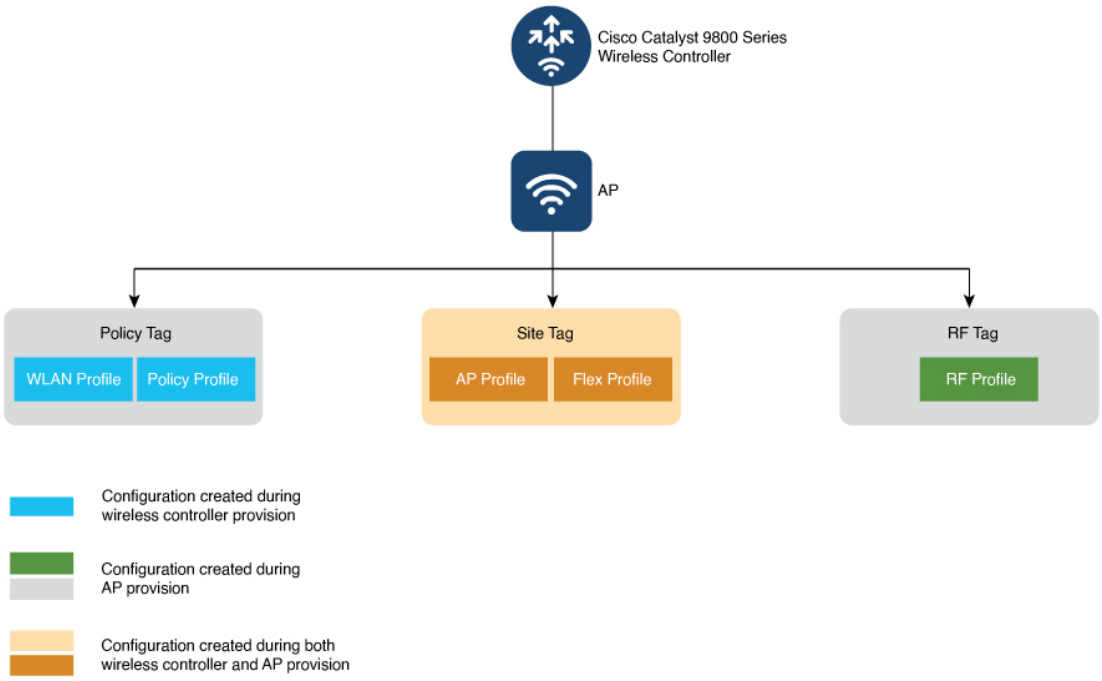
- With resynchronization and compliance run, the manual change is corrected to match the intent configuration.
- Without resynchronization and compliance run, the manual change is not corrected and only the new intent changes are applied.

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

Catalyst Center uses policy tags, site tags, and RF tags to push the wireless network configurations to individual APs through Cisco Catalyst 9800 Series Wireless Controllers.

For the first-time provisioning, Catalyst Center configures both the custom and Catalyst Center-generated site tags, policy tags, and RF tags only during the AP provisioning. For more information about the tag and flex profile configurations, see Overview of AP groups, flex groups, site tags, and policy tags.

This figure shows how Catalyst Center processes the tags.



For information about the tags on the wireless controller, see Understand Catalyst 9800 Wireless Controllers Configuration Model.

This table lists the tags and the associated tag information during the first-time provisioning of wireless controller and APs:

Tag	Design window	Wireless Controller provision (with the Skip AP Provision unchecked)	AP provision
Policy tag	**Design** > **Network Settings** > **Wireless** > **SSIDs**	Autogenerated names for WLAN profile and policy profile are created.	Policy tags with the required WLAN profiles are created.
Site tag	AP profile: **Design** > **Network Settings** > **Wireless** > **AP Profiles** Custom site tag and flex profile: **Design** > **Network Profiles** > **Add Profile** > **Wireless** > **Advanced Settings** > **Provision Group**	For nonflex configurations, an AP profile mapped to the custom site tag is created. **Note** The site tag is created and associated with the AP profile during AP provisioning.	For nonflex: • Site tags are created. • Nondefault AP profile is generated for ROW APs. • Nondefault AP profile is generated for mesh and OEAP sites.
		For flex configurations, intent configurations defined in the feature template with **IP Overlap** enabled and native VLAN configurations are created.	For flex, a nondefault flex profile is created.
RF tag	**Design** > **Network Settings** > **Wireless** > **RF Profiles**	No change	RF tag and RF profiles are created.

This table lists the tags and the associated tag information during the wireless controller and AP reprovisioning when there are changes to the AP intent configurations:

Tag	Design window	Wireless Controller provision (with the Skip AP Provision unchecked)	AP provision
Policy tag	**Design** > **Network Settings** > **Wireless** > **SSIDs**	• WLAN profile and policy profile mappings are configured. • Updates to policy tags are configured for the provisioned APs. • Updates to the policy tag name are configured for the provisioned APs.	• Policy tags with the required profiles are configured. • Updates to the policy tag name are configured.

Tag	Design window	Wireless Controller provision (with the Skip AP Provision unchecked)	AP provision
Site tag	AP profile: **Design** > **Network Settings** > **Wireless** > **AP Profiles** Custom site tag and flex profile: **Design** > **Network Profiles** > **Add Profile** > **Wireless** > **Advanced Settings** > **Provision Group**	Updates to site tags are configured for the provisioned APs.	Site tag, flex profile, and AP profile are created or configured.
RF tag	**Design** > **Network Settings** > **Wireless** > **RF Profiles**	Updates to the RF profile are configured.	RF tags are configured.

Note If there are no provisioned APs on a floor, tags aren't configured on the floor during the wireless controller reprovisioning.

Automated tagging for flapping APs

Catalyst Center supports automated tagging for flapping APs. When an AP flaps more than 10 times in 6 minutes, Catalyst Center assigns the AUTO_INV_EVENT_SYNC_DISABLED tag to the AP automatically. When the AP is assigned with this tag, any event on that AP is discarded. This tag prevents the unnecessary wireless controller synchronization to update the AP information for flapping APs.

If this AP doesn't flap for 10 minutes, Catalyst Center removes the AUTO_INV_EVENT_SYNC_DISABLED tag automatically.

You can view the logs for the tagging and untagging of APs on the **Audit Logs** window.

After the underlying cause of the AP flapping is resolved, we recommend that you perform a manual synchronization to immediately reflect the most current AP details. Alternatively, wait for the next scheduled synchronization to update the AP information.

Configure ROW APs

Use this procedure to configure the Rest of World (ROW) domain APs.

Procedure

Step 1 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.

Note

If you don't create an AP profile, Catalyst Center automatically generates the AP profile with the country code of the selected site and site tags for the ROW AP during AP provisioning or AP PnP onboarding.

Step 2 Add support for the country of operation to the country list on the wireless controller. You must configure at least one site from the country of operation as the managed AP location for the wireless controller. For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller.

Step 3 If the wireless controller is not already provisioned with the configurations in Step 1, on page 18 and Step 2, on page 19, provision the wireless controller. For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller.

Step 4 Configure the AP parameters. For more information, see Configure APs.

Step 5 Provision the AP. For more information, see Provision Cisco APs on day 1.

Note
Onboarding a ROW AP to a site with existing APs may disrupt the services of the existing APs for a brief period.

What to do next

To verify the AP configuration, use the **show ap summary** command. This is a sample output of the command.

```
C9800LC-94#show ap summary
Number of APs: 4

CC = Country Code
RD = Regulatory Domain

AP Name                          Slots AP Model           Ethernet MAC   Radio MAC      CC   RD   IP Address                                 State       Location
-------------------------------------------------------------------------------------------------------------------------------------------------------------
AP68-C9130I-0D40                 3     C9130AXI-B         3c41.[redacted] 1416.[redacted] IN   -B   [redacted]                                 Registered  Texas
C9130AXI-8A40                    3     C9130AXI-D         548a.[redacted] 488b.[redacted] IN   -D   [redacted]                                 Registered  DEFAULT
C9136I-E1F4                      4     C9136I-ROW         4891.[redacted] 6cd6.[redacted] IN   -RW  [redacted]                                 Registered  DEFAULT
C9115AXI-4AD4                    2     C9115AXI-D         6c41.[redacted] a4b4.[redacted] IN   -D   [redacted]                                 Registered  DEFAULT
```

This command displays the country code (CC) and regulatory domain (RD) for the APs. For ROW APs, the regulatory domain is **-RW**.

Note For a ROW AP, if the country code in the command output is **--**, it indicates that the country code is not available for the AP. The operational status of all the radios for the ROW APs without a country code is **down**. You must provision the ROW AP to configure the country code for the ROW AP.

Configure wireless mesh network

In a Cisco wireless mesh network architecture, APs operate in one of these ways:

- Root APs (RAP): Connected to the wired network.
- Mesh APs (MAP): Communicates with other MAPs and RAPs using wireless connections.

The workflow for configuring a wireless mesh network involves these main steps:

1. Wireless controller provisioning: Configure a mesh profile, configure the AP authorization list and provision the wireless controller.
2. AP configuration: Configure AP in bridge mode and deploy.
3. AP provisioning: Configure the mesh role for AP (RAP or MAP) and provision the AP.

Before you begin

All APs are configured and shipped as MAPs. To use the AP as a RAP, you must reconfigure it as a RAP during AP provisioning. A mesh network must contain at least one RAP. For more information on Cisco Wireless Controller configuration and AP configuration for wireless mesh networks, see About wireless mesh networks.

Procedure

Step 1 In the Catalyst Center device inventory (**Provision** > **Inventory**), ensure that the wireless controllers and APs are in managed state and assigned to the respective sites.

Step 2 Create an AP profile with mesh settings. For more information, see Configure mesh settings for an AP profile for Cisco IOS XE devices and Configure mesh settings for an AP profile for Cisco AireOS devices.

Step 3 Add the AP Ethernet MAC address to the AP authorization list. For more information, see Create an AP authorization list.

Step 4 Provision the Cisco Wireless Controller. For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller and Provision a Cisco AireOS Controller.

In the provision configuration window, select the **AP Authorization List** defined in Step 3 and choose the option for authorizing only the mesh access points.

Step 5 (Optional) In the **Configure Access Points** workflow, select the APs and change the AP mode to **Bridge/Flex+Bridge** mode if they are in **Local/Flexconnect** mode. For more information, see Configure APs.

Step 6 Provision the APs. For more information, see Provision Cisco APs on day 1.

- For RAPs, choose the **Mesh Role** as **RAP (Root AP)**.
- For MAPs, choose the **Mesh Role** as **MAP (Mesh AP)**.

What to do next

You can verify the mesh configurations on the Cisco Wireless Controller using these commands:

- AP Ethernet MAC address: **show run | inc username**.
- AP mesh role (MAP/RAP) after provisioning: **show wireless mesh ap summary**.
- Site tag details: **show wireless tag site detailed <site tag name>**.
- AP profile: **show run | section ap profile**.
- Wireless mesh configurations:
  - **show wireless profile mesh summary**
  - **show wireless profile mesh detailed <mesh profile name>**

AP migration from a wireless controller to another wireless controller

You can migrate APs from one wireless controller to another wireless controller with the same floors in the network hierarchy. For more information, see Migrate APs from a Wireless Controller to another Wireless Controller.

AP replacement using RMA workflow

You can replace a faulty access point in the network using the Catalyst Center Return Material Authorization (RMA) feature. The RMA workflow lets you replace failed devices quickly, thus improving productivity and reducing operational expense. For wireless APs, the replacement device is assigned to the same site, provisioned with primary wireless controller, RF profile, and AP group settings, and placed on the same floor map location in Catalyst Center as the failed AP.

For more information, see Replace a faulty access point.

Onboard APs using PnP for non-intent-based deployments

Use this procedure to onboard and provision APs using Plug and Play (PnP) for deployments that:

- do not use intent-based configurations and
- are not provisioned with a network profile from Catalyst Center

The non-intent-based configurations include the Assurance use case and Per-Device Configurations.

Before you begin

- Ensure that the Cisco Catalyst 9800 Series Wireless Controller is added to the inventory.
- Configure the DHCP server with Option 43 for PnP. This option informs the network device of the IP address of the Catalyst Center controller.
- Ensure that the APs are in the factory reset state.
- Ensure the network connectivity between APs, Catalyst Center, and wireless controller.

Procedure

Step 1 Create a regular day-zero template for onboarding APs using PnP.

a) Use these configurations:

- Template Name: Enter a name for the template
- Project Name: **Onboarding Configuration**
- Deployment Type: **Day 0**
- Template Language: **Jinja**
- Software Type: **IOS-XE**
- Device Family: **Wireless Controller**

- Device Model: **Cisco Catalyst 9800 Wireless Controllers**

For more information, refer to Create a regular template.

b) Add these configurations in the template, save, and commit the changes:

- Primary wireless controller IP address
- Primary wireless controller name
- Secondary wireless controller IP address
- Secondary wireless controller name
- Policy tag name
- Site tag name
- RF tag name

For more information, refer to Edit templates.

Catalyst Center pushes these configurations to APs during PnP claim.

For example, add these configurations in the template:

```
{
  "primaryWlcIP": "10.0.0.1",
  "primaryWlcName": "Primary-WLC",
  "secondaryWlcIP": "10.0.0.5",
  "secondaryWlcName": "Secondary-WLC",
  "policyTagName": "default-policy-tag",
  "siteTagName": "default-site-tag",
  "RFTagName": "default-rf-tag"
}
```

Step 2 Claim the APs using PnP.

a) Do not assign the APs to a site.

b) Select the day-zero template that you created for AP onboarding.

For more information, refer to Provision a wireless controller.

After PnP claim, the configuration is pushed to AP and it joins the corresponding wireless controller. The AP appears in the inventory.

What to do next

In the AP console, use the **show pnp log** to verify the PnP claim. A sample output of the command is:

```
#show pnp log
722 - pnp.agent - DEBUG - Setting sid from stored value 551de96a-c719-44f0-8964-16b150f7325d
APC414.A2FB.0CB0#
PNP CONFIG - HOST NAME   : APC414.A2FB.0CB0
PNP CONFIG - PRI WLC IP  : 10.0.0.1
PNP CONFIG - SEC WLC IP  : 10.0.0.5
PNP CONFIG - PRI WLC NAME: Primary-WLC
PNP CONFIG - SEC WLC NAME: Secondary-WLC
PNP CONFIG - Policy Tag  : default-policy-tag
PNP CONFIG - Site Tag    : default-site-tag
```

```
PNP CONFIG - RF Tag      : default-rf-tag
PnP: Config Upgrade received. Start CAPWAP discovery
```

Campus networks configuration use cases for Cisco Catalyst 9800 Series Wireless Controllers

Catalyst Center can learn configurations from an existing Cisco Catalyst 9800 Series Wireless Controller and save the configurations as configuration profiles. Configuration profiles can be learned from wireless controllers that are provisioned using either Per-Device Configurations, provisioned using intent-based network configurations, or available in the inventory without being provisioned. You can provision multiple wireless controllers using configuration profiles, ensuring consistent settings and standardized deployment.

Note This feature is in beta and requires feature enablement. To enable the feature, contact Cisco TAC. If this feature is not enabled, the options for wireless controller-related configurations are unavailable or dimmed.

Configuration profiles are version-specific. The profiles learned from a wireless controller running a specific Cisco IOS XE Release can be applied only to wireless controllers running the same version. Configuration profiles are not associated with site or network and can be used across different networks.

For more information about campus networks, refer to Provision Campus Networks.

Prerequisites

- Wireless controllers must be running Cisco IOS XE Release 17.12 or later.
- Per-Device Configurations must be enabled on the wireless controllers included in the campus network. For more information, refer to Enable Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller.
- Wireless controllers and APs must be added to inventory and assigned to the required sites.

Standardize complete configuration for wireless controllers on day zero

Ensure uniform initial configuration for all wireless controllers in your network by copying device configurations from an existing wireless controller and standardizing the setup.

Before you begin

Refer to Campus networks configuration use cases for Cisco Catalyst 9800 Series Wireless Controllers, on page 23.

Use this procedure to copy the configurations from a wireless controller and apply them to all other wireless controllers in your network to ensure uniform day-zero configurations.

Procedure

Step 1 Create a network and add the wireless controllers that need to be included in the network.

For information about creating a network with wireless controllers, refer to Create a network.

Step 2 Learn configuration profiles from an existing wireless controller.

For more information, refer to Learn configuration profiles from a wireless controller.

Step 3 Standardize the configuration for wireless controllers in the network.

a) Assign the configuration profiles to the required wireless controllers, resolve any validation errors that impact provisioning, and schedule the provisioning.

For more information, refer to Assign configuration profiles to a wireless controller.

Note
Ensure that the wireless controller is running the same Cisco IOS XE Release as the wireless controller from which configuration profile is learned.

b) (Optional) Edit the configuration profile assignment for wireless controllers.

For more information, refer to Edit configuration profile assignment for a wireless controller.

Step 4 Verify that the configuration is pushed to the wireless controllers.

a) From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.
b) Click the network name to view network details.
c) Click the **Devices** tab.
d) Click **wireless controllers**.
e) Click the device name.
f) In the **Sync Status** column, verify that the status is **In Sync** for the wireless controller.

Step 5 Configure the tags (site tag, policy tag, and RF tag) for APs associated with the wireless controllers using Per-Device Configurations.

For more information, refer to Manage APs associated with a Cisco Catalyst 9800 Series Wireless Controller.

Standardize partial configuration for wireless controllers on day zero

Apply and customize partial configuration profiles for wireless controllers, ensuring only required configurations are provisioned during initial deployment.

Use this procedure to customize configuration profiles learned from existing wireless controllers. For example, if a learned profile includes ten SSIDs but only two are needed for a site, modify the profile to match site requirements.

Before you begin

Refer to Campus networks configuration use cases for Cisco Catalyst 9800 Series Wireless Controllers, on page 23.

Procedure

Step 1 Create a network and add the wireless controllers that need to be included in the network.

For information about creating a network with wireless controllers, refer to Create a network.

Step 2 Learn configuration profiles from an existing wireless controller.

For more information, refer to Learn configuration profiles from a wireless controller.

Step 3 Standardize the partial configuration for the required wireless controllers in the network.

a) Duplicate the configuration profile for wireless profiles.

For more information, refer to Manage configuration profiles.

b) (Optional) Edit or delete the configurations in the duplicated profile as needed.

For information about editing or deleting a configuration profile for the wireless controller, refer to Manage configuration profiles.

For example, if you want to use only two out of ten SSIDs in the configuration profile, delete the eight SSIDs that you do not need.

c) Assign the configuration profiles to the required wireless controllers, resolve any validation errors that impact provisioning, and schedule the provisioning.

For more information, refer to Assign configuration profiles to a wireless controller.

Step 4 Verify that the configuration is pushed to the wireless controllers.

a) From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.
b) Click the network name to view network details.
c) Click the **Devices** tab.
d) Click **wireless controllers**.
e) Click the device name.
f) In the **Sync Status** column, verify that the status is **In Sync** for the wireless controller.

Manage configurations for a wireless controller on day *n*

Maintain, update, or remove configurations for wireless controllers by updating configuration profiles.

Use this procedure to add, edit, or delete a setting in a configuration profile for a wireless controller on day n. For example, use this procedure to create an SSID for Wi-Fi 7 clients.

Procedure

Step 1 Manage your configurations in the configuration profile.

a) Edit or delete configurations in the configuration profile for the wireless profile as needed.

For information about editing or deleting a configuration profile for the wireless controller, refer to Manage configuration profiles.

For example, click **Add** in the **WLAN Profiles** table to add an SSID for Wi-Fi 7. After you create the SSID, map it to the policy tag.

The **Sync Status** for the wireless controller (refer to Step 2, on page 26) changes to **Out of sync** as the configuration profile that is already assigned and provisioned on the wireless controller is modified.

b) Verify your updated configurations, resolve any validation errors that impact provisioning, and reprovision the wireless controller with the updated configuration profile.

The **Change type** column identifies the status of each configuration during provisioning. This column displays **Modify** for existing configurations that have been updated, **Add** for newly created configurations, and **No changes** for configurations that are already synchronized and not updated.

For more information, refer to Edit configuration profile assignment for a wireless controller.

Step 2 Verify that the configuration is pushed to the wireless controllers.

a) From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.
b) Click the network name to view network details.
c) Click the **Devices** tab.
d) Click **wireless controllers**.
e) Click the device name.
f) In the **Sync Status** column, verify that the status is **In Sync** for the wireless controller.