Provision Wireless Devices

Wireless Device Provisioning Overview

The following 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.

Cisco DNA 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, Cisco DNA 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, Cisco DNA 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 Dynamic Channel Assignment (DCA) channels configured on the RF profile, only the supported channels as per the country code are considered. You can see the list of unsupported DCA channels in the AP preprovision summary step of the AP provision workflow on Cisco DNA 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.

Visibility and Control of Wireless Device Configurations

The Visibility and Control of Configurations feature provides a solution to further secure your planned network configurations before deploying them onto your devices. With enhanced visibility, you can enforce the previewing of device configurations (CLI and NETCONF commands) before deploying them. With enhanced control, you can ensure only authentic and authorized configurations are provisioned onto your network devices through an IT Service Management (ITSM) check.

The visibility component of this feature is enabled by default, so you can preview device configurations. To disable the feature, on the **System** > **Settings** > **Visibility and Control of Configurations** window, click **Configuration Preview**. For more information, see "Enable Visibility and Control of Configurations" in the *Cisco DNA Center Administrator Guide*.

The control component of this feature is disabled by default. To further secure your planned network configurations, ensure that the control component of this feature is enabled. To enable control, on the **System** > **Settings** > **Visibility and Control of Configurations** window, click **ITSM Approval**. For more information, see "Enable Visibility and Control of Configurations" in the *Cisco DNA Center Administrator Guide*.

Note A workflow supports visibility and control if it displays the following banner message when you schedule the deployment of your task:

This workflow supports enforcing network administrators and other users to preview configurations before deploying them on the network devices. To configure this setting, go to **System** > **Settings** > **Visibility and Control of Configurations**.

If You Enable Only Visibility

On the **Visibility and Control of Configurations** window, if you enable **Configuration Preview**, you must preview the device configurations before deploying them. This means that the **Now** and **Later** scheduling options for deployment are dimmed (unavailable) until you preview your device configurations. You can preview device configurations during the provisioning segment of a visibility-supported workflow or later on the **Activities** > **Work Items** window. These two options offer you the flexibility to preview configurations at your own pace.

Note If there is a conflicting operation when you deploy your planned network configurations, the **Pending Operations** dialog box is displayed. To proceed with the current deployment, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations.

When you first generate a preview configuration on the **Preview Configuration** window, the system automatically chooses the first listed device and generates its configuration preview. While this preview is generating, you can choose another device to generate its configuration preview.

While reviewing the configurations on the **Preview Configuration** window, you can do the following:

- Filter the data in the configuration preview with the **Config Sourced From** drop-down list.
- For better visualization and readability of NETCONF YANG configuration, display the configuration preview in tree view by clicking the **Show in tree view** toggle button. This toggle button is available only for Cisco Catalyst 9800 Series Wireless Controllers.

Note The **Config Sourced From** drop-down list is not available in the tree view.

After reviewing the configurations on the **Preview Configuration** window, you can do the following:

- If you aren't ready to deploy the configurations and want to review them later on the **Work Items** window, click **Exit and Preview Later**.
- If you want to discard the work item and return to the current activity, click **Discard**. If you discard this work item, you can't recover it later.
- If you want to retain any generated configurations and discard all other resources, click **Discard**. Then in the **Discard** dialog box, check the **Retain generated configs (if any)** check box and click **Accept**.

  If you retain any generated configurations and discard all other resources, **Exit** will display instead of **Exit and Preview Later** because you've previewed all the configurations and chosen to discard the nongenerated ones.

Tip Consider retaining any generated configurations and discarding all other resources if a configuration preview fails so that you or your IT administrator can further inspect the issue.

- When you're ready to submit the configurations for all the devices listed, click **Deploy**.

  If there are multiple devices, you must click each device to preview its configuration. However, when you click **Deploy**, the configurations are pushed to all the devices even if the configurations are not previewed on all devices.

Note When you preview the configurations, Cisco DNA Center creates a snapshot of the configuration previews. If there are any changes in the network settings or network profiles after this operation is scheduled for deployment, the changes are not included during the device provisioning.

- If **Save Intent** displays instead of **Deploy**, the parameters that you chose during the workflow are already present on the device. To save those parameters to the database, click **Save Intent**. No configuration will be pushed to the device because the device already has the required configuration.

If You Enable Visibility and Control

On the **Visibility and Control of Configurations** window, if **Configuration Preview** and **ITSM Approval** are both enabled, you must preview the planned network configurations and submit them to an IT administrator for approval before deploying them. You can submit the planned network configurations during the provisioning segment of a visibility- and control- supported workflow or later on the **Activities** > **Work Items** window. These two options offer you the flexibility to preview configurations at your own pace.

When you first generate a preview configuration on the **Preview Configuration** window, the system automatically chooses the first listed device and generates its configuration preview. While this preview is generating, you can choose another device to generate its configuration preview.

While reviewing the configurations on the **Preview Configuration** window, you can do the following:

- Filter the data in the configuration preview with the **Config Sourced From** drop-down list.
- For better visualization and readability of NETCONF YANG configuration, display the configuration preview in tree view by clicking the **Show in tree view** toggle button. This toggle button is available only for Cisco Catalyst 9800 Series Wireless Controllers.

Note The **Config Sourced From** drop-down list is not available in the tree view.

After reviewing the configurations on the **Preview Configuration** window, you can do the following:

- If you aren't ready to deploy the configurations and would like to review them later on the **Activities** > **Work Items** window, click **Exit and Preview Later**.
- If you want to discard the entire work item and return to the current activity, click **Discard**, and then in the **Discard** dialog box, click **Accept**. If you discard this work item, you can't recover it later.
- If you want to retain any generated configurations and discard all other resources, click **Discard**. Then in the **Discard** dialog box, check the **Retain generated configs (if any)** check box and click **Accept**.

  If you retain any generated configurations and discard all other resources, **Exit** will display instead of **Exit and Preview Later** because you've previewed all the configurations and chosen to discard the nongenerated ones.

Tip Consider retaining any generated configurations and discarding all other resources if a configuration preview fails so that you or your IT administrator can further inspect the issue.

- When you're ready to submit the configurations for ITSM approval, click **Submit for Approval**.

  If there are multiple devices, you must click each device to preview its configuration. However, when you click **Submit for Approval**, the configurations are pushed to all the devices even if the configurations are not previewed on all devices.

Note When you preview the configurations, Cisco DNA Center creates a snapshot of the configuration previews. If there are any changes in the network settings or network profiles after this operation is scheduled for deployment, the changes are not included during the device provisioning.

- If **Save Intent** displays instead of **Submit for Approval**, the parameters that you chose during the workflow are already present on the device. To save those parameters to the database, click **Save Intent**. Because no configuration will be pushed to the device, ITSM approval isn't required.

Prerequisites for Provisioning a Cisco AireOS Controller

- Make sure that you have defined the following global network settings before provisioning a Cisco Wireless Controller:
  - 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 Configure Global CLI Credentials, Configure Global SNMPv2c Credentials, Configure Global SNMPv3 Credentials, and Configure 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 to Release 2.3.7 from an earlier release:

- For WPA3-Enterprise SSIDs, Cisco DNA Center enables the Dot1x-SHA256 authentication key management settings for the SSIDs.
- For WPA2-WPA3-Enterprise SSIDs, Cisco DNA 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 Add a Device to a Site.

- You cannot reuse any pre-existing VLANs on devices. Provisioning fails if Cisco DNA 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 Cisco DNA Center manually. You must perform all configurations from the Cisco DNA Center GUI.

Provision a Cisco AireOS Controller

Before you begin

Ensure the prerequisite is met. For more information, see Prerequisites for Provisioning a Cisco AireOS Controller, on page 5.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

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

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

The available devices in the selected site is displayed in the **Inventory** window.

Step 3 From the **DEVICE TYPE** list, click the **WLCs** tab, and from the **Reachability** list, click the **Reachable** tab to get the list of wireless controllers that are discovered and reachable.

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 is displayed.

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 is displayed.

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 the following:

Note This check box is displayed only if an AP authorization list is available. For more information about 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, Cisco DNA 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, Cisco DNA 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 is displayed.

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 Under **Mobility Group**, click **Configure** to configure the wireless controller as the mobility peer.

Step 25 In the **Configure Mobility Group** slide-in pane, from the **Mobility Group Name** drop-down list, you can either add a new mobility group by clicking **+**, or choose a mobility group from the existing mobility groups.

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

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

Step 26 In the **RF Group Name** text box, enter a name for the RF group.

Step 27 Under **Mobility Peers**, click **Add** to configure the wireless controller as a mobility peer.

Step 28 In the **Add Mobility Peer** slide-in pane, configure the following:

a) Choose one of the following types of mobility peers:

- To include mobility peers that are managed by Cisco DNA Center, click **Managed WLC**.
- To include mobility peers that are not managed by Cisco DNA 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, Cisco DNA Center creates a mobility group in 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**, configure the following:

- In the **Device Name** field, enter the device name.
- (Optional) From the **Device Series** drop-down list, choose the device series.
- In the **Public IP Address** field, enter the public IP address.
- (Optional) In the **Private IP Address** field, enter the private IP 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 29 Click **Configure Mobility**.

Step 30 To reset the mobility group name and the RF group name, you can do one of the following:

- 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**.
- On the **Provision** > **Configuration** window, under **Mobility Group**, click **Reset**.

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

Step 31 Click **Next**.

The **Model Configuration** window is displayed.

Step 32 In the **Devices** pane, you can either search for a model config design by entering its name in the **Find** field, or expand the device and select a model configuration design.

The selected model configuration design is displayed in the right pane.

Step 33 Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the model configuration design.

You cannot edit all the configurations at this step.

Step 34 After making the necessary changes, click **Apply**.

Step 35 Click **Next**.

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

Step 36 Search for the device or the template in the **Devices** panel.

Step 37 Enter a value for the predefined template variable in the **wlanid** field.

Step 38 Click **Next**.

Step 39 In the **Summary** step, review the device details, and click **Next** to provision the device.

Step 40 In the **Provision Device** slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option.

- To immediately deploy the configuration, click **Now**.
- To schedule the deployment for a later date and time, click **Later**, and define the date, time, and time zone of the deployment.
- To preview the configurations, click **Generate configuration preview**.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see Visibility and Control of Wireless Device Configurations, on page 2.

Step 41 Click **Apply**.

If you chose **Now** or **Later** in the **Provision Device** slide-in pane, the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 42 If you chose **Generate configuration preview** in the **Provision Device** slide-in pane, depending on the Visibility and Control of Configurations settings, do the following:

a. Review the device configurations.

For more information, see Visibility and Control of Wireless Device Configurations, on page 2.

b. When you're ready, click **Deploy** or **Submit for Approval**. If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

c. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

d. Click **Submit**.

When the configurations are successfully submitted, a success message is displayed.

If you previewed and scheduled the task for deployment, you can view the task on the **Tasks** window.

If you submitted the configurations for ITSM approval, you can view the work item's status on the **Work Items** window. If it's not approved, you must resubmit the work item for ITSM approval. When it's approved, it will be deployed at the scheduled time, which you can view on the **Tasks** window.

Note When you provision, Cisco DNA Center pushes the configurations to the wireless controller and configures the device based on the network intent. During reprovisioning, if there are any out-of-band configurations on the device, Cisco DNA Center doesn't overwrite these configurations unless they are part of the intent.

Step 43 Provision the secondary controller.

Step 44 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 45 After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 46 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 47 Click **See Details** under **Device Provisioning**.

Step 48 Click **View Details** under **Deployment of network intent**, and click the device name.

Step 49 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 50 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 Cisco DNA 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 in the Managed state.
- 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 the following 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

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

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

Step 2 Check the check box next to the 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 is displayed.

Note A warning is displayed at the top of the pane if the controller you selected hasn't been assigned to a site. Cisco DNA Center will not push its telemetry configuration to the controller until it's a site member.

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 Cisco 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 is displayed at the top of the **High Availability** window, along with the following message:

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

Step 6 Click **Configure HA**.
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 complete, both wireless controllers reboot. This process may take up to 2.5 minutes to complete.

Step 7 To verify the HA configuration, on the **Devices** > **Inventory** window, click the device that you configured as an HA device.

Step 8 Click the **Wireless Info** tab.

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

This is triggered by the inventory poller or manual resynchronization. By now, the secondary wireless controller (wireless controller 2) is deleted from Cisco DNA 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

Cisco DNA Center sends the following commands to configure Cisco Wireless Controller HA.

Cisco DNA Center sends the following commands to wireless controller 1:

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

Cisco DNA Center sends the following commands to wireless controller 2:

- **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 the following 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 Cisco DNA Center Disable HA feature is supported on Cisco Catalyst 9800 Series Wireless Controllers and Cisco AireOS Controllers.

Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Device** > **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 is displayed.

High Availability slide-in pane shows the **REDUNDANCY SUMMARY** of selected wireless controller configured from outside Cisco DNA Center.

Step 4 In the **Warning** window, click **OK**.

A success message appears at the bottom of the screen indicating that the HA feature has been successfully disabled for the selected wireless controller.

Provision a Cisco AP—Day 1 AP Provisioning

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.
- 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 6 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 41.
- If you update the AP zone configurations, you must reprovision the wireless controller. For more information, see Provision a Cisco AireOS Controller, on page 6 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 41.
- 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.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Note You can either search for a site by entering its name or expand **Global** to select the site. Devices that are available in the selected site are displayed in the **Inventory** window.

To filter the devices based on various criteria, such as **Device Family** or **Reachability Status**, click **Filter**, make your selections, and then click **Apply**.

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

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

Step 4 In the **Assign Site** step, configure the following parameters:

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

Note Cisco DNA Center does not 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 5 In the **Configuration** step, configure the following parameters:

a) Click **Advanced Configuration** to configure radio antenna 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.

b) Configure the beam selection value for AP radio slot 1 and slot 2 from the **Slot 1** and **Slot 2** drop-down list.
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 **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**.
g) Click **Next**.

Step 6 In the **Summary** step, review the device details, and click **Next** to provision the AP.

Step 7 In the **Provision Device** slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option.

- To immediately deploy the configuration, click **Now**.
- To schedule the deployment for a later date and time, click **Later**, and define the date, time, and time zone of the deployment.
- To preview the configurations, click **Generate configuration preview**.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see Visibility and Control of Wireless Device Configurations, on page 2.

Step 8 Click **Apply**.

If you chose **Now** or **Later** in the **Provision Device** slide-in pane, the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 9 If you chose **Generate configuration preview** in the **Provision Device** slide-in pane, depending on the Visibility and Control of Configurations settings, do the following:

a. Review the device configurations.

For more information, see Visibility and Control of Wireless Device Configurations, on page 2.

b. When you're ready, click **Deploy** or **Submit for Approval**. If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

c. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

d. Click **Submit**.

When the configurations are successfully submitted, a success message is displayed.

If you previewed and scheduled the task for deployment, you can view the task on the **Tasks** window.

If you submitted the configurations for ITSM approval, you can view the work item's status on the **Work Items** window. If it's not approved, you must resubmit the work item for ITSM approval. When it's approved, it will be deployed at the scheduled time, which you can view on the **Tasks** window.

Step 10 You are 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.

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. Cisco DNA 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.

Step 1 From the top-left corner, click the menu icon and 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**.

A success message is displayed: `ICMP Ping status updated successfully`.

Cisco DNA 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 Configure Global CLI Credentials, Configure Global SNMPv2c Credentials, and Configure 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 Cisco DNA 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.

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

Step 2 The DHCP server allocates the IP address with Option #43, which is the IP address of the Cisco DNA 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 is displayed.

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. Cisco DNA 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 6.

Provision Cisco AireOS Controllers in the Existing Deployment

Before you begin

With Cisco DNA Center, you can add and provision the Cisco Wireless Controller, which belongs to existing sites with pre-existing infrastructure.

- Start by running a Discovery job on the device. All your devices are displayed on the **Inventory** window. For more information, see Discover Your Network and About Inventory.
- The wireless controller should be reachable and in the Managed state on the **Inventory** window. For more information, see About Inventory.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

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

Step 2 Click **Filter** and enter the appropriate values in the selected filter field. For example, for the **Device Name** filter, enter the name of the device.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

Step 3 Check the check box next to the wireless controller device name that you want to provision.

Step 4 From the **Actions** drop-down list, choose **More** > **Learn Device Config**.

The **Site Assignment** window opens and the **Learn Device Configuration** workflow begins.

Note You can also start this workflow by doing the following:

a. From the **Inventory** window, click the device's link to open a pop-up window that provides high-level information for that device.

b. Click **View Device Details** to open the device's details page.

c. Click **Learn WLC Config**.

Step 5 Associate a site to the controller in the **Assign Site** step:

a) Click **Choose a site** to assign a site to the controller.
b) In the **Choose a site** slide-in pane, select a site to which you want to associate the wireless controller, and click **Save**.
c) Click **Next**.

Step 6 The **Resolve Conflict** step shows any conflicting configurations in Cisco DNA Center that you need to resolve.

Step 7 Click **Next**.

Step 8 The **Design Object** window lists all the learned configurations.

a) Click **Network** in the left pane.

The right pane displays network configurations that were learned as a part of device configuration learning and shows the following information:

- **AAA Server** details.
- **Systems Settings**, with details about the IP address and protocol of the AAA server.
- **DHCP Server** details.
- Enter the **Shared Secret** for the AAA server.

b) Click **Wireless** in the left pane.

The right pane lists the enterprise SSIDs, guest SSIDs, antenna radio profiles, and wireless interface details.

For an SSID with a preshared key (PSK), enter the **passphrase key**.

c) Click **Discarded Config** in the left pane.

The right pane lists the conflicting or the existing configurations on Cisco DNA Center. The discarded configuration entries are categorized as:

- Duplicate design entity
- Unknown device configuration for Radio Policy

d) Click **Next**.

The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.

e) Click **Save**.

Step 9 Choose **Design** > **Network Profiles** to assign a site to the network profile.

Step 10 In the **Network Profiles** window, configure the following:

a) Click **Assign Site** to add sites to the selected profile.
b) In the **Add Sites to Profile** window, choose a site from the drop-down list, and click **Save**.

Step 11 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

a) Click **Filter** to locate the device that you want to provision.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

b) Check the check box next to the controller device name that you want to provision.
c) From the **Actions** drop-down list, choose **Provision**.
d) Review the details in the **Assign Site** window, and click **Next**.

The **Configurations** step is displayed.

e) Under **Interface and VLAN Configuration**, click **+Add** to configure interface and VLAN details.
f) In the **Configure Interface and VLAN** window, configure the required fields, and click **OK**.
g) Click **Next**.

Step 12 In the **Summary** window, review the configuration settings.

Step 13 Click **Deploy**.

Step 14 In the **Provision Devices** slide-in pane, do the following 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 **Work Items** window, click the menu icon and choose **Activities** > **Work Items**.

d) In the **Work Items** 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 the following:

1. Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
2. Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

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 Cisco DNA 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.

The following 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. Supports up to 80 Gbps throughput and occupies a 2-rack unit space. 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. Supports up to 2000 access points and 32,000 clients. Supports up to 40 Gbps throughput and occupies a 1-rack unit space. Provides four 1-GE or 10-GE uplink ports.
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). Cisco Catalyst 9800-CL Cloud Wireless Controller is the next generation of enterprise-class virtual wireless controllers built for high availability and security. 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. 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. • Cisco Catalyst 9800-L Copper Series Wireless Controller (9800-L-C RJ45) • Cisco Catalyst 9800-L Fiber Series Wireless Controller 9800-L-F SFP)

The following 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 • VMware ESXi vSphere 6.5[1] • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	• Linux KVM based on Red Hat Enterprise Linux 7.1 and 7.2 • 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 the following: 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.

The following table lists the Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) versions supported in Cisco DNA 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 4.1.1 3.12.3 3.11.3 3.11.2 3.11.1	ENCS 5400 UCS-E UCS-C	Cisco DNA Center supports the following NFVIS upgrade paths: NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2. Cisco Enterprise NFVIS 3.12.1 is not supported on any versions of Cisco DNA Center. Upgrade to Cisco Enterprise NFVIS 3.12.1 from Cisco Enterprise NFVIS 3.11.x using Cisco DNA Center is not supported. Upgrade to Cisco Enterprise NFVIS 3.12.2 from Cisco Enterprise NFVIS 3.12.1 using Cisco DNA Center is not supported. Upgrade to Cisco Enterprise NFVIS 3.12.2 from 3.11.2 is supported using Cisco DNA Center. Cisco Enterprise NFVIS 3.12.2 is supported on Cisco DNA Center.

Cisco Enterprise NFVIS Version	Enterprise Network Compute System Device Platform	Notes
3.12.2 3.11.3 3.11.2 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 Cisco DNA Center

1. Install Cisco DNA Center.

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

2. For information on software image upgrade, see Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller, on page 25.

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

   From the top-left corner, click the menu icon and choose **System Settings** > **Software Updates** > **Installed Apps**.

4. Integrate Cisco Identity Services Engine with Cisco DNA Center. After integration, any devices that Cisco DNA 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 are displayed 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 the following 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 Cisco DNA Center.

   To import and upload an existing network hierarchy, see Import Your Site Hierarchy to Cisco DNA 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.

    Cisco DNA 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; Cisco DNA 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 to Release 2.3.7 from an earlier release:

- For WPA3-Enterprise SSIDs, Cisco DNA Center enables the Dot1x-SHA256 authentication key management settings for the SSIDs.
- For WPA2-WPA3-Enterprise SSIDs, Cisco DNA 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. Configure the following in the **Policy** window for the Cisco Catalyst 9800 Series Wireless Controller:

    - 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 26.

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 41.

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.

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

The **Inventory** window is displayed 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 Assign a Software Image to 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 Specify a Golden Software Image.

Step 5 Provision the software image.

From the top-left corner, click the menu icon and 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 the following prerequisites:

- Both the Cisco Catalyst 9800 Series Wireless Controller devices are running the same software version and have the active software image on the primary Catalyst 9800 Series Wireless Controller.
- The service port and management port of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured.
- The redundancy port 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, 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 Cisco DNA Center.
- The devices are reachable and are in the **Managed** state.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

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

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

All the devices available in that selected site are displayed in the **Inventory** window.

Step 3 From the **Device Type** list, click the **WLCs** tab, and from the **Reachability** list, click the **Reachable** tab to get the list of wireless controllers that are discovered and reachable.

Step 4 In the **Inventory** window, click the desired Cisco Catalyst 9800 Series Wireless Controller name to configure as a primary controller.

Step 5 Click the **High Availability** tab.

The selected Catalyst 9800 Series Wireless Controller by default becomes the primary controller and the **Primary C9800** field is grayed out.

Step 6 From the **Select Primary Interface** and **Secondary Interface** drop-down lists, choose the interface that is used for HA connectivity.

The HA interface serves the following 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 is displayed at the top of the **High Availability** window, along with the following message:

Ensure that the Redundancy Management IP and Peer Redundancy Management IP are not 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.
- Cisco DNA 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 In the **Netmask** field, enter the netmask address.

Step 10 Click **Configure HA**.

The HA configuration is initiated at 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 11 After the HA is initiated, the **Redundancy Summary** under **High Availability** tab displays the **Sync Status** as **HA Pairing is in Progress**. When Cisco DNA Center finds that the HA pairing is successful, the **SyncStatus** becomes **Complete**.

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

Step 12 To manually resynchronize the controller, on the **Provision** > **Inventory** window, select the controller that you want to synchronize manually.

Step 13 From the **Actions** drop-down list, choose **Resync**.

Step 14 The following is the list of actions that occur after the process is complete:

- 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 in order 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 Cisco DNA Center then in a HA setup, the CTS credentials for active and standby controllers are synchronized and hence, during a HA switchover, Cisco DNA Center does not 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 Cisco DNA Center.

Commands to Configure High Availability on Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Use the following 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 the following 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 the following 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 the following 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 the following 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

Cisco DNA 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 must be used for HA.

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.

Cisco DNA 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.

Note The primary and secondary controllers must be of the same device type. For example, if the primary device is a Catalyst 9800 Series Wireless Controller, the secondary device must also be a Catalyst 9800 Series Wireless Controller.

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 the following 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.
- Cisco DNA 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 Cisco DNA 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 Cisco DNA Center

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

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window is displayed 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 is displayed.

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 is displayed, which shows the primary AP managed 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 **Configure Interface and VLAN** area, configure the IP address and subnet mask details, and click **Next**.

Step 11 In the **Advanced Configuration** window, configure 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 **Deploy**.

Step 13 Click **Now** to deploy the device immediately. Click **Later** to schedule the deployment for a later time.

Step 14 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 15 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window is displayed.

Step 16 Click **Choose a site** to assign the managed AP location for the secondary controller.

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

Step 17 In the **Choose a site** window, check the check box next to the site name to associate the secondary controller, and click **Save**.

Step 18 Click **Next**.

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

Step 19 Add or update the managed AP locations for the secondary controller by clicking **Select Secondary Managed AP Locations**.

Step 20 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 21 Configure the interface and VLAN details for the secondary controller.

Step 22 Under the **Configure Interface and VLAN** area, configure the IP address and subnet mask details for the secondary controller, and click **Next**.

Step 23 In the **Advanced Configuration** window, configure values for the predefined template variables, and click **Next**.

Step 24 In the **Summary** window, verify the managed AP locations for the secondary controller and other configuration details, and click **Deploy**.

Step 25 Click **Now** to deploy the device immediately. Click **Later** to schedule the deployment for a later time.

Step 26 To verify the managed locations of the primary and secondary controllers, click the device name of the controllers that you provisioned on the **Provision** > **Network Devices** > **Inventory** window.

Step 27 In the dialog box, click **View Device Details**.

Step 28 In the device details window, click the **Managed ap locations** tab to view the primary and secondary managed location details.

Step 29 Provision the AP for the primary controller.

Step 30 On the **Network Devices** > **Inventory** window, check the check box next to the AP that you want to provision.

Step 31 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

Step 32 In the **Assign Site** window, click **Choose a Floor** to select the floor from the primary managed location.

Step 33 Click **Next**.

The **Configuration** window is displayed.

Step 34 By default, the custom RF profile that you marked as the default under **Design** > **Network Settings** > **Wireless** > **RF Profiles** > **Basic RF Profile** is chosen in the **RF Profile** drop-down list.

You can change the default RF profile value for an AP by selecting a value from the **RF Profile** drop-down list.

Step 35 Click **Next**.

Step 36 In the **Summary** window, review the configuration details.

Step 37 Click **Deploy** to provision the primary AP.

Step 38 You are prompted with a message that creation or modification of an AP group is in progress.

You are prompted with a message stating `After provisioning AP(s) will reboot. Do you want to continue?`.

Step 39 Click **OK**.

When deployment succeeds, the **Last Sync Status** column in the **Device Inventory** window shows `SUCCESS`.

Mobility Configuration Overview

The mobility configuration in Cisco DNA 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.

Cisco DNA 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 the following 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, Cisco DNA 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

The following 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 Cisco DNA 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 Cisco DNA 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

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window is displayed, 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 is displayed.

For more information, see Mobility Configuration Overview, on page 33.

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 Cisco DNA 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, configure the following:

a) Choose one of the following types of mobility peers:

- To include mobility peers that are managed by Cisco DNA Center, click **Managed WLC**.
- To include mobility peers that are not managed by Cisco DNA 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, Cisco DNA 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**, configure the following:

- In the **Device Name** field, enter the device name.
- (Optional) From the **Device Series** drop-down list, choose the device series.
- In the **Public IP Address** field, enter the public IP address.
- (Optional) In the **Private IP Address** field, enter the private IP 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 the following 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 In the **Configure Mobility Group** slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option.

- To immediately deploy the configuration, click **Now**.
- To schedule the deployment for a later date and time, click **Later**, and define the date, time, and time zone of the deployment.
- To preview the configurations, click **Generate configuration preview**.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see Visibility and Control of Wireless Device Configurations, on page 2.

Step 14 Click **Apply**.

If you chose **Now** or **Later** in the **Configure Mobility Group** slide-in pane, the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 15 If you chose **Generate configuration preview** in the **Configure Mobility Group** slide-in pane, depending on the Visibility and Control of Configurations settings, do the following:

a. Review the device configurations.

For more information, see Visibility and Control of Wireless Device Configurations, on page 2.

b. When you're ready, click **Deploy** or **Submit for Approval**. If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

c. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

d. Click **Submit**.

When the configurations are successfully submitted, a success message is displayed.

If you previewed and scheduled the task for deployment, you can view the task on the **Tasks** window.

If you submitted the configurations for ITSM approval, you can view the work item's status on the **Work Items** window. If it's not approved, you must resubmit the work item for ITSM approval. When it's approved, it will be deployed at the scheduled time, which you can view on the **Tasks** window.

Configure AP Impersonation

Cisco DNA 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.

Step 1 From the top-left corner, click the menu icon and 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 the 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.

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

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

From the left hierarchy tree, choose 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, Cisco DNA 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 41.

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 High Availability 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 High Availability 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 Cisco DNA 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 Cisco DNA 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 perform a rolling AP upgrade on both devices. Instead, one controller must go through a normal upgrade. You can perform a 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.

Step 1 Install Cisco DNA Center.

For more information, see the Cisco Digital Network Architecture Center Installation Guide.

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

From the top-left corner, click the menu icon and 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 Cisco DNA Center.

To import and upload an existing network hierarchy, see Import Your Site Hierarchy to Cisco DNA 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 33.

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 41.

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 Assign a Software Image to 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 Specify a Golden Software Image.

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 the following information:

- **Distribution Operation**: Provides information about the image distribution process. The image gets copied from Cisco DNA 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

Before you begin

Ensure that you have completed the steps in Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center, on page 22.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

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

Step 2 In the **Devices** table, check the check box next to the Catalyst 9800 Series Wireless Controller name that you want to provision.

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

Step 4 In the **Assign Site** window, click **Choose a Site** to associate with a site.

Step 5 In the **Choose a site** slide-in pane, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller, and click **Save**.

You can choose 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.

Step 6 Click **Next**.

Step 7 In the **Configuration** window, choose a role for the Cisco Catalyst 9800 Series Wireless Controller: **Active Main WLC** or **Anchor**.

Step 8 Click **Select Primary Managed AP Locations** to choose the managed AP location for the primary controller.

Step 9 Click **Select Secondary Managed AP Locations** to choose the managed AP location for the secondary controller.

Step 10 You can choose either a parent site or individual sites, and click **Save**.

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

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

Step 11 (Optional) Check the **AP Authorization List** check box to choose the authorization list for AP authorization, and do the following:

Note This check box is displayed only if an AP authorization list is available. For more information about 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, Cisco DNA 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, Cisco DNA 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 12 For an active main wireless controller, you need to configure the interface and VLAN details.

Step 13 In the **Assign Interface** area, do the following:

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

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.
- Assigning an IP address, gateway IP address, and subnet mask is not required for the Cisco Catalyst 9800 Series Wireless Controller.
- Effective with Release 2.3.7.3, for the FlexConnect SSIDs, VLANs are not 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.

Step 14 (Optional) Check the **Skip AP Provision** check box to skip configuring the AP related commands while provisioning the Cisco Catalyst 9800 Series Wireless Controller.

Step 15 Click **Next**.

Step 16 In the **Devices** pane of the **Model Configuration** window, you can either search for a model configuration design by entering its name in the **Find** field, or expand the device and select a model configuration design.

The selected model configuration design is displayed in the right pane.

Step 17 Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the model configuration design.

You cannot edit all the configurations at this step.

Step 18 After making the necessary changes, click **Apply**.

Step 19 Click **Next**.

Step 20 In the **Devices** pane of the **Advanced Configuration** window, search for the device or template.

Step 21 In the **wlanid** field, enter a value for the predefined template variable, and click **Next**.

Step 22 In the **Summary** window, review the configuration settings, and click **Next**.

Step 23 In the **Provision Device** slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option.

- To immediately deploy the configuration, click **Now**.
- To schedule the deployment for a later date and time, click **Later**, and define the date, time, and time zone of the deployment.

- To preview the configurations, click **Generate configuration preview**.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see Visibility and Control of Wireless Device Configurations, on page 2.

Step 24 Click **Apply**.

If you chose **Now** or **Later** in the **Provision Device** slide-in pane, the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 25 If you chose **Generate configuration preview** in the **Provision Device** slide-in pane, depending on the Visibility and Control of Configurations settings, do the following:

a. Review the device configurations.

For more information, see Visibility and Control of Wireless Device Configurations, on page 2.

b. When you're ready, click **Deploy** or **Submit for Approval**. If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

c. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

d. Click **Submit**.

When the configurations are successfully submitted, a success message is displayed.

If you previewed and scheduled the task for deployment, you can view the task on the **Tasks** window.

If you submitted the configurations for ITSM approval, you can view the work item's status on the **Work Items** window. If it's not approved, you must resubmit the work item for ITSM approval. When it's approved, it will be deployed at the scheduled time, which you can view on the **Tasks** window.

Note When you provision, Cisco DNA Center pushes the configurations to the wireless controller and configures the device based on the network intent. During reprovisioning, if there are any out-of-band configurations on the device, Cisco DNA Center doesn't overwrite these configurations unless they are part of the intent.

Step 26 To verify the configurations that are pushed from Cisco DNA Center to the device, use the following commands on the Cisco Catalyst 9800 Series 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, choose **Provision**.

Step 29 Under the **Provisioning Status** column, click a device's **See Details** link 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.

Configure Cisco Wireless Controllers on the Existing Infrastructure

With Cisco DNA Center, you can add and provision devices such as Cisco Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers in the existing deployment.

Before you begin

- Start by running a Discovery job on the device. All your devices are displayed on the **Inventory** window. For more information, see Discover Your Network and About Inventory.
- The wireless controller should be reachable and in Managed state on the **Inventory** window. For more information, see About Inventory.
- To discover Cisco Catalyst 9800 Series Wireless Controller, you must enable NETCONF and set the port to 830. For more information, see Discovery Overview.
- 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, import it into Cisco DNA Center.

  For more information about importing and uploading an existing network hierarchy, see Import Your Site Hierarchy to Cisco DNA Center.

  For more information about creating a new network hierarchy, see Create, Edit and Delete a Site and Add, Edit, and Delete a Building.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

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

Step 2 Click **Filter** and enter the appropriate values in the selected filter field. For example, for the **Device Name** filter, enter the name of the device.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

Step 3 Check the check box next to the wireless controller device name that you want to provision.

Step 4 From the **Actions** drop-down list, choose **More** > **Learn Device Config**.

The **Site Assignment** window opens and the **Learn Device Configuration** workflow begins.

Note You can also start this workflow by doing the following:

a. From the **Inventory** window, click the device's link to open a pop-up window that provides high-level information for that device.

b. Click **View Device Details** to open the device's details page.

c. Click **Learn WLC Config**.

Step 5 Follow Step 3 through Step 13 in Learn Device Configurations from Devices with Pre-Existing Infrastructure.

Step 6 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

Step 7 Click **Filter** to locate the device that you want to provision.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

Step 8 Check the check box next to the wireless controller that you want to provision.

Step 9 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

Step 10 Review the details in the **Assign Site** step, and click **Next**.

Step 11 In the **Configuration** step, configure the following:

a) Under **Interface and VLAN Configuration**, click **+Add** to configure interface and VLAN details.
b) In the **Configure Interface and VLAN** window, configure the required fields, and click **OK**.
c) Click **Next**.

Step 12 In the **Model Configuration** step, configure the following.

- In the **Devices** pane, you can either search for a model config design by entering its name in the Find field, or expand the device and select a model config design. The selected model config design is displayed in the right pane.
- Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the model config design. You cannot edit all the configurations at this step.
- After making the necessary changes, click **Apply**.
- Click **Next**.

Step 13 In the **Advanced Configuration** window, you can enter values for the predefined template variables.

- Search for the device or the template in the Devices panel.
- Enter a value for the predefined template variable in the **wlanid** field, and click **Next**.

Step 14 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 15 To proceed, click **Deploy**.

Step 16 In the **Schedule** window, click **Now** or **Later** to indicate when you want to start the configuration, and click **Apply**.

Step 17 Provision the AP. For information, see Provision a Cisco AP—Day 1 AP Provisioning, on page 13.

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 at the global level. The credentials that are defined at the global level are inherited by the sites.

  For more information, see Configure Global CLI Credentials, Configure Global SNMPv2c Credentials, and Configure 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 is IP address of the Cisco DNA Center Plug and Play server. Using this IP address, the APs contact the PnP server and download the configuration.
- 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

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 Cisco DNA 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** > **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** 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 is displayed.

Step 6 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 7 Click **Next**.

Step 8 To configure a device, click the device name in the **Configuration** window.

Step 9 In the **Configuration for device name** window, assign the static IP details for the device.

Step 10 Click **Save**.

Step 11 Click **Next**.

The **Summary** window is displayed.

Step 12 Click **Claim** in the **Summary** window.

After the Cisco Embedded Wireless Controller on Catalyst Access Points is claimed, the IP address configured is assigned to the Cisco Embedded Wireless Controller.

The claimed device, which is a Cisco Embedded Wireless Controller with an internal AP, is now available under **Provision** > **Network Devices** > **Inventory**.

Step 13 To provision the additional controller, see Provision a Cisco AireOS Controller, on page 6.

Step 14 To bulk import devices from a CSV file, see Add Devices in Bulk.

Step 15 To add devices manually, see Add or Edit a Device.

Migrate Cisco AireOS Controller to Cisco Catalyst 9800 Series Wireless Controller Using Cisco DNA Center

Before you begin

- Design your network hierarchy by adding sites, buildings, and floors.
- Discover the Cisco Catalyst 9800 Series Wireless Controller by running the Discovery feature and add it to the Inventory. Make sure that the device status is reachable and in the Managed state.

  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.
- Discover the Cisco AireOS Controllers and add it to the Inventory. Make sure that the device status is reachable and in the Managed state.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window is displayed, which lists the discovered devices.

Step 2 Check the check box next to the Cisco AireOS Controller.

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

Step 4 In the **Assign Device to Site** window, click **Choose a Site**.

Step 5 In the **Add Sites** window, check the check box next to the site name to associate a Cisco AireOS Controller.

Step 6 Click **Save**.

Step 7 From the **Actions** drop-down list, choose **More** > **Learn Device Config**.

The **Site Assignment** window opens and the **Learn Device Configuration** workflow begins.

Note You can also start this workflow by doing the following:

a. From the **Inventory** window, click the device's link to open a dialog box that provides high-level information for that device.

b. Click **View Device Details** to open the device's details window.

c. Click **Learn WLC Config**.

Step 8 In the **Assign Site** window, click **Next**.

Step 9 The **Resolve Conflict** window shows any conflicting configurations in Cisco DNA Center that you need to resolve. Click **Next**.

Step 10 In the **Design Object** window, click **Next**.

Step 11 In the left pane, click **Network**.

The right pane displays network configurations that were learned as part of the device configuration learning process, and shows the following information:

- AAA server details.

- Systems settings, with details about the IP address and protocol of the AAA server. Enter the shared secret for the AAA server because the passwords are encrypted and Cisco DNA Center cannot learn passwords.
- DHCP server, with details about all the DHCP servers available in the device.
- NTP server, with details about all the NTP servers available in the device.

Step 12 Click **Next**.

Step 13 In the left pane, click **Wireless**.

The **Wireless** window displays the enterprise SSIDs, guest SSIDs, wireless interfaces, and RF profiles that are present on the device.

Step 14 For an SSID with a preshared key (PSK), enter the passphrase key.

Step 15 In the left pane, click **Discarded Config**.

This displays the conflicting and the existing configurations on Cisco DNA Center. The discarded configuration entries are available under the following categories:

- Duplicate design entity
- Unknown device configuration for radio policy

Step 16 Click **Next**.

Step 17 The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.

Step 18 Click **Save**.

A success message is displayed.

Step 19 Choose **Design** > **Network Settings** > **Wireless** to view the SSID and interface configurations that Cisco DNA Center has learned from the Cisco AireOS Controller.

Step 20 Choose **Design** > **Network Profiles** to assign a site to the network profile.

Step 21 In the **Network Profiles** window, click **Assign Site** to add sites to the selected profile.

Step 22 In the **Add Sites to Profile window**, choose a site from the drop-down list, and click **Save**.

Step 23 Click the **Provision** tab.

Step 24 Check the check box next to the Cisco Catalyst 9800 Series Wireless Controller that you want to provision.

Step 25 From the **Actions** drop-down list, choose **Provision**.

Step 26 Click **Choose a site** to assign a site for the Cisco Catalyst 9800 Series Wireless Controller.

Step 27 In the **Choose a site** window, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.

Step 28 Click **Next**.

The **Configuration** window is displayed.

Step 29 Select a role for the Cisco Catalyst 9800 Series Wireless Controller as **Active Main WLC**.

Step 30 Click **Select Primary Managed AP Locations** to configure a managed AP location for the primary controller.

Step 31 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.

Step 32 Click **Save**.

Step 33 Click **Next**.

Step 34 The **Summary** window shows the configurations that will be pushed to the Cisco Catalyst 9800 Series Wireless Controller from the Cisco AireOS Controller.

Step 35 Click **Deploy** to provision the Cisco Catalyst 9800 Series Wireless Controller.

Step 36 Click **Now** to deploy the device immediately. Click **Later** to schedule deployment for a later time and click **Apply**.

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 To manually resynchronize the Cisco Catalyst 9800 Series Wireless Controller, on the **Provision** > **Inventory** window, select the controller that you want to manually synchronize.

Step 40 From the **Actions** drop-down list, choose **Resync**.

Step 41 Provision the AP.

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 Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches
Fabric Edge	Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches Cisco Catalyst 3600 Series Switches Cisco Catalyst 3850 Series Switches
APs	Cisco 802.11ac Wave 2 APs: • Cisco Aironet 1810 Series OfficeExtend Access Points • Cisco Aironet 1810W Series Access Points • Cisco Aironet 1815i Access Point • Cisco Aironet 1815w Access Point • Cisco Aironet 1815m Access Point • Cisco 1830 Aironet Series Access Points • Cisco Aironet 1850 Series Access Points

Device Role	Platforms
	• Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points Cisco 802.11ac Wave 1 APs • Cisco Aironet 1700 Series Access Points • Cisco Aironet 2700 Series Access Points • Cisco Aironet 3700 Series Access Points Cisco Catalyst 9105 Series Wi-Fi 6 Access Points Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Cisco Catalyst 9117 Series Wi-Fi 6 Access Points Cisco Catalyst 9120 Series Wi-Fi 6 Access Points Cisco Catalyst 9124 Series Wi-Fi 6 Access Points Cisco Catalyst 9130 Series Wi-Fi 6 Access Points Cisco Catalyst 9136 Series Wi-Fi 6 Access Points

Preconfiguration

On the Cisco Catalyst 9800 Series Wireless Controller, make sure that the following 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 an automated underlay for provisioning.

Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches

1. Install Cisco DNA Center.

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

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

   From the top-left corner, click the menu icon and choose **System** > **Software Updates** > **Installed Apps**.

3. Integrate Cisco Identity Services Engine with Cisco DNA Center. After Cisco ISE is registered with Cisco DNA Center, any device that Cisco DNA 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 Cisco DNA Center.

   To import and upload an existing network hierarchy, see the Import Your Site Hierarchy to Cisco DNA 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 Global Device Credentials Overview, Configure Global CLI Credentials, Configure Global SNMPv2c Credentials, Configure Global SNMPv3 Credentials, and Configure 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 Cisco DNA 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. Configure the following on the **Policy** window:

    - 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 Fabric Networks.

    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 51.

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.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

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

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

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

Step 4 In the **Assign Device to Site** step, do the following:

a) Click **Choose a site**.
b) In the **Choose a site** slide-in pane, check the check box next to the site to associate the device.
c) Click **Save**.
d) Click **Apply**.
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 5 In the **Devices** > **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 **Deploy**.
d) In the **Provision Devices** window, do the following to preview the CLI configuration:

1. Click **Generate Configuration Preview** radio button.
2. In the **Task Name** field, enter a name for the CLI preview task, and click **Apply**.
3. 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 **Work Items** window, click the menu icon and choose **Activities** > **Work Items**.
4. In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
5. View the CLI configuration details and click **Deploy**.
6. Click **Now** to deploy the device immediately or click **Later** to schedule the deployment for a later time and click **Apply**.
7. In the **Information** dialog box, do the following:
   a. Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
   b. Click **No** if you want to retain the task in the **Work Items** window.

      Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

Step 6 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 7 To add devices to a fabric site, click the menu icon and choose **Provision** > **Fabric Sites**.

Step 8 Create a fabric site. For more information, see Add a Fabric Site.

Step 9 Add an IP transit network.

Step 10 Add devices and associate virtual networks to a fabric site.

Step 11 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 12 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**.

a) If you have not installed the wireless package on Cisco Catalyst 9000 Series Switches before enabling the wireless functionality, a warning message is displayed by Cisco DNA Center: `9800-SW image is necessary for turning on the capability. Click "OK" to import the 9800-SW image manually.`
b) Click **OK** to install the image manually.
c) 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.
d) Click **Import**.

The progress of the import is displayed.

e) Click **Activate image on device**.

A warning message is displayed: `Activate image on device will reboot the device. Are you sure you want to reboot the device?`

f) Click **Yes**.

The device reboots and comes online after the device package upgrade is complete.

g) In the dialog box, the AP locations that are managed by the controllers are displayed. You can change, remove, or reassign the site here.
h) Click **Next**.

Step 13 In the **Summary** window, review the configuration settings, and click **Save**.

Step 14 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 15 In the Cisco DNA Center GUI, click the **Provision** tab.

Step 16 Click the **Fabric** tab.

A list of fabric sites is displayed.

Step 17 Select the fabric site that was created, and click the **Host Onboarding** tab to enable IP pool for APs.

Step 18 Select the authentication template that is applied for devices in the fabric site. Then, click **Save**.

Step 19 Under **Virtual Networks**, click **INFRA_VN** to associate one or more IP pools with the selected virtual network.

Step 20 Under **Virtual Network**, click the guest virtual networks to associate IP pools for the selected guest virtual network.

Step 21 Check the **IP Pool Name** check box that was created for APs during the design phase.

Step 22 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 Cisco wireless controller through one of the discovery methods.

Step 23 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 24 Manually trigger resynchronization by choosing **Inventory** > **Resync** to see the APs on Cisco DNA 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 25 Provision the AP.

For more information, see Provision a Cisco AP—Day 1 AP Provisioning, on page 13.

Step 26 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 do not work. Always the last deployed policy takes precedence when you are setting up the relevance.

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.

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.

Cisco DNA Center supports the guest anchor feature for the following device combinations:

- 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 the following limitations:

- 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

Follow these steps to configure a guest anchor Cisco Wireless Controller.

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 6.

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 6.

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 Configure Global CLI Credentials, Configure Global SNMPv2c Credentials, Configure Global SNMPv3 Credentials, and Configure Global HTTPS Credentials.

Prerequisites for Configuring IRCM on 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.

IRCM: Cisco AireOS Controller and Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Ensure the prerequisite for configuring IRCM is met. For more information, see Prerequisites for Configuring IRCM on Cisco Controller Device, on page 57.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window is displayed 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 the following:

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 Cisco DNA Center. See Integrate the Meraki Dashboard.
- Create the SSID. See Create SSIDs for an Enterprise Wireless Network.

Note The Meraki dashboard supports the following 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 59.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

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

Step 2 To view the Meraki dashboard, expand the **Global** site in the left pane, and select a building.

All Meraki dashboards available in the selected building are displayed.

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 is displayed, 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 is displayed. You can view the managed building in the primary location.

Step 8 Click **Select Secondary Managed AP Locations** to select 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 the following 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 **Work Items** window, click the menu icon and choose **Activities** > **Work Items**.

d) In the **Work Items** 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 the following:

1. Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
2. Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

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

Provision Remote Teleworker Devices

The following 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. The following 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, 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.

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.

[2] Supported with Cisco Aironet 1815 Teleworker Access Point only.

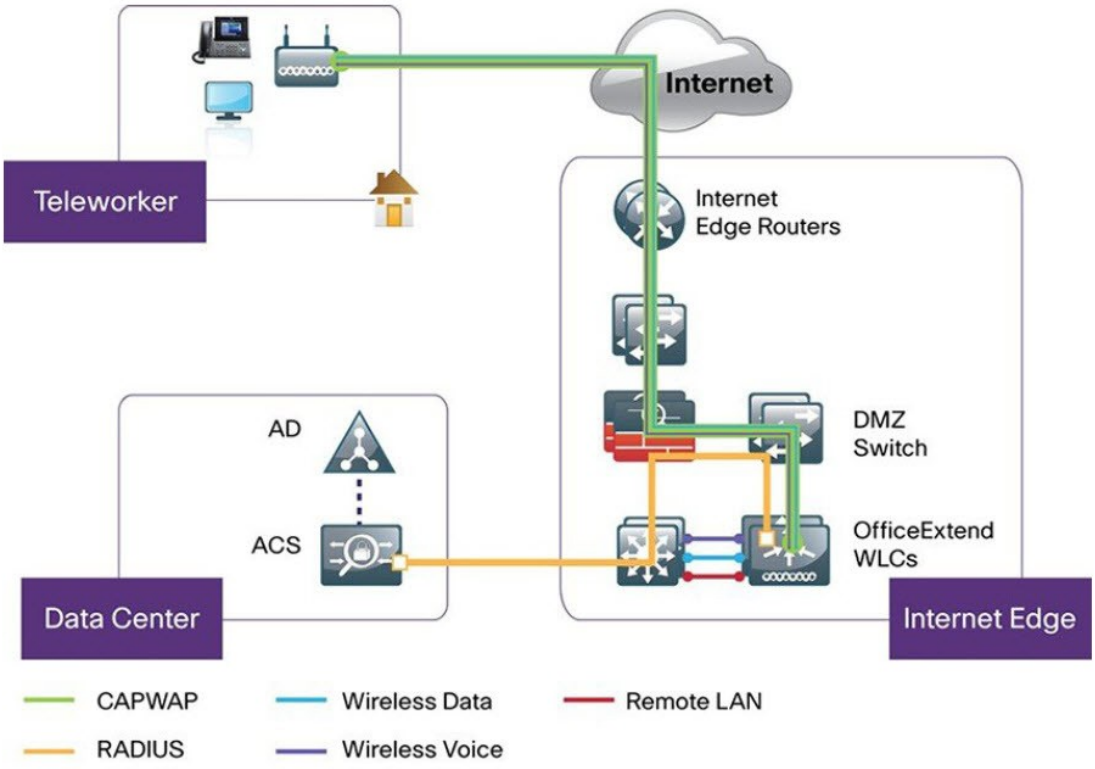
Corporate Firewall

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. Once enabled, the remote teleworker function cannot 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 cannot configure the network profile for Flex Connect 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 information, see Discover Your Network or Add a Network Device.
- Configure global wireless network settings appropriate for your network. For 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.

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 top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.
b) From the left hierarchy tree, choose 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 Add a Device to a Site.

Step 5 Assign the APs to the site. See Add a 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, choose Global.
b) From the top-left corner, click the menu icon and 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 top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The **Inventory** window is displayed 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.
h) Click **Next**.
i) In the **Model Configuration** 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**.

Step 8 After the Cisco Wireless Controller is provisioned, you can provision the APs.

a) From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The **Inventory** window is displayed 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**.