Configure Network Profiles

Network Profiles Overview

Network profiles allow you to configure settings and apply them to a specific site or group of sites. Cisco DNA Center supports up to 50 network profiles. You can create network profiles for various elements in Cisco DNA Center:

- Create Network Profiles for Assurance, on page 1

- Create Network Profiles for Firewall, on page 3

- Create Network Profiles for Routing, on page 4

- Create Network Profiles for Switching, on page 6

- Create Network Profiles for Wireless, on page 6

Create Network Profiles for Assurance

Creating a network profile for Assurance allows you to configure issue settings and apply them to a site or group of sites independently from the global issues settings. You can enable or disable an issue, and you can change its priority.

Notes:

- In Assurance, synchronization to the network device health score is available only for global issue settings, not custom issue settings. For information, see the *Cisco DNA Assurance User Guide*.

- Some global issues are not customizable. These issues are not displayed in the list of custom issues for you to modify.

- To display modified issues at the top of the list, sort by **Last Modified**.

- To delete custom settings, you must first unassign all the sites.

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

Step 2   Click +**Add Profile** and choose **Assurance**.

Step 3   In the **Profile Name** field, enter a valid profile name and click **Next**.

Cisco DNA Center adds the profile and the **Edit Profile** window appears.

Step 4   Set the **DEVICE TYPE** and **CATEGORY** filters to view the type of issues you want to configure.

Step 5   Click an issue in the **Issue Name** column to open a slide-in pane with the settings.

Note   For some issues, changes made to the settings are shared across multiple device types. In the slide-in pane, Cisco DNA Center displays a caution that indicates the affected device types.

Step 6   To enable or disable whether Cisco DNA Center monitors the issue, click the **Enabled** toggle button.

Step 7   To set the issue priority, click the **Priority** drop-down list and select the priority. The options are:

- **P1**: A critical issue that needs immediate attention and can have a wide impact on network operations.

- **P2**: A major issue that can potentially impact multiple devices or clients.

- **P3**: A minor issue that has a localized or minimal impact.

- **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

Step 8   (For certain issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Examples of a trigger condition:

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
Memory Utilization of Access Points greater than 90%.
```

Step 9   (Optional) If there are any changes to the settings, you can hover your cursor over **View Default Settings** to display the default settings. Click **Use Default** to restore all the issue settings to the default values.

Step 10   Click **Apply**.

Step 11   (For certain issues) Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered.

Step 12   To assign the profile to sites, click **Assign Sites**. Check the check box next to the sites that you want to associate with this profile and click **Save**.

The **Edit Profile** window appears.

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

Step 13   Click **Done**.

The newly added profile appears on the **Network Profiles** window.

Create Network Profiles for Firewall

This workflow shows how to:

1. Create custom configurations.

2. Create Firepower Threat Defense (FTD) configurations.

3. View the profile summary.

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

Step 2 Click +**Add Profile** and choose **Firewall**.

The **Firewall Type** page appears.

Step 3 To create custom configurations for regular firewalls like Adaptive Security Appliance (ASA) firewalls, do the following:

a) In the **Name** field, enter the profile name.

b) Choose the number of devices from the **Devices** drop-down list.

Note You can choose up to 10 devices per profile.

c) Choose the type of device from the **Device Type** drop-down list.

d) (Optional) From the **Device Tag** drop-down list, choose the device tags.

e) Click **Next**.

The **Custom Configuration** page appears.

f) From the **Template** drop-down list, choose a template.

Note If there are no templates, you must create at least one template in **Tools** > **Template Hub**. For information, see Create Templates.

g) Click **Next**.

The **Summary** page appears. This page summarizes the custom configurations. Based on the selected device type, a hardware recommendation is provided.

h) Click **Save**.

The **Network Profiles** page appears.

i) To assign a site to the network profile, click **Assign Sites**. For more information, see Create, Edit and Delete a Site.

Step 4 To create FTD configurations to configure the FTD devices, do the following:

a) In the **Name** field, enter the profile name.

b) From the **Devices** drop-down list, choose the number of devices.

Note You can choose up to 10 devices per profile.

c) To provision an FTD firewall, check the **FTD** check box.

d) From the **Device Type** drop-down list, choose the type of device.

e) (Optional) Choose the device tags from the **Device Tag** drop-down list.

f) Click **Next**.

The **FTD Configuration** page appears.

g) Click the **Routed Mode** or **Transparent Mode** radio button.

h) Click **Next**.

The **Summary** page appears. This page summarizes the FTD configurations. Based on the selected device type, hardware recommendation is provided on this page.

i) Click **Save**.

The **Network Profiles** page appears.

j) To assign a site to the network profile, click **Assign Sites**. For information, see Create, Edit and Delete a Site.

Create Network Profiles for Routing

This workflow shows how to:

1. Configure the router WAN.

2. Configure the router LAN.

3. Configure the integrated switch configuration.

4. Create custom configurations.

5. View the profile summary.

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

Step 2 Click + **Add Profile** and choose **Routing**.

Step 3 The **Router WAN Configuration** window is displayed.

- Enter the profile name in the **Name** text box.

- Select the number of **Service Providers** and **Devices** from the drop-down list. Up to three service providers and ten devices are supported per profile.

- Select the **Service Provider Profile** from the drop-down list. For more information, see Configure Service Provider Profiles.

- Select the **Device Type** from the drop-down list.

- Enter a unique string in the **Device Tag** to identify the different devices, or select an existing tag from the drop-down list. Use the device tag if two or more devices are of the same type. If all the devices are of a different type, the device tag is optional. Select the appropriate tag, because your selection is used as part of the matching criteria for day-zero and day-n templates applied to the network profile.

- To enable at least one line link for each device to proceed, click **O** and check the check box next to **Connect**. Select the **Line Type** from the drop-down list. Click **OK**.

  If you select multiple service providers, you can select the primary interface as gigabit Ethernet and the secondary as cellular, or both the interfaces as gigabit Ethernet. You can also select the primary interface as cellular and the secondary interface as gigabit Ethernet.

| Note | Only Cisco 1100 Series Integrated Services Routers, Cisco 4200 Series Integrated Services Routers, Cisco 4300 Series Integrated Services Routers, and Cisco 4400 Series Integrated Services Routers support the cellular interface. |

• Click **Next**.

Step 4 The **Router LAN Configuration** page is displayed.

• Click the **Configure Connection** radio button and choose L2, L3, or both.

• If you choose **L2**, select the **Type** from the drop-down list and enter the **VLAN ID/Allowed VLAN** and the **Description**.

• If you choose **L3**, select the **Protocol Routing** from the drop-down list and enter the **Protocol Qualifier**.

You can click **Skip** to skip the configuration.

• Click **Next**.

Step 5 The **Integrated Switch Configuration** page is displayed.

The integrated switch configuration allows you to add new VLANs or retain the previous configuration selected in the router LAN configuration.

• To add one or more new VLANs, click +.

• To delete a VLAN, click **x**.

• Click **Next**.

| Note | Switchport Interface support is available only for Cisco 1100 Series and Cisco 4000 series Integrated Services Routers. |

Step 6 The **Custom Configuration** page is displayed.

The custom configurations are optional. You can skip this step and apply the configurations at any time in the Network Profiles page.

If you choose to add custom configurations:

• Click the **Onboarding Template(s)** or **Day-N Templates** tab, as required.

• Choose a template from the drop-down list. The templates are filtered by **Device Type** and **Tag Name**.

• Click **Next**.

Step 7 On the **Summary** page, click **Save**.

This page summarizes the router configurations. Based on the devices and services selected, the hardware recommendation is provided.

Step 8 The **Network Profiles** page is displayed.

Click **Assign Sites** to assign a site to the network profile. For more information, see Create, Edit and Delete a Site.

Create Network Profiles for Switching

You can apply two types of configuration templates to a switching profile:

- Onboarding template
- Day-*n* template

Before you begin

Define the **Onboarding Configuration** template that you want to apply to the devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. See Create Templates to Automate Device Configuration Changes.

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

Step 2   Click **+Add Profile** and choose **Switching**.

Step 3   In the Switching profile window, enter the profile name in the **Profile Name** text box.

Depending on the type of template that you want to create, click **OnBoarding Template(s)** or **Day-N Template(s)**.

- Click **+Add**.
- Select **Switches and Hubs** from the **Device Type** drop-down list.
- Select the **Tag Name** from the drop-down list. This step is optional. If the tag that you selected has already been associated with a template, only that template is available in the Template drop-down list.
- Select the **Device Type** from the drop-down list.
- Select a **Template** from the drop-down list. You can select the Onboarding Configuration template that you have already created.

Step 4   Click **Save**.

The profile that is configured on the switch is applied when the switch is provisioned. Note that you must add the network profile to a site for it to be effective.

Create Network Profiles for Wireless

Before you begin

- Ensure that you have created wireless SSIDs, RF profiles, and AP profiles under the **Design** > **Network Settings** > **Wireless** tab.
- If necessary, ensure that you have created templates in the **Tools** > **Template Hub** window.
- If necessary, ensure that you have created model configuration designs in the **Tools** > **Model Config Editor** window.

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

Step 2   Click **Add Profile** and choose **Wireless**.

Step 3   Enter a valid profile name in the **Profile Name** field.

Step 4   To add sites to the profile, click **Assign** and do the following:

a) In the **Add Sites to Profile** slide-in pane, check the check box next to the sites that you want to associate with this profile.

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

b) Click **Save**.

Step 5   Configure the required settings in the following tabs:

- **SSIDs**: For more information, see Add SSIDs to a Network Profile, on page 7.

- (Optional) **AP Zones**: For more information, see Add AP Zones to a Network Profile, on page 9.

- **Model Configs**: For more information, see Add Model Configurations to a Network Profile, on page 10.

- **Templates**: For more information, see Add Templates to a Network Profile, on page 10.

- (Optional) **Advanced Settings**: For more information, see Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 11 and Configure Additional Interfaces for a Network Profile, on page 18.

Step 6   Click **Save** to add the network profile.

Cisco DNA Center displays the new network profile on the **Design** > **Network Profiles** window.

Add SSIDs to a Network Profile

Before you begin

Ensure that you have created wireless SSIDs under the **Design** > **Network Settings** > **Wireless** > **SSIDs** window.

Step 1   In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), click the **SSID** tab.

Step 2   Click **Add SSID**.

Step 3   From the **SSID** drop-down list, choose the SSID that you have already created.

Step 4   (Optional) In the **WLAN Profile Name** field, enter a name for the WLAN profile.

Based on the WLAN profile name, Cisco DNA Center automatically generates the policy profile name.

Note	• If an SSID associated with a network profile doesn't have site-level overrides on the **Design** > **Network Settings** > **Wireless** window, Cisco DNA Center uses the WLAN profile name available in the network profile during provisioning.
	• If you need to associate an SSID that has site-level overrides on the **Design** > **Network Settings** > **Wireless** window (for configurations such as fabric, FlexConnect, guest anchor, user interfaces, scheduler, and so on) with multiple network profiles, ensure that the WLAN profile name is unique for the SSID across all network profiles to prevent provisioning failure. If an SSID associated with a network profile has site-level overrides, Cisco DNA Center uses the WLAN profile name available in the overriden SSID during provisioning for the corresponding sites.
	• If you modify the WLAN profile name for an existing SSID that is provisioned on a wireless controller, during the wireless controller reprovisioning, this SSID is deleted and recreated with the new WLAN profile name.
	• When you upgrade to this release from a release earlier than Release 2.3.5, Cisco DNA Center populates the provisioned WLAN profile name and policy profile name to the corresponding existing SSIDs.

Step 5 Specify whether the SSID is fabric or nonfabric using the **Yes** or **No** radio buttons.

To create a nonfabric SSID, click **No**, and configure the following parameters:

- Click the **Enable SSID Scheduler** toggle button and choose the scheduler from the drop-down list.

- To use an interface for traffic switching, click the **Interface** radio button. From the **Interface Name** drop-down list, choose an interface name for the SSID, or click the plus icon (⊕) to create a wireless interface.

- To use a VLAN group for traffic switching, click the **VLAN Group** radio button. From the **VLAN Group Name** drop-down list, choose a VLAN group name for the SSID, or click the plus icon (⊕) to create a VLAN group.

- In the **Do you need Anchor for this SSID?** area, click **Yes** to add an anchor to the SSID. By default, **No** is selected.

- If you choose **Yes**, from the **Select Anchor Group** drop-down list, choose an anchor group for the SSID. For more information about anchor groups, see Create an Anchor Group.

- If you choose **No**, to enable local switching for WLAN, check the **Flex Connect Local Switching**.

  If you add an anchor to the SSID, you can't enable **Flex Connect Local Switching**.

Note	If you modify any nonflex SSIDs that are already provisioned on the wireless controller to flex SSIDs (or conversely), you must reprovision the wireless controller. If you don't reprovision the wireless controller, the expected intent isn't configured on the wireless controller. For example, if you modify a nonflex SSID to flex SSID and don't reprovision the wireless controller, the SSID remains nonflex on the wireless controller and flex site tags aren't created.

  If you enable **Flex Connect Local Switching** for an SSID, all the APs on the floor where the network profile is mapped, switch to FlexConnect mode.

  The **Flex Group** option is enabled in the **Advanced Settings** tab. For more information, see Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 11.

  When you enable local switching, any FlexConnect AP that advertises this WLAN can locally switch data packets.

- If you have enabled the **Flex Connect Local Switching** check box, enter a value for the VLAN ID in the **Local to VLAN** field.

Note	When you modify the local VLAN ID of an existing SSID and reprovision the AP without reprovisioning the wireless controller, the latest value of the local VLAN ID is updated in the flex profile used by the AP. If the same flex profile is used by other APs, these APs also have the updated local VLAN ID.

Step 6 (Optional) To add another SSID, click the plus icon (➕) and configure its parameters.

What to do next

Configure the other necessary settings for the network profile. For more information, see Create Network Profiles for Wireless, on page 6.

Add AP Zones to a Network Profile

An AP zone allows you to associate different SSIDs and RF profiles for a set of APs on the same site. You can use device tags to identify the APs for which you want to apply AP zone. From the **AP Zones** tab, you can create separate AP zones with a subset of SSIDs configured in the network profile for a device tag.

Cisco DNA Center applies the AP zone configurations to APs during AP provisioning.

Note	• Cisco DNA Center doesn't apply AP zone configurations to the APs claimed from the Plug and Play (PnP) process.
	• If an AP zone is already provisioned on an AP and you update the AP zone configuration, you must reprovision the wireless controller. Reprovisioning the AP is not necessary.

During AP provisioning:

- Based on the device tag and site of the AP, Cisco DNA Center selects the corresponding AP zone and automatically assigns the RF profile.
- If two AP zones are configured for an AP, you can choose the required AP zone.
- If there are no AP zones for an AP, you can choose the required RF profile.

Before you begin

Ensure that you have created wireless SSIDs under the **Design** > **Network Settings** > **Wireless** > **SSIDs** window.

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), click the **AP Zones** tab.
Step 2 Click **Add AP Zone**.
Step 3 In the **AP Zone Name** field, enter a name for the AP zone.
Step 4 From the **Device Tags** drop-down list, check the check box next to the device tags that you want to choose.
Step 5 From the **RF Profile** drop-down list, choose an RF profile.

Step 6 From the **SSID** drop-down list, choose the SSIDs.

Step 7 (Optional) To add another AP zone, click the plus icon ( ) and configure its parameters.

What to do next

Configure the other necessary settings for the network profile. For more information, see Create Network Profiles for Wireless, on page 6.

To apply the AP zone configuration to an AP:

1. Reprovision the wireless controller. For more information, see Provision a Cisco AireOS Controller and Provision a Cisco Catalyst 9800 Series Wireless Controller.

2. Provision the AP. For more information, see Provision a Cisco AP—Day 1 AP Provisioning.

Add Model Configurations to a Network Profile

You can attach model configuration designs to a network profile.

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), click the **Model Configs** tab.

Step 2 Click **Add Model Config**.

Step 3 In the **Add Model Config** slide-in pane, do the following:

   a. Click **Device Type(s)** and choose a device type.

      You can either search for a device name by entering its name in the **Search** field, or expand **Switches and Hubs** or **Wireless Controller** and choose a device type.

   b. Expand **Wireless** and choose the model configuration designs that you want to attach to this network profile.

   c. From the **Tags** drop-down list under **APPLICABILITY**, choose the applicable tags.

   d. Click **Add**.

What to do next

Configure the other necessary settings for the network profile. For more information, see Create Network Profiles for Wireless, on page 6.

Add Templates to a Network Profile

You can associate a template with a network profile.

Before you begin

You must create the necessary templates in the **Tools** > **Template Hub** window. For more information, see Create Templates.

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), click the **Templates** tab.

Step 2 Do the following:

- To associate an onboarding template, click the **OnBoarding Template(s)** tab.

- To associate a day-*n* template, click the **Day-N Template(s)** tab.

Step 3 Click **Attach Templates**.

Step 4 In the **Add Template** slide-in pane, do the following:

a) Under **Templates**, click a template name.

You can either search for a template by entering its name in the **Search** field, or expand a project and choose a template.

b) Click **Add**.

What to do next

Configure the other necessary settings for the network profile. For more information, see Create Network Profiles for Wireless, on page 6.

Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile

Cisco DNA Center allows you to add AP groups, flex groups, site tags, and policy tags in a network profile. Preprovisioning AP groups and flex groups saves time during AP provisioning by eliminating the need to make repetitive configuration changes and ensures consistency across your devices. You can define custom names for AP groups, site tags, and policy tags in the **Advanced Settings** tab of the **Design** > **Network Profiles** > **Wireless** window.

Note Flex group configuration is available only when the network profile has at least one associated flex-based SSID.

Cisco DNA Center configures and applies the newly added custom names specified in the **Provision Group** settings of the **Advanced Settings** tab to the APs during Cisco Wireless Controller provisioning. If you don't configure the custom names, Cisco DNA Center uses the autogenerated AP group names and tags for the APs.

Note

- AP group and flex group configurations are applicable to Cisco AireOS Wireless Controllers.

- Site tag and policy tag configurations are applicable to Cisco Catalyst 9800 Series Wireless Controllers.

  Newly added site tag and policy tag configurations are applied when you provision the APs. Provisioning the wireless controller alone won't configure the new custom tags on the APs. You must reprovision the wireless controller or the APs if there are any modifications to the tags after provisioning.

  Note the following scenarios while provisioning or reprovisioning the wireless controller and APs:

  - If there are no custom site or policy tags configured on the network profile, then Cisco DNA Center uses the autogenerated tags and configures it on the wireless controller and applies to the APs only during AP provisioning.

  - If there are custom site or policy tags configured on the network profile, then Cisco DNA Center configures the custom tags on the wireless controller and applies to the APs only during AP provisioning.

  - If the wireless controller and AP are already provisioned with autogenerated tags and if you create new custom tags in the network profile, then you must reprovision the wireless controller or the AP to apply the changes.

  - If the wireless controller and AP are already provisioned with custom tags and if you delete the custom tags from the network profile, then you must reprovision the wireless controller or the APs.

    - Reprovisioning the wireless controller deletes the custom tag configurations and configures the autogenerated tags on the wireless controller and the associated APs.

    - Reprovisioning the APs directly, without reprovisioning the wireless controller, configures the autogenerated tags on the APs but doesn't delete the custom tag configurations from the wireless controller. The tags are deleted during the next wireless controller reprovisioning.

  - If you've upgraded to Cisco DNA Center with FlexConnect Native VLAN override configured and site tags that are mapped to the same custom Flex profile for all the floors in a site, then you must reconfigure the network profile with different site tags for each floor or else provisioning may fail.

You can use the same AP groups and flex groups across sites (buildings or floors) within an area. However, you can't reuse the same AP groups and flex groups across multiple areas in the network hierarchy. Child sites inherit the AP groups and flex groups from their parent sites. However, if you create AP groups or flex groups for a child site, it overrides the settings inherited from its parent site. If an SSID is overridden for different floors in a building, you can't reuse the AP groups or flex groups for such floors.

Custom policy tags can be reused across sites (areas, buildings, and floors). When you assign a custom policy tag to a site—an area, a building or multiple floors in a building, all APs provisioned to that site and AP zone can use the same custom policy tag. By default, the custom policy tags are applicable for APs in the default AP zone; for custom AP zones, edit the policy tag and assign the custom policy tag to the required zones.

Note the following while reusing the custom policy tags:

- Child sites inherit the custom policy tags from the parent sites. However, if you create another policy tag for the child site, then it overrides the settings inherited from the parent site.

- A custom policy tag can be assigned to multiple sites and multiple AP zones. All AP zones associated with the policy tag must share the same set of SSIDs and the SSIDs must have the same configuration.

If a policy tag is associated to multiple AP zones that have different SSID configuration, an error is shown while editing the policy tag or the network profile.

- A custom policy tag cannot be shared when any of the sites that share the custom policy tag and are managed by the same wireless controller, have different SSID configurations due to a site-level SSID override. In such cases, a validation error occurs during provisioning—either AP provisioning or wireless controller provisioning (if skip AP provision is unchecked) due to different WLAN profile and policy profile mappings for the same custom policy tag. An error message with the reason for failure is displayed in the configuration preview. The error message provides details for up to five sites that have a mismatch for the custom policy tag. For more information on the custom policy tag usage, see Custom Policy Tag Reuse Use Case Examples, on page 14.

- Custom policy tag reuse is supported when learning device configurations from a pre-existing infrastructure as well.

- Policy tags are mapped to WLAN and RLAN profiles. Any changes in the policy tag may impact the RLAN configurations.

- Policy tag reuse is not supported for Cisco DNA Center autogenerated tags.

Before you begin

- Ensure that you have assigned a site to the network profile.

- To create flex group names, under the **SSIDs** tab, ensure that you have checked the **Flex Connect Local Switching** check box and defined the VLAN ID in the **Local to VLAN** field to mark the nonfabric SSID as a flex-based SSID. For more information, see Add SSIDs to a Network Profile, on page 7.

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

Step 1   In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), hover your cursor over **Advanced Settings** and click **Provision Group**.

Step 2   (Optional) To create an AP group in the network profile, expand **AP Groups and AP Profiles** and click **Create Custom AP Group**.

In the **Add AP Group** slide-in pane, do the following:

a)   In the **AP Group Name** field, enter the AP group name.

b)   From the **AP Zone** drop-down list, choose an AP zone.

To broadcast all the SSIDs associated with the network profile, choose **Not Applicable**.

Note   This drop-down list is enabled if you have added AP zones to the network profile in the **AP Zones** tab. For more information, see Add AP Zones to a Network Profile, on page 9.

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

c)   From the **AP Profile** drop-down list, choose an AP profile.

To create an AP profile, click **Create New**. For more information, see AP Profiles.

d)   From the **RF Profile** drop-down list, choose an RF profile.

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

e) In the **Select Sites** area, you can either search for a site by entering its name or expand **Global** to choose a site.

f) Click **Save**.

Step 3 (Optional) To create a flex group in the network profile, expand **Flex Group** and click **Create Flex Group**.

In the **Create Flex Group** slide-in pane, do the following:

a) In the **Flex Group Name** field, enter the flex group name.

b) In the **Select Sites** area, you can either search for a site by entering its name or expand **Global** to choose a site.

c) Click **Save**.

Step 4 (Optional) To create a site tag in the network profile, expand **Site Tags and AP Profiles** and click **Create Custom Site Tag**.

In the **Create Site Tag** slide-in pane, do the following:

a) In the **Site Tag Name** field, enter the site tag name.

b) From the **AP Profile** drop-down list, choose an AP profile.

To create an AP profile, click **Create New**. For more information, see AP Profiles.

c) In the **Flex Profile Name** field, enter the flex profile name.

Note	To enable the **Flex Profile Name** field, in the **SSID** tab, check the **Flex Connect Local Switching** check box. For more information, see Add SSIDs to a Network Profile, on page 7.

d) In the **Select Sites** area, you can either search for a site by entering its name, or expand **Global** to choose a site.

You can select multiple areas under an area.

e) Click **Save**.

Step 5 (Optional) To create a policy tag in the network profile, expand **Policy Tag** and click **Create Policy Tag**.

In the **Create Policy Tag** slide-in pane, do the following:

a) In the **Policy Tag Name** field, enter the policy tag name.

b) From the **AP Zone** drop-down list, choose an AP zone.

Note	This drop-down list is enabled if you have added AP zones to the network profile in the **AP Zones** tab. For more information, see Add AP Zones to a Network Profile, on page 9.

c) In the **Select Sites** area, you can either search for a site by entering its name or expand **Global** to choose a site.

d) Click **Save**.

What to do next

Configure the other necessary settings for the network profile. For more information, see Create Network Profiles for Wireless, on page 6.

Custom Policy Tag Reuse Use Case Examples

Scenario 1

A custom policy tag is shared between multiple sites with no site overrides and all sites are managed by the same Cisco Wireless Controller.

Site	Site Override	Policy Tag and AP Zone	Primary wireless controller
Building 1/Floor 1	None	*Custom Policy Tag 1, default-zone*	*wireless controller 1*
Building 1/Floor 2	None	*Custom Policy Tag 1, default-zone*	*wireless controller 1*

In this scenario, the custom policy tags can be shared between the sites and the APs can be successfully provisioned to these sites using the same custom policy tag.

Scenario 2

A custom policy tag is shared between multiple sites where some sites have site overrides for SSID and all the sites are managed by the same wireless controller.

Site	Site Override	Policy Tag and AP Zone	Primary wireless controller
Building 1/Floor 1	Site Override	*Custom Policy Tag 1, default-zone*	*wireless controller 1*
Building 1/Floor 2	None	*Custom Policy Tag 1, default-zone*	*wireless controller 1*

In this scenario, the custom policy tag cannot be reused because the same tag has two different WLAN profile and policy profile mappings for the same SSID. If you provision APs to these sites using the same custom policy tag, a validation error occurs during provisioning.

✎
Note The AP provisioning for the first site in this site hierarchy (*Building 1/Floor 1*) will be successful but a validation error is shown during the second AP provisioning at *Building 1/Floor 2*, which is attempting to reuse the custom policy tag.

Scenario 3

A custom policy tag is shared between multiple sites where some sites have site overrides for SSID and the sites are managed by different primary wireless controllers.

Site	Site Override	Policy Tag and AP Zone	Primary wireless controller
Building 1/Floor 1	Site Override	*Custom Policy Tag 1, default-zone*	*wireless controller 2*
Building 1/Floor 2	None	*Custom Policy Tag 1, default-zone*	*wireless controller 1*

In this scenario, the custom policy tags can be reused and the APs can be successfully provisioned to these sites using the same custom policy tag.

Scenario 4

A custom policy tag is shared between sites which have different policy profile (learned from pre-existing infrastructure) and all the sites are managed by the same wireless controller.

Site	Site Override	Policy Profile	Policy Tag and AP Zone	Primary wireless controller
Building 1/Floor 1	None	*Profile 1* (learned from pre-existing infrastructure)	*Custom Policy Tag 1, default-zone*	*wireless controller 1*
Building 1/Floor 2	None	*Profile 2* (learned from pre-existing infrastructure)	*Custom Policy Tag 1, default-zone*	*wireless controller 1*

In this scenario, the custom policy tag cannot be reused because the same tag is mapped to two different policy profiles for the same SSID on the same wireless controller. If you provision APs to these sites using the same custom policy tag, a validation error occurs during provisioning.

Note The AP provisioning for the first site in this site hierarchy (*Building 1/Floor 1*) will be successful but a validation error is shown during the second AP provisioning at *Building 1/Floor 2*, which is attempting to reuse the custom policy tag.

Scenario 5

A custom policy tag is shared between multiple sites where some sites have no site overrides for the primary wireless controller and some sites have overrides for the secondary wireless controller. All the sites are managed by the same primary wireless controller and have N+1 HA configured.

Site	Site Override	Policy Tag and AP Zone	Primary wireless controller	Secondary wireless controller
Building 1/Floor 1	No Override from Global level	*Custom Policy Tag 1, default -zone*	*wireless controller 2*	-
Building 2	Site Override	*Custom Policy Tag 1, default -zone*	*wireless controller 1*	*wireless controller 2*
Building 2/Floor 1	No Override from *Building 2*	*Custom Policy Tag 1, default -zone*	*wireless controller 1*	*wireless controller 2*
Building 2/Floor 2	No Override from *Building 2*	*Custom Policy Tag 1, default -zone*	*wireless controller 1*	*wireless controller 2*

In this scenario, since all the sites are managed by the same N+1 wireless controller, the custom policy tag cannot be reused for *wireless controller 2* because the same tag has two different WLAN profile and policy profile mappings for the same SSID on the same wireless controller (*wireless controller 2*). A validation error occurs when you provision *wireless controller 2*. However, there's no error expected while provisioning the *wireless controller 1*.

✎

| Note | Validation is done independently for each of the wireless controllers. |

Scenario 6

A custom policy tag is shared across areas with the same network profile.

Site	Site Override	Policy Tag and AP Zone	Primary wireless controller
Area 1/Building 1/Floor 1	None	*Custom Policy Tag 1, default-zone*	*wireless controller 1*
Area 2/Building 2/Floor 1	None	*Custom Policy Tag 1, default-zone*	*wireless controller 1 or 2*

In this scenario, custom policy tags can be shared across wireless controllers managing different areas under the same network profile.

Scenario 7

A custom policy tag is shared across areas with multiple network profiles.

Example 1

Site	Network Profile	Site Override	Policy Tag and AP Zone	Primary wireless controller
Area 1/Building 1/Floor 1	*Profile 1*	None	*Custom Policy Tag 1, default-zone*	*wireless controller 1*
Area 2/Building 2/Floor 1	*Profile 2*	None	*Custom Policy Tag 1, default-zone*	*wireless controller 1 or 2*

In the above example, custom policy tag can be reused across areas with different network profiles.

Example 2

Site	Network Profile	Site Override	Policy Tag and AP Zone	Primary wireless controller
Area 1/Building 1/Floor 1	*Profile 1*	None	*Custom Policy Tag 1, default-zone*	*wireless controller 1*
Area 2/Building 2/Floor 1	*Profile 2*	Site Override in *Area 2*	*Custom Policy Tag 1, default-zone*	*wireless controller 1 or 2*

In the above example, the custom policy tag cannot be reused due to site override in *Area 2*.

Scenario 8

A custom policy tag is shared across multiple AP zones.

Example 1

Site	Site Override	Policy Tag and AP Zone	Primary wireless controller
Area 1/Building 1/Floor 1	None	*Custom Policy Tag 1, workarea (SSID 1)*	*wireless controller 1*
Area 2/Building 2/Floor 1	None	*Custom Policy Tag 1, corridor (SSID 1)*	*wireless controller 1*

In the above example, the same custom policy tag can be reused across two AP zones (*workarea, corridor*) when they have the same set of SSID (*SSID 1)*).

Example 2

Site	Site Override	Policy Tag and AP Zone	Primary wireless controller
Area 1/Building 1/Floor 1	None	*Custom Policy Tag 1, workarea (SSID 1, SSID 2)*	*wireless controller 1*
Area 2/Building 2/Floor 1	None	*Custom Policy Tag 1, corridor (SSID 1)*	*wireless controller 1*

In the above example, the custom policy tag cannot be reused because the AP zones do not have the same set of SSIDs.

Note Reconfiguring a shared custom policy tag (for example, swapping the AP zone for a policy tag with another tag) results in conflicting configurations for existing APs on different floors that are yet to be reprovisioned. This prevents provisioning because the APs that are yet to be provisioned are still using the old configuration. However, reconfiguration of a shared custom policy tag is allowed in cases where all the APs that share the tag are on the same floor. The APs are updated with the latest configuration when you reprovision the APs of all the zones.

Configure Additional Interfaces for a Network Profile

An additional interface on a Cisco Wireless Controller maps a WLAN to a VLAN or subnet. You can configure additional interfaces for a network profile for wireless.

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), hover your cursor over **Advanced Settings** and click **Additional Interface**.

Step 2 To create an additional interface, click **Create New Interface** and do the following:

a) In the **Interface Name** field of the **Add Interface** slide-in pane, enter a name for the interface.

b) In the **VLAN ID** field, enter a VLAN ID. The valid range is from 0 through 4094.

c) Click **Save**.

Alternatively, you can create an additional interface on the **Design** > **Network Settings** > **Wireless** > **Interfaces & VLAN Groups** > **Interfaces** window. For more information, see Create a Wireless Interface.

Step 3 To add additional interfaces to a network profile, do one of the following:

- Click the plus icon (+) next to the required additional interface.

- Click the additional interface name, and then click **Add Selected**.

  Note To choose multiple additional interfaces, press **Shift**, click the additional interface names, and then click **Add Selected**.

- To add all the additional interfaces, click **Add All**. You can use the **Search** field to filter the additional interfaces.

What to do next

After configuring the necessary settings for the network profile, click **Save**. For more information, see Create Network Profiles for Wireless, on page 6.