



Build and Deploy Workflows

- [Catalyst Center Workflow Navigation, on page 1](#)
- [Discover Devices, on page 1](#)
- [AP Refresh Workflow, on page 3](#)
- [Configure User-Defined Network, on page 6](#)
- [Enable Application Hosting on Switches, on page 9](#)
- [Enable IoT Services, on page 10](#)
- [AP Configuration in Catalyst Center, on page 11](#)
- [Learn Device Configurations from Devices with Pre-Existing Infrastructure, on page 24](#)
- [Replace Device, on page 28](#)
- [Create a Remote Support Authorization, on page 32](#)
- [Create an Event Notification, on page 33](#)
- [Configure Remote LAN, on page 36](#)

Catalyst Center Workflow Navigation

Catalyst Center workflows are similar to wizards. The workflows are embedded in the GUI to guide you through multistep tasks that would otherwise be too complex or advanced to complete. You can access many of them from various menu options or directly from the **Workflows** menu option.

Use these guidelines to help you navigate through the workflows:

- Follow the steps in the workflow and click **Next** to go to the next page.
- When you hover your cursor near the top of each page in the workflow, a **Progress bar** displays, showing you the steps to complete the process and which step you are currently on.
- Some workflows open a dialog box that you can click through to see a visual overview of the task. At any point in the task overview, you can click **Let's Do it** to jump directly to the beginning of the workflow. To skip the task overview in the future, check the **Don't show this to me again** check box.

Discover Devices

This workflow guides you from device discovery to network health.

Before you begin

- Your devices must have the required device configurations, as described in [Discovery Prerequisites](#).
- Enable CDP on your network devices, if you want to use CDP discovery protocol.
- Enable LLDP on your network devices, if you want to use LLDP discovery protocol.
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Step 1 From the top-left corner, click the menu icon and choose **Workflows > Discover Devices**.

Step 2 If a task overview window opens, click **Let's Do it** to go directly to the workflow.

Step 3 In the **Discover Devices** window, complete the following fields:

- a) Enter a name for the discovery job.
- b) Under **Discovery Type**, choose the protocol used to discover devices and complete the corresponding fields, as follows:
 - **CDP**: Enter the **IP Address**, **CDP Level**, and **Subnet Filter**.
 - **IP Address Range**: Enter the **Starting IP Address** and **Ending IP Address**.
 - **LLDP**: Enter the **IP Address**, **LLDP Level**, and **Subnet Filter**.
- c) Choose the **Preferred Management IP Address**.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential that Catalyst Center will configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see [Discovery Credentials](#).

- a) In the left pane, click **CLI** to add CLI credentials.
- b) Expand **SNMP** to add SNMP credentials.
- c) Expand **Advanced Settings** and configure the following settings:
 - **Protocol Order**: Choose **SSH** or **Telnet**. If you choose both, you can specify the order in which they are used by dragging the protocols up or down.
 - **SNMP Polling Properties**: Use the global SNMP polling properties defined in the **Network Settings > Device Credentials** window or modify for this discovery instance.

Note You can configure other credentials such as, NETCONF and HTTP(S), if required.

Step 5 In the **Schedule Job** window, do the following:

- a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.
If you choose the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.
- b) Click the toggle button to enable or disable the **Discover new devices only** option.
- c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box is displayed with information about the settings that will be enabled on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview will not be generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, choose any one of the following options:

- **Assign to site without Configuration Preview:** Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see [Search the Network Hierarchy](#).
- **Skip site assignment for now:** Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

You can view the status of the task in the **Activities > Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

AP Refresh Workflow

The AP Refresh feature allows you to replace both provisioned and unprovisioned older AP models with newer AP models, using the Access Point Refresh workflow. You can use this procedure to replace old APs with new ones in Catalyst Center for the following use cases:

- Automation use case: Deployments where wireless controller and APs are provisioned through Catalyst Center network intent configurations. After AP refresh, the new AP is provisioned with the network intent configuration.
- Assurance use case: Deployments where Catalyst Center is used primarily for Assurance purposes and the wireless controller and APs are not provisioned through Catalyst Center network intent configurations. The new AP isn't provisioned after AP refresh and only the old configuration is copied to the new AP.

For device compatibility information, see the [Catalyst Center Compatibility Matrix](#).

Before you begin

- Ensure that the old AP is in the Unreachable state and assigned to a site.
- The new AP must not be assigned to any site.
- For the automation use case, the old AP site must be provisioned as a managed AP location for the wireless controller to which the new AP is associated.
- For the Assurance use case, the new AP must join the same wireless controller where the old AP was previously associated.

- For the automation use case, you must connect the new AP to a wireless controller. The new AP must either be available in the Catalyst Center inventory or be able to contact Catalyst Center through Plug and Play (PnP). It must be in the Reachable state.
- For the Assurance use case, you must connect the new AP to a wireless controller. The new AP must be available in the Catalyst Center inventory.



Note The Assurance use case isn't supported for APs onboarded through PnP.

Step 1 From the top-left corner, click the menu icon and choose **Workflows > Access Point Refresh**.

Note If an **Overview** window opens, click **Let's Do it** to start the workflow.

Step 2 In the **Before you begin** window, view the prerequisites for the AP refresh workflow.

Step 3 In the **Get started** window, enter a unique name for the task.

Step 4 In the **Select your scenario** window, click the radio button next to the required use case: **Automation Usecase** or **Assurance Usecase**

Step 5 In the **Select Access Points** window, do the following:

- In the left pane, check the check box next to the floor where you want to refresh the AP.
- In the right pane, check the check box next to the device name that you want to replace.


Step 6 In the **Assign New APs to Old APs** window, do the following:

- (Optional) To automatically detect the new APs using SwitchPort, click the corresponding toggle button.

Ensure that the Cisco Discovery Protocol (CDP) is enabled on the wireless controller or AP for automatic detection of new APs.

Note Automatic detection of the new AP using SwitchPort isn't supported when it's onboarded through PnP.

When you enable the automatic detection of new APs, this workflow performs the following:

- If the new AP is connected to the same switch port where the old AP is connected, the serial number of the new AP is automatically populated.
 - If the new AP isn't onboarded yet, the serial number of the new AP is detected after it's discovered. Alternatively, you can enter the serial number of the new AP.
- Select a method through which you want to provide new AP details:
 - To add the new AP details using the GUI, click the edit icon () for the AP, and in the **Edit details** window, do the following:
 - (Optional) Update the new AP name.
 - (Optional) From the **Choose Platform ID** drop-down list, choose the platform of the new AP.
 - From the **Choose Serial Number** drop-down list, choose the serial number of the new AP.

If the new AP is already associated with a wireless controller and is available in the inventory, Catalyst Center displays the serial number of that AP as **Managed** in the **Choose Serial Number** drop-down list.

If the new AP has contacted Catalyst Center through PnP, Catalyst Center displays the serial number of that AP as **Unclaimed** in the **Choose Serial Number** drop-down list.

If the serial number of the new AP isn't available in the Inventory, the **Serial Number** drop-down list doesn't contain the serial number. To add a new serial number that isn't present in the inventory, from the **Choose Serial Number** drop-down list, enter the serial number and click +.

Note If you enable the automatic detection of new APs using SwitchPort, choosing the serial number is optional.

4. Click **Save**.

- To add the new AP details using a comma-separated value (CSV) file, do the following:
 1. Click **Download CSV**. The downloaded CSV template file contains the old AP details. Update the device name and add the serial number of the new AP.
 2. To import the CSV file, click **Upload CSV**.
 3. In the **Upload CSV** window, you can either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**.

Catalyst Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message is displayed. Click **View Details** to get more details about the error message.

4. Click **Upload**.

Step 7 In the **Configuration to be copied from Old APs to New** window, view the configuration that will be copied from the old AP to the new AP.

Step 8 If Catalyst Center detects any errors or unresolved dependencies, the **Resolve Dependencies** window is displayed. You must resolve any errors and dependencies before proceeding, including the following:

- **Device EULA Acceptance:** Accept the device End-User License Agreement (EULA) by providing your Cisco.com credentials.
- **Update the Cisco Wireless Controller software image version:** You must resolve this dependency even though it doesn't stop you from proceeding with the AP refresh.
- **AP Connected SwitchPort:** You must resolve this dependency even though it doesn't stop you from proceeding with the AP refresh.

Step 9 In the **Schedule Access Point Refresh Task** window, click **Now** or **Run Later** to schedule the AP refresh task for a later date and time.

Step 10 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 11 In the **Track Replacement Status** window, monitor the AP replacement status:

- If the AP replacement succeeds, the **Replacement Status** shows **REPLACED**.
- If the AP replacement fails, the **Replacement Status** shows **Error**.

Note If the new AP isn't yet discovered in the inventory and the corresponding AP refresh entry is waiting for the new device to be connected, or if the PnP claim process is in progress, resynchronize the Cisco Wireless Controller.

Step 12 (Optional) In the **Track Replacement Status** window, do any of the following:

- To view the latest AP replacement status, click **Refresh Data**.
- To get more information about the AP replacement status, click **View Details**.
- To delete a replacement entry, under the **Actions** column, click the three blue dots and click **Delete**. In the **Warning** dialog box, click **Yes**.
- To download the provisioning summary to a CSV file that you can save locally, click **Export**.
- To download the provisioning status report, click **Download Report**.

Step 13 Click **Next** to view the refresh summary.

After a successful replacement, an AP refresh event is generated in Cisco Catalyst Assurance for the old and new APs.

Step 14 (Optional) View the AP refresh event under **Event Viewer** in the **AP View 360** window.

Catalyst Center automatically updates the new APs on the respective floor maps in the **Network Hierarchy** window.

Configure User-Defined Network

The following sections provide information about configuring the Cisco User-Defined Network service using workflows in Catalyst Center.

Overview of User-Defined Network Service

Home, consumer, and IoT devices on the network, such as printers, speakers, Apple TV, Google Chromecast, ring doorbells, smart bulbs, and so on, depend on the Simple Service Discovery Protocols (SSDP) such as Apple Bonjour, multicast DNS (mDNS), and Universal Plug and Play (UPnP) to provide the easy discovery and usage of devices.

The Cisco User-Defined Network service provides secure and remote onboarding of client devices in shared environments such as dormitory rooms, residence halls, class rooms, and auditoriums. With the User-Defined Network service, users can securely use SSDPs such as Apple Bonjour, mDNS protocols such as AirPlay, AirPrint, Screen Mirroring, Print, or UPnP protocol to interact and share with only their registered device in the shared environment.

The User-Defined Network service provides the following solution:

- Easy and secure onboarding of client devices.
- Automatic segmentation of client devices that belong to a particular user.
- Ability to invite other users to share their devices.

Prerequisites for Configuring the User-Defined Network Service

Before configuring the Cisco User-Defined Network service, the following prerequisites must be completed:

- Confirm that APs have joined the Cisco Wireless Controller.
- Discover Cisco Wireless Controllers and APs in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.
- Map the AAA server client endpoint with Cisco Identity Services Engine.
- Add the authentication tokens to Catalyst Center.
- Create nonfabric enterprise SSIDs or guest wireless SSIDs with any security, and map them to the network profile.
- Provision SSIDs.

Configure Cisco User-Defined Network

This procedure shows how to configure the Cisco User-Defined Network (UDN) using workflows.

-
- Step 1** From the top-left corner, click the menu icon and choose **Workflows > Configure Cisco UDN**.
Alternatively, you can configure the Cisco UDN from **Provision > Services > Cisco User Defined Network**.
- Step 2** If a task overview window opens, click **Let's Do It** to go directly to the workflow.
- a) Click **Click here**.
The **Cloud Authentication** window opens.
 - b) Hover over **Where did I get my token encryption key?** and click **Go to the Portal**.
The Cisco Cloud Services application opens in a new tab.
 - c) Log in to Cisco Cloud Services using your Cisco.com account ID and password.
The Cisco Cloud Services home window lists the subscribed offers for your region as a card.
- Step 3** Generate an authentication token using the Cisco Cloud Services portal to allow Catalyst Center to connect with Cisco Cloud Services:
- a) In the Cisco Cloud Services GUI, click the menu icon and choose **Applications > Product** to register Catalyst Center to your cloud subscription.
By default, the **ALL** tab opens and is highlighted with a blue tick mark. You can register either from the **ALL** tab or from the **Cisco DNA Center** tab.
Note Catalyst Center registration fails intermittently on the Cisco Cloud Services portal. This is an intermittent issue that occurs during every alternate deregistration due to communication failure from Cisco Cloud Services to Catalyst Center in all regions.
 - b) To register from the **ALL** tab:
 - Click **Register**.
The **Register Product** slide-in pane appears.

- In the **Product Name** field, enter a name.
- From the **Product Type** drop-down list, choose **Cisco DNA Center**.
- Click **Register**.
- The **OTP Generated** dialog box appears after successful registration of Catalyst Center. To copy the OTP, click **Copy**, and click **close**.

c) Alternatively, to register from the **Cisco DNA Center** tab:

- Click **Register** to securely connect your products to the relevant cloud applications and services offered by Cisco and its partners.
The **Register Product** slide-in pane appears.
- In the **Cisco DNA Center Name** field, enter the name of the on-premises Catalyst Center.
- In the **OTP Generated** dialog box, click **Copy** to copy the OTP and click **close**.

Step 4 Navigate back to the **Cloud Authentication** window to establish the connection:

- a) In the Catalyst Center GUI, click the menu icon and choose **System > Settings > External Services > Cloud Authentication**.
- b) Click **Add OTP Key**.
- c) In the **OTP Code** field, paste the OTP that you generated and copied in the Cisco Cloud Services application, and click **Done**.
- d) In the **Success** dialog box, click **OK**.

Step 5 Verify whether the connection has been established between Catalyst Center and Cisco Cloud Services on the **Cisco Cloud Services > Applications > Products** window.

The **Registration Status** column shows the status as **Registered** after a successful registration.

Step 6 Enable sites and provision Cisco UDN services on your network:

- a) Navigate back to the **Welcome to Cisco User Defined Network** window in Catalyst Center.
- b) Click **Next**.
- c) In the **Select Sites** window, choose the sites where you want to enable the Cisco UDN service.
- d) In the **SSID(s)** window, do the following:
 - From the **SSID(s)** drop-down list, choose the SSIDs where you want to enable the Cisco UDN service.
 - To limit the unicast traffic for the selected SSID, turn on **Unicast Traffic Containment**.
 - Click **Apply Individually** to apply unicast traffic containment for a specific site.
 - Click **Apply to all** to apply the unicast traffic containment for all sites.
 - Click **Next**.

Step 7 In the **Scheduling** window, click **Now** or **Later** to indicate when you want to provision the Cisco UDN service. Then, click **Next**.

Step 8 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

- a) Expand the **Connection Status** area to view the connection status between Catalyst Center and Cisco UDN Cloud.

A "Paired with Cisco Cloud Services" message appears after establishing a connection between Catalyst Center and Cisco UDN Cloud.

- b) Click **Configure**.

In the next window, a check mark is shown next to each step as it completes.

Enable Application Hosting on Switches

The following procedure shows how to enable docker applications such as ThousandEyes Enterprise Agent and iPerf in selected switches at a specific site.

Before you begin

- Complete the prerequisites. For more information, see [Prerequisites for Application Hosting](#).
- Add the application to Catalyst Center. For more information, see [Add an Application](#).
- Check the readiness of the switch to host the application. For more information, see [View Device Readiness to Host an Application](#).

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

Step 2 Choose the application and click **Install** at the bottom of the window.

Alternatively, you can also launch the workflow by choosing **Workflows > Enable Apps on Switches > Let's Do it**.

Note At the top of the workflow window, place your cursor on the blue progress bar and switch back to the previous step listed.

Step 3 In the **Select Site** window, navigate to the building where you want to enable the application.

Step 4 In the **Select App** window, click on the application you want to select.

Note You can access the + **New App** link to add an application that is not present in Catalyst Center.

Step 5 In the **Select Switches** window, check the check box next to the device name for which you want to enable the application.

Note You can import or export devices in bulk by providing the details in the specified template in the **Select Switches** dialog box.

Step 6 Complete the following settings in the **Configuration App** window:

- **App Networking**

- **Device Network:** From the **Select Network** drop-down list, choose a VLAN to configure the application.

- **App IP address:** From the **Address Type** drop-down list, choose **Static** or **Dynamic**. If you choose **Static**, click the thumbnail icon and enter the **IP Address**, **Gateway**, **Prefix/Mask**, and **DNS** for the application.

- **Resource Allocation:** Check the **Allocate resources as asked by the app** or the **Allocate all resources available on the device** check box.

- **Custom Settings:** (Applicable only for Cisco package applications) Enter the configuration details for the attributes that are specified by the application.
- **App Data:** Browse and upload the application-specific files. To identify the required application-specific files, see the relevant application document.
- **Docker Runtime Options:** Enter the docker runtime options required by the application.

- Step 7** In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)
The **Provisioning Task** window displays the task name that tracks the deployment of the application on the switches.
- Step 8** Review the automatically generated task name and click **Provision**.
- Step 9** In the **Track Provisioning Status** window, you can track the progress of the deployment.
- Step 10** Click **View Details** to view the provisioning status of the individual devices and failures, if any and click **Next**.
The application is enabled successfully.
The summary of the task result and the success/failure counts are displayed.
- Step 11** Click **Manage App**, where you can manage the lifecycle operations of the application to perform day-*n* tasks.
-

Enable IoT Services

The following sections provide information about enabling IoT technologies such as Bluetooth, Zigbee, and ESL on Cisco Catalyst 9100 Series Access Points using **Workflows** in Catalyst Center.

Enable IoT Services on Cisco Catalyst 9100 Series Access Points

This procedure shows how to enable IoT technologies such as Bluetooth, Zigbee, and ESL on selected Catalyst 9100 Series Access Points.

- Step 1** From the top-left corner, click the menu icon and choose **Workflows > Enable IOT Services**.
- Step 2** If a task overview window opens, click **Let's Do It** to go directly to the workflow.
- Step 3** In the **Select Site** window, navigate to the floor where you want to enable the IoT service, and click **Next**.
- Step 4** In the **Select the Application** window, select the SES-imagotag ESL Connector application to enable IoT in your network, and click **Next**.

Note To add an application that is not present in the Catalyst Center, see [Add an Application](#).

The **Select Access Points** window shows all the APs available on the particular floor.

- Step 5** In the **Select Access Points** window, check the check box adjacent to the **Device Name** where you want to install the IoT connector application, and click **Next**.
- Step 6** In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)
- Step 7** The **Provisioning Task** window, which displays the task name created to track deployment of any application on APs, is displayed. Review the auto-generated task name and click **Provision**.

- Step 8** In the **Track Provisioning Status** window, you can track the progress of the deployment. Click **View Details** to view the provisioning status and click **Next**.
- Step 9** The **Done! Task Completed** window appears. Click **Manage IoT Application** to perform day-*n* tasks.
-

Manage IoT Applications

This procedure shows how to manage IoT applications.

Before you begin

You must have enabled IoT services on Cisco Catalyst 9000 Series Access Points.

- Step 1** After enabling IoT services, click **Manage IoT Application** in the **Done! Task Completed** window.
- Step 2** Check the check box next to the **Hostname** and perform the following tasks:
- To start the application, from the **Actions** drop-down list, choose **Start App**.
 - To stop the application, from the **Actions** drop-down list, choose **Stop App**.
 - To edit the application configuration, from the **Actions** drop-down list, choose **Edit App Config**.
 - To upgrade the application, from the **Actions** drop-down list, choose **Upgrade App**.
 - To uninstall the application from the selected AP, from the **Actions** drop-down list, choose **Uninstall App**.
- Step 3** Click the AP name to view details, such as the AP name, status, IP address, and health.
- Step 4** Click **Tech Support logs** to collect Application Hosting logs.
-

AP Configuration in Catalyst Center

The **Configure Access Points** workflow allows you to configure and deploy AP-level parameters, such as the AP location, admin status, mode, and so on. You can also configure radio-level parameters, such as the radio power level, channel settings, and so on.

Configure APs

This procedure shows how to configure AP and radio parameters in Catalyst Center.

The following settings configured using the **Configure Access Points** workflow aren't overwritten when the wireless controller or APs are reprovisioned:

- Admin status for radios (only applicable for Cisco AireOS Wireless Controllers)
- AP primary controller
- AP secondary controller



Note The AP configuration is generated from the information available in the Catalyst Center inventory. To ensure the latest configuration is generated, complete an inventory sync on the controller.

Step 1 From the top-left corner, click the menu icon and choose **Workflows > Configure Access Points**.
If the **Configure Your Access Points** dialog box displays, click **Let's Do It** to go directly to the workflow.

Step 2 In the **Get Started** window, enter a unique name for the workflow in the **Task Name** field and click **Next**.

Step 3 In the **How do you want to configure APs?** window, do the following:

- a) Click the **Configure AP And Radio Parameters** radio button.
- b) Check the check box next to the tasks that you want to perform:

- **Modify AP Name**
- **Configure AP Parameters**
- **Configure 5 GHz Radio Parameters**
- **Configure 2.4 GHz Radio Parameters**
- **Configure 6 GHz Radio Parameters**
- **Configure Dual-Band (XOR) Radio Parameters**
- **Configure Tri-Radio Parameters**
- **Create Template**

Note Based on the check boxes that you check, Catalyst Center displays the corresponding subsequent configuration steps.

- c) Click **Next**.

Step 4 In the **Select Access Points** window, do the following:

- a) Click one of the following tabs:
 - **Assigned APs**: Lists the APs that are assigned to a site.
 - **Unassigned APs**: Lists the APs that are not assigned to any site.
- b) If you chose the **Assigned APs** tab, navigate to the site where you want to apply AP-related configurations.
The right pane lists all the APs available in the selected site.

Note You can select up to 2000 sites in this window.

- c) If you chose the **Unassigned APs** tab, check the **Unassigned Devices** check box.
The right pane lists all the APs that are not assigned to any site.
- d) Check the check boxes next to the AP names that you want to configure.
We recommend that you select a maximum of 2000 APs in this window.

To filter APs based on specific details, click the search icon and choose from the filter options: **Quick Filters**, **Advanced Filters**, or **Recent Filters**. Choose the required option in the filter and click **Apply**.

To edit or customize the **Access Points** table, click the gear icon in the top-right corner of the table and do the following:

- To define the **Table Density**, click **Table Appearance**.
- To select the columns that you want to display in the table, click **Edit Table Columns**.
- To customize your current view, click **Edit Custom Views**.
- Click **Apply** to save the changes or click **Reset All Settings** to apply the default settings for the table.

e) Click **Next**.

Step 5

(Optional) In the **Modify AP Name** window, modify one or more AP names using one of the following methods:

- **Create a New Naming Convention:** Click this radio button, enter a name based on your naming convention, and click **Apply Pattern**. The **Access Points** table shows the new AP names based on the naming pattern that you entered.
- **Upload a CSV file:** Click this radio button, download the sample CSV template file, and add your AP names to it. Then, upload the CSV file either by dragging and dropping it into the drop area or by clicking **Choose a file** and browsing to select it.

Step 6

(Optional) In the **Configure AP Parameters** window, configure the AP parameters.

- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
- **AP Mode:** Check this check box and choose the AP mode from the **Select AP Mode** drop-down list. Valid modes are **Local/Flexconnect**, **Monitor**, **Sniffer**, and **Bridge/Flex+Bridge**.

Note When you change the AP mode from **Monitor** or **Sniffer** to **Local/Flexconnect**, Catalyst Center uses the following settings:

If **FlexConnect Local Switching** is enabled on any associated SSID, Catalyst Center sets **FlexConnect** mode on the AP. Otherwise, it sets **Local** mode on the AP.

For unassigned APs or APs that are assigned but not provisioned, Catalyst Center sets **FlexConnect** mode on the AP as follows:

- For Cisco AireOS Wireless Controller: If **FlexConnect Local Switching** is enabled on any associated SSID in the AP group where the AP is present.
- For Cisco Catalyst 9800 Series Wireless Controller: If **Local site** is disabled on the current associated site tag of the AP.

- **AP Location:** Check this check box to enter the AP location details in the **Enter Location** field.

To use the currently assigned site as the AP location, check the **Use currently assigned site location** check box. If you check this check box, the **Enter Location** field is disabled. You can view the AP location that is being configured for each AP by clicking **Click here to see location details** before pushing this change to the device.

Note If you check the **Use currently assigned site location check box**, for APs that are not assigned to any site, Catalyst Center doesn't configure the AP location.

- **AP LED Status:** To disable the APs LED status, check this check box and click **Disable**.

- **LED Brightness Level:** Check this check box and choose the brightness level from the **LED Brightness Level**.
- **AP Failover Priority:** Check this check box and, from the **AP Failover Priority** drop-down list, choose one of the following failover priorities:
 - **Low** (Default): Level 1 priority, which is the lowest priority level.
 - **Medium:** Level 2 priority.
 - **High:** Level 3 priority.
 - **Critical:** Level 4 priority, which is the highest priority level.
- **High Availability:** Check this check box and configure the primary, secondary, and tertiary controller name and the IP address for the AP.

If you choose **Inherit from site** / **Clear** for the primary and secondary controllers:

- For the APs that are in Provisioned state, the controllers that are configured as primary and secondary for the floor where the AP is assigned are configured as the primary and secondary controllers on the AP.
- For the APs that are not in Provisioned state, the current primary and secondary controller configuration is cleared from the AP.

For the tertiary controller, only the **Clear** option is available.

- Note**
- If AP fallback is disabled on the controller, the AP doesn't join the newly configured primary, secondary, and tertiary controller.
 - If the AP is a ROW AP, ensure that you have added support for the country of operation to the country list on the controller. You must configure at least one site from the country of operation as the managed AP location for the controller.

- **CleanAir Pro / CleanAir / Spectrum Intelligence:** To disable the CleanAir spectrum intelligence for 2.4-GHz, 5-GHz, or 6-GHz radio band, check the corresponding check box, and click **Disable**.

- Note** You can configure CleanAir spectrum intelligence only on CleanAir spectrum intelligence-capable APs that are in the **Local/FlexConnect** or **Monitor** modes. If CleanAir spectrum intelligence is disabled on the 802.11a network, the operational status is down for the AP.

- Note** The **AP Height** parameter is no longer available in the **Configure Access Points** workflow. You can configure the AP height in the **Design > Network Hierarchy** window. For more information, see [Edit an AP](#).

Step 7

(Optional) In the **Configure 5 GHz Radio Parameters** window, configure the 5-GHz radio parameters.

- a) To view the list of applicable APs for the 5-GHz radio parameter configuration, click **View Devices**.

Catalyst Center displays the **View Devices** option only when APs that support 5-GHz radio parameters are available.

- b) Configure the following 802.11 a/n/ac/ax parameters:

- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
- **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.

- **Channel Assignment:** To choose custom channel numbers, check this check box and click **Custom**. Choose a custom channel number from the **Select Custom Channel** drop-down list.
- **Channel Width:** To choose channel width, check this check box and choose the channel bandwidth.
- **Antenna Gain:** To choose an antenna, check this check box and choose an antenna from the **Select Antenna** drop-down list. If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 through 40.

Note The selected antenna name isn't reflected in wireless maps.

- **Antenna Cable:** To choose an antenna cable, check this check box and choose the antenna cable from the **Select Antenna Cable** drop-down list. If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 through 40.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design > Network Hierarchy** window. For more information, see [Edit an AP](#).

Step 8

(Optional) In the **Configure 2.4 GHz Radio Parameters** window, configure the 2.4-GHz radio parameters.

- a) To view the list of applicable APs for the 2.4-GHz radio parameter configuration, click **View Devices**.

Catalyst Center displays the **View Devices** option only when APs that support 2.4-GHz radio parameters are available.

- b) Configure the following 802.11 b/g/n parameters:

- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
- **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.
- **Channel Assignment:** To choose custom channel numbers, check this check box and click **Custom**. Choose a custom channel number from the **Select Custom Channel** drop-down list.
- **Antenna Gain:** To choose an antenna, check this check box and choose an antenna from the **Select Antenna** drop-down list. If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 through 40.

Note The selected antenna name isn't reflected in wireless maps.

- **Antenna Cable:** To choose an antenna cable, check this check box and choose the antenna cable from the **Select Antenna Cable** drop-down list. If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 through 40.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design > Network Hierarchy** window. For more information, see [Edit an AP](#).

Step 9

(Optional) In the **Configure 6 GHz Radio Parameters** window, configure the 6-GHz radio parameters.

- a) To view the list of applicable APs for the 6-GHz radio parameter configuration, click **View Devices**. Catalyst Center displays the **View Devices** option only when APs that support 6-GHz radio parameters are available.
- b) Configure the following parameters:
- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
 - **Radio Role Assignment:** To choose a radio role, check this check box and click **Auto**, **Client-Serving**, or **Monitor**.
 - **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.
 - **Channel Assignment:** To choose a custom channel number, check this check box and click **Custom**. Choose a custom channel number from the **Select Custom Channel** drop-down list.
 - **Channel Width:** To choose channel width, check this check box and choose the channel bandwidth.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design > Network Hierarchy** window. For more information, see [Edit an AP](#).

Step 10

(Optional) In the **Configure Dual-Band (XOR) Radio Parameters** window, configure the dual-band (XOR) radio parameters.

- a) To view the list of applicable APs for the dual-band (XOR) radio parameter configuration, click **View Devices**. Catalyst Center displays the **View Devices** option only when APs that support dual-band (XOR) parameters are available.

You can configure dual-band (XOR) radio parameters on the following APs:

- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst 9120 Series Access Points
- Cisco Catalyst 9166 Series Access Points

Note Cisco Catalyst 9166 Series Access Point supports dual-band (XOR) between 5-GHz and 6-GHz radio modes. The other APs support dual-band (XOR) between 2.4-GHz and 5-GHz radio modes.

- b) Configure the following parameters:
- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
 - **Radio Role Assignment:** To choose a radio role, check this check box and click **Auto**, **Client-Serving**, or **Monitor**. Click the required option for radio band.
 - **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.
 - **Channel Assignment:** To choose a custom channel number, check this check box and click **Custom**. Choose a custom channel number from the **Select Custom Channel** drop-down list.

- **Channel Width:** To choose channel width, check this check box and choose the channel bandwidth.

Note If the dual radio mode is enabled on a dual-band (XOR)-capable AP, its slot 2 can't be in the **Client-Serving** radio role with the 160 MHz channel width.

- **Antenna Gain:** To choose an antenna, check this check box and choose an antenna from the **Select Antenna** drop-down list. If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 through 40.

Note The selected antenna name isn't reflected in wireless maps.

- **Antenna Cable:** To choose an antenna cable, check this check box and choose the antenna cable from the **Select Antenna Cable** drop-down list. If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 through 40.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design > Network Hierarchy** window. For more information, see [Edit an AP](#).

Step 11 (Optional) In the **Configure Tri-Radio Parameters** window, configure the tri-radio parameters.

- To view the list of applicable APs for the tri-radio parameter configuration, click **View Devices**.

Note

- Catalyst Center displays the **View Devices** option only when APs that support tri-radio parameters are available.
- Catalyst Center doesn't support tri-radio parameter configuration for APs that are in **Monitor** or **Sniffer** modes.

You can configure tri-radio parameters for the following APs:

- Cisco Catalyst 9124AXE Series Access Points
- Cisco Catalyst 9130AXI Series Access Points
- Cisco Catalyst 9130AXE Series Access Points

- Configure the following parameters:

- **Dual Radio Mode:** To choose the dual radio mode, check this check box and click **Auto**, **Enable**, or **Disable**.

Note When you enable dual radio mode, global tri-radio mode is enabled on the corresponding wireless controllers.

- **Radio Role Assignment:** To choose a radio role, check this check box and click **Auto**, **Client-Serving**, or **Monitor**.

- **Admin Status:** To disable the admin status, check this check box and click **Disable**.

- **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.

- **Channel Assignment:** To choose custom channel numbers, check this check box and click **Custom**. Choose a custom channel number from the **Select Custom Channel** drop-down list.

- **Channel Width:** To choose channel width, check this check box and choose the channel width.

Note Catalyst Center enables this parameter when you choose the **Custom** option for **Channel Assignment**.

- **Antenna Gain:** To choose an antenna, check this check box and choose an antenna from the **Select Antenna** drop-down list. If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 through 40.

Note The selected antenna name isn't reflected in wireless maps.

- **Antenna Cable:** To choose an antenna cable, check this check box and choose the antenna cable from the **Select Antenna Cable** drop-down list. If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 through 40.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design > Network Hierarchy** window. For more information, see [Edit an AP](#).

Step 12 (Optional) In the **Save As Reusable Template** window, choose one of the following options:

- To save as a new template, click **Create** and enter a name for the template in the **Template Name** field. By default, the **Template Name** field is autofilled with the workflow name. You can use the same name or change as required.
- If you want to skip the template creation, click **Do Not Save**.

Note The maximum number of templates supported is 500.

Step 13 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 14 In the **Schedule Provision** window, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now:** Immediately deploy the configurations.
- **Later:** Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview:** Review the configurations before deploying them.

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

Step 15 If necessary, update the task name in the **Task Name** field.

Step 16 Click **Configure**.

Note If you choose to save this configured workflow as a new template, it's created when you click **Configure**.

Step 17 On the **Performing Initial Checks** window, ensure the following issues display successful validations so that you can continue with your current deployment:

- **Pending Operations:** Because you can run multiple simultaneous AP configuration tasks without conflicting with your current deployment, this precheck displays a successful validation.

- **Device Compliance:** This precheck is unsupported in this workflow. So, this precheck displays a successful validation so that you can continue with your current deployment.

For more information, see [Network Provisioning Prechecks](#).

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 18 (Optional) If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

For more information, see [Visibility and Control of Wireless Device Configurations](#).

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.
- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

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

When the device configurations are deployed, they are pushed to all the devices even if they aren't previewed on all the devices.

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

e. Click **Submit**.

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

Schedule Recurring Events for APs

This procedure shows how to schedule recurring events for AP and radio parameters in Catalyst Center.

Step 1 From the top-left corner, click the menu icon and choose **Workflows > Configure Access Points**.

If the **Configure Your Access Points** dialog box displays, click **Let's Do It** to go directly to the workflow.

Step 2 In the **Get Started** window, enter a unique name for the task in the **Task Name** field.

Step 3 In the **How do you want to configure APs?** window, click the **Schedule Recurring Events For AP And Radio Parameters** radio button.

Step 4

In the **Select Access Points** window, do the following:

- a) Navigate to the site where you want to apply AP-related configurations.

The right pane lists all the APs available in the selected site.

- b) Check the check boxes next to the names of the APs that you want to configure.

Step 5

In the **Select AP and Radio Parameters** window, choose the AP and radio parameters that you want to configure.

Catalyst Center applies certain settings to only one of the AP slots, as follows:

- **5 GHz Admin Status:** Applied to slot 1 of the AP.
- **2.4 GHz Admin Status:** Applied to slot 0 of the AP.
- **6 GHz Admin Status:** Applied to slot 3 of the 6 GHz-capable Cisco Catalyst 9136 Series APs and slot 2 of the 6 GHz-capable Cisco Catalyst 9164 Series APs.
- **Dual-Band (XOR) Admin Status:** Applied to slot 0 of the following dual-band (XOR)-capable APs:
 - Cisco Aironet 2800 Series Access Points
 - Cisco Aironet 3800 Series Access Points
 - Cisco Aironet 4800 Series Access Points
 - Cisco Catalyst 9120 Series Access Points

Applied to slot 2 of the dual-band (XOR)-capable Cisco Catalyst 9166 Series APs.

- **Tri-Radio Admin Status:** Applied to slot 2 of the tri-radio-capable APs with dual radio mode enabled.

To disable the configuration of a parameter, check the corresponding check box and click **Disable**.

Step 6

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

Step 7

In the **Schedule Provision** window, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now:** Immediately deploy the configurations.
- **Later:** Schedule the date and time and define the time zone of the deployment.

For more information about the recurrence settings, see the following table.

Recurrence Setting	Description
None	Runs once and doesn't repeat.
Hourly	Catalyst Center runs the AP configuration task at every specified hour interval. In the Run at Interval (Hours) field, specify the interval, in number of hours, to repeat the task. The valid range is from 1 to 48.
Daily	Runs the AP configuration task at every specified day interval. In the Run at Interval (Days) field, specify the interval, in number of days, to repeat the task. The valid range is from 1 to 14.
Weekly	Runs the AP configuration task at every specified week interval. In the Run at Interval (Weeks) field, specify the interval, in weeks, to repeat the task. The valid range is from 1 to 52.

Recurrence Setting	Description
Set Schedule End	<p>If you choose Hourly, Daily, or Weekly, check the Set Schedule End check box to complete the recurrence end settings:</p> <ul style="list-style-type: none"> To specify an end date, click End Date and specify the end date. <ul style="list-style-type: none"> Note Catalyst Center allows a maximum end date of 3 years from the start date. To end the recurring event after a specified number of occurrences, click End After and specify the number of occurrences. <ul style="list-style-type: none"> Note Catalyst Center allows a minimum value of 2.

- **Generate configuration preview:** Review the configurations before deploying them.

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

Step 8 If necessary, update the task name in the **Task Name** field.

Step 9 Click **Configure**.

Step 10 On the **Performing Initial Checks** window, ensure the following issues display successful validations so that you can continue with your current deployment:

- **Pending Operations:** Because you can run multiple simultaneous AP configuration tasks without conflicting with your current deployment, this precheck displays a successful validation.
- **Device Compliance:** This precheck is unsupported in this workflow. So, this precheck displays a successful validation so that you can continue with your current deployment.

For more information, see [Network Provisioning Prechecks](#).

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 11 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

- On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.
- On the **Preview Configuration** window, review the device configurations.

For more information, see [Visibility and Control of Wireless Device Configurations](#).
- Do one of the following:
 - When you're ready, click **Deploy** or **Submit for Approval**.
 - If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

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

When the device configurations are deployed, they are pushed to all the devices even if they aren't previewed on all the devices.

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

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

Configure APs Using Existing Templates

This procedure shows how to configure AP and radio parameters in Catalyst Center using an existing template.

Before you begin

Ensure that AP configuration templates are available. To create a new template, choose the **Create Template** option in the **Configure AP And Radio Parameters** workflow. For more information, see [Configure APs, on page 11](#).

- Step 1** From the top-left corner, click the menu icon and choose **Workflows > Configure Access Points**.
If the **Configure Your Access Points** dialog box displays, click **Let's Do It** to go directly to the workflow.
- Step 2** In the **Get Started** window, enter a unique name for the workflow in the **Task Name** field and click **Next**.
- Step 3** In the **How do you want to configure APs?** window, do the following:
 - a) Click the **Configure AP Parameters Using Existing Templates** radio button.
A list of templates is displayed.
 - b) (Optional) To view the configurations in a template, click the template name.
 - c) Check the check box next to the template name that you want.
You can choose only one template at a time.
 - d) Click **Next**.
- Step 4** In the **Select Access Points** window, do the following:
 - a) Navigate to the site where you want to apply AP-related configurations.
The right pane lists all the APs available in the selected site.
 - b) Check the check boxes next to the AP names that you want to configure.
 - c) Click **Next**.
- Step 5** Based on the configuration settings in the selected template, Catalyst Center displays the corresponding subsequent configuration windows. Each of the following configuration windows displays the preconfigured settings as per the

template. You can choose to continue with existing configurations or reconfigure as required. For more information on configuring the AP and radio parameters, see [Configure APs, on page 11](#).

Note In the **Modify AP Name** window, the list of APs displayed is based on the APs selected in the previous step (**Select Access Points** window) and not as per the template settings.

- **Modify AP Name**
- **Configure AP Parameters**
- **Configure 5 GHz Radio Parameters**
- **Configure 2.4 GHz Radio Parameters**
- **Configure 6 GHz Radio Parameters**
- **Configure Dual-Band (XOR) Radio Parameters**
- **Configure Tri-Radio Parameters**

Step 6 (Optional) In the **Save As Reusable Template** window, choose one of the following options to save the configuration changes as a template, or click **Do Not Save** if you don't want to save the changes at this point:

- To save as a new template, click **Create** and enter a name in the **Template Name** field.
- To update the existing template, click **Update**.

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

Step 8 In the **Schedule Provision** window, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

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

Step 9 If necessary, update the task name in the **Task Name** field.

Step 10 Click **Configure**.

Step 11 On the **Performing Initial Checks** window, ensure the following issues display successful validations so that you can continue with your current deployment:

- **Pending Operations**: Because you can run multiple simultaneous AP configuration tasks without conflicting with your current deployment, this precheck displays a successful validation.
- **Device Compliance**: This precheck is unsupported in this workflow. So, this precheck displays a successful validation so that you can continue with your current deployment.

For more information, see [Network Provisioning Prechecks](#).

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

- Step 12** If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:
- On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.
 - On the **Preview Configuration** window, review the device configurations.
For more information, see [Visibility and Control of Wireless Device Configurations](#).
 - Do one of the following:
 - When you're ready, click **Deploy** or **Submit for Approval**.
 - If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

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

When the device configurations are deployed, they are pushed to all the devices even if they aren't previewed on all the devices.

- 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.
- Click **Submit**.

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

Learn Device Configurations from Devices with Pre-Existing Infrastructure

The following procedure shows how to learn configuration from devices with pre-existing infrastructure using Catalyst Center.

- Step 1** From the top-left corner, click the menu icon and choose **Workflows > Learn Device Configuration > Let's Do it** to launch the workflow.

Note At the top of the workflow window, place your cursor over the blue progress bar to see the current step you are on and also to switch back to any of the previous steps.

- Step 2** In the **Select a WLC to Learn Configuration** window, click on the wireless controller whose configurations have not been learned by Catalyst Center and click **Next**.

- Step 3** In the **Site Assignment** window, select sites that aren't associated with the existing wireless network profiles for wireless controllers and APs.

- Note** While you can learn device configuration without site assignment, we recommend that you assign sites, which is required to manage the same wireless controller from Catalyst Center.
- a) To assign a site to a wireless controller, click **Assign Site** next to the **Device Name**.
 - In the **Assign Site** window, navigate to the building that you want to associate and click **Save**.
 - b) To assign sites to an AP, check the check box next to the AP name in the **Unified APs** table and click **Assign Site**.
 - In the **Assign Site** window, navigate to the floor and click **Save**.
 - c) Click **Next**.

Step 4

In the **Learned Network Settings** window, review the following learned network settings.

These settings are saved to the physical location of the device. The network servers that are displayed in this window are saved at the site level.

- Enter the **Shared Secret** for AAA servers.

- **System Settings**

- To save a AAA server as a Cisco ISE server, click the **Cisco ISE Server** toggle button and enter the **Username**, **Password**, and **FQDN** details.

Note If the Cisco ISE server is already present on Catalyst Center, you cannot save a AAA server as a Cisco ISE server.

After configuring a AAA server as a Cisco ISE server, the certificate from the Cisco ISE server is automatically accepted to establish the trust.

- Click the **Virtual IP Address(es)** toggle button to enter the load balancer IP address.
- **AAA Server**: Shows the network servers configured on Catalyst Center. These network servers are prepopulated.
 - You can customize **Network** or **Client/Endpoint** for the AAA server. The servers and protocols are chosen by default.
 - From the drop-down list, choose **IP Address (Primary)** and **IP Address (Secondary)**. These servers are saved at the global level.
 - **DHCP Server**: Shows all the DHCP servers available on the device.
 - **NTP Server**: Shows all the NTP servers available on the device.
- Click **Next**.

Step 5

In the **Assign Sites to Configurations Learned** window, you can view the following learned configurations if the configuration is available on the device. The configurations that aren't assigned to sites are ignored.

- Flex Override
- AAA Server
- VLAN Entry
- Mesh Configuration

- Enable Remote Teleworker

Step 6 In the **Learned Wireless Configuration** window, review the configurations learned from the wireless controller. The wireless configurations that appear in this window are saved at the global level.

- The **Supported** tab shows the list of learned configurations, such as **SSID**, **RF Profiles**, **Interfaces**, **Interface Groups**, **aWIPS and Forensic Capture Enablement**, **Pre Auth ACLs**, and **VLAN**.
 - By default, the NAC configuration enabled SSIDs are learned as guest SSID. Click the **Edit** icon next to the **SSID Type** in the **SSIDs** table to change the SSID type from Guest to Enterprise.
 - To ignore the configuration, check the check box next to the learned configuration, and click **Ignore Config** in the corresponding table.
 - To relearn an ignored SSID, RF profile, interface, or interface group, select it and click **Relearn Config** in the corresponding table.
- The **Unsupported** tab shows the configurations that are not learned, such as **SSIDs**, **RF Profiles**, **Interfaces**, **Pre Auth ACLs**, and **Interface Groups**. You can address these unsupported or unknown configurations and use CLI templates.

Step 7 In the **Assign Sites to Learned SSIDs** window, review and resolve any multiple WLAN profile conflicts.

- The SSIDs that are saved at the global level and learned with multiple WLAN profiles are listed. You can assign a WLAN profile from each SSID to global and another profile to a particular site to resolve the conflict.
- (Optional) To assign a WLAN profile to a site, click **Assign Site** in the corresponding SSID row.
 - In the **Assign Site** window, choose a site and click **Save**

Note Only the sites that do not have any wireless configurations or profiles that are associated to them can be overwritten. If there is no fresh site, exit from the current workflow, create a new site, and then restart the workflow.

Step 8 In the **Resolve Configuration Conflicts** window, review and resolve the available conflicts.

Configurations learned from the device and the configurations saved at the global level are shown.

Choose a configuration set to resolve the conflict:

- **Use DNAC Configuration:** To save configurations at the global level.
- **Use Device Configuration:** To learn configurations from the device.
Selecting device configuration overwrites the configurations saved at the global level.
- **Use Custom Configuration:** To customize the configurations by choosing the required **Wireless Interface**.

Step 9 In the **Model Configs Learned** window, review the model configuration.

The model configurations are a set of model-based, discoverable, and customizable configuration capabilities that can be deployed on network devices. Model configurations can be deployed on various hardware platforms and software types. Catalyst Center discovers and learns model configs from device-specific configurations such as CLI. The learned model configs are saved in designs that can be attached to network profiles.

Expand and review the following wireless model config design types:

- AAA Radius Attributes Configuration
- Advanced SSID Configuration
- CleanAir Configuration
- Dot11ax Configuration
- Event Driven RRM Configuration
- Global IPv6 Configuration
- Multicast Configuration
- RRM General Configuration

If you want to ignore any configuration from each model configuration design type, select the configuration in the corresponding table and click **Ignore Config**. To relearn the ignored configuration, select the ignored configuration and click **Relearn Config**.

Step 10 In the **CLI Templates Learned** window, review the CLI templates and use these templates to address the unknown or unsupported configurations.

- All the ignored WLAN configs are chosen by default. Click **Ignore Template** to restrict the template from addressing the configs. Click **Relearn Template** to address the configs.
- All the unknown or unsupported configs are chosen by default. Click **Ignore Template** to restrict the template from addressing the configs. Click **Relearn Template** to address the configs.

Step 11 In the **Network Profiles** window, review the learned network profile configuration. Based on the configurations learned, Catalyst Center creates the network profile. You can either use the learned network profile or create a new network profile. The SSIDs are learned and grouped while creating network profile.

For Cisco AireOS Wireless Controllers, the Flex group and AP groups are mapped to the network profile. Depending on the AP site assignment, the network profile is assigned to the appropriate site.

For Cisco Catalyst 9800 Series Wireless Controllers, the site tag, policy tag, and site hierarchy that is mapped to the network profile is displayed.

- Based on the AP site assignment configuration, network profile is assigned to the appropriate site. Click **Sites Assigned** to view details on the site assigned to the network profile.
- To create a new network profile, click **Create New Profile**.

The **New Profile** window appears.

- In the **Network Profile Name** field, enter a name for the network profile.
 - From the **SSIDs** table, check the check box next to the **Network Name** to select the SSID.
 - Click **Save**.
 - (Optional) Review the template details and edit if you want to make any changes.
 - To assign a site to a network profile, click **Assign Site**. In the **Assign Site** window, choose a site and click **Save**.
- Click **Sites Assigned** to view the sites assigned to this profile.

- To attach a template to a network profile, click **Assign Template**. In the **Assign Template** window, choose templates from the **Select Templates** drop-down list for each device in the existing deployment and click **Save**.

Click **View Templates** to view the templates assigned to the profile.

- To ignore a network profile, click **Ignore Profile** and click **Continue**.

If a profile is marked as ignored, all the profile attributes of that profile are removed. This cannot be undone by relearning the profile. To relearn an ignored profile, click **Relearn Profile**.

- To add a site tag to a network profile, click **Add** in the **Site Tag** table. In the **Add Site Tag** window, choose a site tag from the **Select Site Tag** drop-down list, choose a site from the hierarchy, and click **Save**.

Step 12 (Optional) In the **Network Profile - Model Configurations** window, associate model configurations learned by Catalyst Center into the network profiles.

- Click **Add**.
- In the **Add Model Configs to Network Profile** window, do the following:
 - Expand the model config design that you want to add.
 - Choose the design. For **Advanced SSID Configuration**, for each design, choose SSIDs from the drop-down list in the **Applicable SSID** column.
 - Click **Apply**.
- To delete a model config added to the network profile, choose the model config and click **Delete**.
- Click **Next**.

Step 13 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 14 Click **Save**.

The network configurations are created at the global and site level appropriately.

Step 15 From the top-left corner, click the menu icon and choose **Design > Network Settings**.

- In the **Network** tab, you can view all the network configurations learned from devices.
- In the **Wireless** tab, you can view all the wireless configurations learned from devices.

The learned configurations are pushed to devices when the devices are provisioned.

Replace Device

This procedure explains how to replace a faulty device.

For Cisco switch stacks (hardware stacking), you don't need to follow a separate procedure in Catalyst Center for member switch replacement, which is handled by the active switch. The member switch is replaced by the active switch by providing the software image and configuration. Full stack replacement is handled by Catalyst Center.



Note You can also replace a faulty device from the **Inventory** window. For more details, see [Replace a Faulty Device](#).

Before you begin

- The software image version of the faulty device must be imported in the image repository before marking the device for replacement.
- The faulty device must be in an unreachable state.
- The faulty device must be assigned to a user-defined site, if the replacement device onboards to Catalyst Center through Plug and Play (PnP).
- The replacement device must not be in a provisioning state while triggering the RMA workflow.
- For switch stacks replacement, the number of stacks for the faulty and replacement device must be the same.

-
- Step 1** From the top-left corner, click the menu icon and choose **Workflows > Replace Device**.
- Step 2** If a task overview window opens, click **Let's Do it** to go directly to the workflow.
- Step 3** In the **Get started** window, enter a unique **Task Name** for your workflow.
- Step 4** In the **Choose Device Type** window, choose the type of faulty device that you want to replace.
- Step 5** In the **Choose Site** window, choose the site in which you have the faulty device.
- Step 6** In the **Choose Faulty Device** window, choose one faulty device that you want to replace.
- Step 7** In the **Choose Faulty Device** window, if you don't find the faulty device, do the following:
- a) Click **Add Faulty Device**.
 - b) Choose the faulty device and click **Next**.
 - c) In the **Mark for Replacement** window, click **Mark**.
- Step 8** In the **Choose Replacement Device** window, choose a replacement device from the **Unclaimed** tab or the **Managed** tab.
- The **Unclaimed** tab shows the devices that are onboarded through PnP. The **Managed** tab shows the devices that are onboarded either through Inventory or the discovery process.
- Step 9** (Optional) If the replacement device is not yet onboarded, do the following:
- a) In the **Choose Replacement Device** window, click **Add Device**.
 - b) In the **Add New Device** window, enter the serial number of the device and click **Add New Device**.
- Alternatively, do the following:
- a) In the **Choose Replacement Device** window, click **Sync with Smart Account**.
 - b) In the **Sync with Smart Account** window, click **Sync**.
- Step 10** In the **Schedule Replacement** window, depending on the Visibility and Control of Configurations settings, choose an available option.
- To schedule the replacement immediately, click **Now**.

- To schedule the replacement 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** options are dimmed (unavailable). For more information, see [Visibility and Control of Device Configurations](#).

Step 11 Edit the default **Task Name**, if required.

Step 12 Do one of the following:

- If you have chosen **Now** or **Later**, click **Apply**.
- If you have chosen **Generate configuration preview**, click **Preview**.

Step 13 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.
If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.
- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see [Network Provisioning Prechecks](#).

Step 14 If you chose **Generate configuration preview**, in the **Preview Configuration** window, depending on the Visibility and Control of Configurations settings, do the following:

- Review the device configurations.
- 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.
- 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.
- 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 **Tasks** window. If it's not approved, you must resubmit the work item for ITSM approval. When it's approved, it will deploy at the scheduled time, which you can view on the **Tasks** window.

Step 15 If you didn't choose to generate a configuration preview in the preceding steps, do the following:

- Click **Review** to view the chosen device type, faulty device details, and replacement device details.
- In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

- c. Under **Replacement Device**, click **View** to view the configuration of the replacement device.
- d. Click **Replace**.
- e. Click **Monitor Replacement Status** to go to the **Mark for Replacement** view in the **Provision** window.
- f. Click **Replace Status** to view the status of the RMA workflow progress, as follows:
 - Running readiness checks for device replacement.
 - Claim the (PnP) replacement device.
 - Distribute and activate the software image to the replacement device.
 - Deploy licenses.
 - Provision VLAN configurations.
 - Provision startup configurations.
 - Reload the replacement device.
 - Check for reachability of the replacement device.
 - Deploy SNMPv3 credentials to the replacement device.
 - Synchronize the replacement device.
 - Remove the faulty device from CSSM.
 - Add the replacement device to CSSM.
 - Revoke and create the PKI certificate.
 - Update Cisco ISE.
 - Delete the faulty device.

After the workflow is completed, the **Replace Status** is updated to **Replaced**.

Step 16 If an error message appears, click the error link. Click **Retry** to retrigger the workflow with the same set of faulty and replacement devices.

Note The main inventory window displays the details of the new replacement device that has replaced the faulty device.

Step 17 (Optional) You can exit the workflow at any stage and resume it later. The Exit option is shown at the bottom-left corner in all the windows. To exit the workflow and resume it later, do the following:

- a) Click **Exit**.
- b) In the confirmation window, click **Exit**.

A workflow **In Progress** card with the task name is created.

- c) To resume the workflow from where you left, click the **In Progress** card.
 - If a device has an **In progress** card and you try to replace the same device from the **Inventory > Marked for Replacement** window, a confirmation message with the serial number and task name of **In progress** appears. Click **Yes** to resume the workflow or **Cancel** to start a new workflow.

- If you click the **In progress** card for a device that is unmarked for replacement, a **Warning message** appears. Click **Yes** and choose a different faulty device to start a new workflow. If you click **Cancel**, the workflow is canceled.

Create a Remote Support Authorization

The following procedure describes how to create a remote support authorization.



Note The Catalyst Center remote support authorization is supported only with RADKit version 1.2.1 and later.

Before you begin

You must create the SSH credentials before completing a remote support authorization. To create SSH credentials, see [Configure SSH Credentials](#).

-
- Step 1** From the top-left corner, click the menu icon and choose **Workflows > Create a Remote Support Authorization**.
- Step 2** If a task overview window is displayed, click **Let's Do It** to go directly to the workflow.
- Step 3** In the **Access Permission Agreement** window, do the following:
- Check the **I agree to provide access to network devices** check box to provide access to network devices.
 - Check the **I agree to provide access to Catalyst Center** check box to allow a Cisco specialist to access your Catalyst Center setup using SSH credentials.
- Note** You can revoke the authorization at any time before it expires. To revoke the authorization, see [View the Remote Support Authorization Dashboard](#).
- Step 4** Click **Next Step**.
- Step 5** In the **Set up the Authorization** window, complete the following fields:
- **Cisco Specialist Email Address**
 - **Existing Case Number(s)**
 - **Access Justification**
- Step 6** Click **Next Step**.
- Step 7** In the **Schedule the Access** window, click **Now** or **Later** to indicate when you want to allow the Cisco specialist to access Catalyst Center.
- Step 8** Click **Next Step**.
- Step 9** In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)
- Step 10** Click **Create**.
- The **Done! Authorization is created** window is displayed.

- Step 11** Click **View All Authorizations** to navigate to the **Remote Support Authorization** window. For information, see [View the Remote Support Authorization Dashboard](#).
-

Create an Event Notification

Catalyst Center event notification allows you to associate multiple channels inside one notification that delivers the details of selected events that occur at multiple points.

- Step 1** From the top-left corner, click the menu icon and choose **Workflows > Create a New Notification**.
- Step 2** If a task overview window opens, click **Let's Do It** to go directly to the workflow.
- Step 3** In the **Select Channels** window, choose the notification channels.
- The supported channels are **REST**, **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, **EMAIL**, and custom channels. Assurance events do not support SNMP.
- Step 4** In the **Select Site and Events** window, from the **Select a site** drop-down list, choose a specific site for which you want to be notified for the selected events.
- Note** You can choose multiple sites at a time.
- Step 5** Click either the plus icon next to an event, or click **Add All** to add all the events to the respective notification.
- Step 6** To remove an event from the notification, click either the cross icon next to the event that you want to remove, or click **Remove All** to remove all the event from the event list.
- Note**
- When you choose a notification channel, a table in the **Select Site and Events** window lists the number of events supported by the chosen notification channel.
 - When you choose more than one notification channel, a table in the **Select Site and Events** window lists the number of supported events that are common in the chosen notification channels.
- Step 7** In the **Configure Notification** window, configure the following values:
- a. If you choose an **EMAIL** notification channel, configure the following in the **Email Settings** window:
 1. Click the link to access the Email GUI window and configure a new email server.

- Note**
- Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you choose **EMAIL**, but have not yet configured the email settings, you are prompted to access the GUI window where you can perform this task. Email settings are configured in the **Email** tab.

(Optional) To access the **Email** tab, click the menu icon and choose **System > Settings > External Services**.

Expand **External Services**, choose **Destinations**, and click the **Email** tab.

- Up to 20 email addresses per endpoint can be configured to receive email notifications. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center validates the email addresses and notifies you if the syntax is incorrect.
 - If you need to configure more than 20 email addresses per endpoint, you can use a group email alias.
 - When using email destinations for event subscriptions, the emails that are sent show events with a UTC timestamp.
- Click either **Select Existing Instance** to use the existing email instance or **Create New Instance** to create a new email instance.
 - If you click **Select Existing Instance**, from the **Select Instance** drop-down list, choose an email instance.
 - Enter the email addresses in the **From** and **To** fields and a subject for the **Subject** header in the email.
- b. If you choose a **SYSLOG** notification, configure the following values in the **Syslog Settings** window:
- Click the link to access the Syslog GUI window and configure a new syslog endpoint (syslog server hostname and port number).

- Note**
- Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you choose **SYSLOG**, but have not yet configured the syslog server settings, you are prompted to access the GUI window where you can perform this task. Syslog server settings are configured in the **Syslog** tab.

(Optional) To access the **Syslog** tab, click the menu icon and choose **System > Settings > External Services**.

Expand **External Services**, choose **Destinations**, and click the **Syslog** tab.

- In the **Protocol** field, enter either TCP or UDP.
 - In the **Port** field, enter the port number of the syslog server.
 - In the **Hostname/IP** field, enter the hostname or IP address of the syslog server.
 - From the **Select Instance** drop-down list, choose the syslog instance.
- c. If you choose a **REST** notification, configure the following values in the **REST Settings** window:
- Click the link to access the REST Webhook GUI window and configure a new webhook endpoint.

Note Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you select **REST**, but have not yet configured the webhook settings, you are prompted to access the GUI window where you can perform this task. Webhook settings are configured in the **Webhook** tab.

(Optional) To access the **Webhook** tab, click the menu icon and choose **System > Settings > External Services**.

Expand **External Services**, choose **Destinations**, and click the **Webhook** tab.

- From the **Webhook Instance** drop-down list, choose a notification endpoint and URL.
- In the **URL** field, enter the URL address of the REST API endpoint that the event will be sent to.
Trust certificate: Whether a trust certificate is required for REST API endpoint notification.
Method: Either the PUT or POST method.
- **Basic:** Authentication where the client sends HTTP requests with the word *Basic* in the authorization header, followed by a space and a base64-encoded string username:password. If you choose **Basic** in the GUI, the **Headers** field is automatically populated with the **Authorization** value.
- **Token:** Authentication where users are authenticated using a security token provided by the server. If you choose **Token**, the **Headers** field is automatically populated with the **X-Auth-Token** value.
- **No Authentication:** No authentication needed.
- **Headers:** The **Header Name** and **Header Value**.

Note The **Headers** fields may be automatically populated depending on your Authentication selection.

d. If you choose **SNMP** notification channel, configure the following values in the **SNMP Settings** window:

1. Click the link to access the SNMP GUI window and configure a new SNMP endpoint.

Note Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you select **SNMP**, but have not yet configured the SNMP settings, you are prompted to access the GUI window where you can perform this task. SNMP settings are configured in the **SNMP** tab.

(Optional) To access the **SNMP** tab, click the menu icon and choose **System > Settings > External Services**.

Expand **External Services**, choose **Destinations**, and click the **SNMP** tab.

The SNMP trap notification is only available for a system hardware event. When the health state of hardware components changes, a system hardware event triggers notifications to subscribers. Hardware components monitored for changes include CPU, memory, disk, NIC, fan, power supply, and RAID controller.

2. From the **SNMP Instance** drop-down list, choose the notification endpoint.
3. **Create a new endpoint:** Enter a new endpoint name and description.
4. In the **Hostname/IP Address** field, enter the hostname or IP address for the SNMP trap receiver (server).
5. In the **Port** field, enter the port number for the SNMP trap receiver (server).

- e. If you choose **PAGERDUTY** notification channel, configure the following in the **PAGERDUTY settings** window:
 1. In the **SERVICE CONFIGURATION** area, click either **Select Existing Instance** to use the existing PagerDuty instance or **Create New Instance** to create a new PagerDuty instance.
 2. From the **Select Instance** drop-down list, choose a PagerDuty instance.
 3. In the **PagerDuty Events API URL** field, enter a PagerDuty event API URL.
 4. In the **PagerDuty Integration Key** field, enter a PagerDuty integration key.
- f. If you choose **WEBEX** notification channel, configure the following values in the **WEBEX Settings** window:
 1. From the **Select Instance** drop-down list, choose a Webex instance.
 2. In the **Webex URL** field, enter the Webex URL.
 3. In the **Webex Room ID** field, enter the Webex room ID.
 4. In the **Webex Bot Access Token** field, enter the Webex bot access token.

Step 8 Click **Save**.

In the **Name and Description** window, do the following:

- a) In the **Name** field, enter a unique name for the notification.
- b) In the **Description** box, enter a description of the notification.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Click **Finish**.

The **Done! Your new notification is complete** window appears.

Configure Remote LAN

Remote LAN (RLAN) allows you to configure RLAN ports on APs for Cisco Wireless Controller. Wireless controller authenticates the wired clients and allows them to connect to the network.

Catalyst Center supports RLAN configuration only on Cisco Catalyst 9800 Series Wireless Controller. You can configure RLAN for nonfabric sites on wireless controllers that run Cisco IOS XE Release 16.12 or later. You can configure RLAN for fabric sites on wireless controllers that run Cisco IOS XE Release 17.7 or later.



Note Catalyst Center doesn't support RLAN configuration on Cisco AireOS Wireless Controllers.

This section provides information about how to configure RLAN ports.

Before you begin

- Ensure that you have provisioned a Cisco Wireless Controller and at least one AP for the site.

To configure RLAN ports for fabric sites:

- Ensure that you have provisioned the required fabric site.
- Ensure that you have created IP pools and Security Group Tags (SGT).

Step 1 From the top-left corner, click the menu icon and choose **Workflows > Configure RLAN**.

Step 2 If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Get Started** window, enter a unique name for the task.

Step 4 In the **Select Floor** window, navigate to the floor where you want to configure RLAN ports.

The right pane shows the summary for the selected floor. Catalyst Center configures RLAN for all the APs provisioned on the selected floor.

Step 5 In the **Remote LAN Configuration** window, do the following:

a) Choose the required RLAN port from the **Port 1**, **Port 2**, and **Port 3** options.

If the AP has a single RLAN port, Catalyst Center ignores the **Port 2** and **Port 3** configurations for the AP.

b) Click the **Enable RLAN** toggle button to enable or disable RLAN.

c) In the **Connectivity Settings** area, click the **Fabric** toggle button to configure RLAN ports for a fabric or nonfabric site.

Note After you configure the connectivity settings for fabric or nonfabric, you can't modify the option later.

If you enable the **Fabric** toggle button, do the following:

- In the **IP Address Pool** field, enter the IP address.
- (Optional) From the **Scalable Group Tag** drop-down list, choose the required option.

If you disable the **Fabric** toggle button, do the following:

- From the **Select Switching** drop-down list, choose the required option.
- In the **VLAN** field, enter the VLAN number. The valid range for VLAN is from 1 through 4096.

d) In the **Security Settings** area, do the following:

- In the **Maximum End Points** field, enter the number of endpoints. The valid range is from 0 through 10000.

Note This field configures the client connections per RLAN. 0 indicates unlimited client connections.

- In the **Timeout Period (in seconds)** field, enter the timeout period, in seconds. The valid range for timeout is from 0 through 86400.
- (Optional) From the **Layer 2** drop-down list, choose the required option.
- (Optional) To enable MAC filtering, check the **MAC Filtering** check box.
- (Optional) From the **Fallback Authentication** drop-down list, choose the required option.

Note Fallback mechanism is supported on both fabric and nonfabric sites on Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.8 or later.

- (Optional) From the **Layer 3** drop-down list, choose the required option.
- (Optional) From the **Select a AAA Server Group** drop-down list, choose an AAA server group.

This drop-down list provides the list of AAA server groups configured as part of WLAN provisioning on the primary controller. If you don't choose an AAA server group, Catalyst Center configures the default method under the RLAN profile for the selected security settings.

- e) (Optional) In the **Point over Ethernet Settings** area, use the **PoE** toggle button to enable or disable the Point over Ethernet (PoE).

Note Catalyst Center enables PoE only on APs with PoE-capable ports.

Step 6 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 7 In the **Schedule Task** window, based on the Visibility of Configurations settings, choose an available option.

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

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

Step 8 Click **Apply**.

Step 9 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.
If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.
- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see [Network Provisioning Prechecks](#).

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 10 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

- a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.
- b. On the **Preview Configuration** window, review the device configurations.
For more information, see [Visibility and Control of Wireless Device Configurations](#).
- c. Do one of the following:
 - When you're ready, click **Deploy** or **Submit for Approval**.
 - If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

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

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

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

What to do next

You can view the status of the RLAN configuration in the **Activities > Tasks** window.

If you have provisioned a secondary wireless controller, reprovision the secondary wireless controller from the **Provision > Inventory** window.

