Build and Deploy Workflows

AP Refresh Workflow

The AP Refresh feature allows you to replace older AP models with newer AP models, using the Access Point Refresh workflow. You can use the following procedure to replace old APs with new ones in Cisco DNA Center.

For device compatibility information, see the *Cisco DNA Center Compatibility Matrix*.

Before you begin

- The old AP must be provisioned and in Unreachable state.
- The new AP must be connected to a Cisco Wireless Controller and available in the Cisco DNA Center Inventory, in Reachable state.
- The old and new APs must be associated with the same wireless controller.

Step 1 Click the menu icon (☰) and choose **Workflows** > **Access Point Refresh**.

A library of available workflows is displayed. These workflows guide you step by step through a particular task.

Step 2 Click **Let's Do it**.

To skip this window in the future, check **Don't show this to me again**.

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

Step 4 In the **Select Network Sites** window, navigate to the floor where you want to refresh the AP and click **Next**.

The right pane shows the selected building, floor, and the total number of APs provisioned on that floor.

You can replace the APs that are already in Provisioned state.

Step 5 In the **Select Access Points** window, check the check box next to the device name that you want to replace, and click **Next**.

Step 6 In the **Select procedure for providing New Access Points** window, select a method through which you want to provide new AP details: **Add New Access Point detail via CSV file** or **Add New Access Point detail via GUI**.

- Click the **Add New Access Point detail via CSV file** radio button to upload a comma-separated value (CSV) file that contains the new device name and serial number.
  - To do this, click the **Download Selected Devices List** template and add the device name and serial number of the new AP. The downloaded CSV template file contains the old AP details. After adding the device name and serial number of the new AP, you can either import the CSV file or drag and drop the CSV file into the drag-and-drop area.
  - To import the CSV file, click **Choose file** and browse to the location of the CSV file, and click **Open**.

    Cisco DNA Center performs a validation check. If the uploaded CSV file does not meet the requirement, an error message appears. Click **View Details** to get more details about the error message.

- To add the new AP details using the GUI, click the **Add New Access Point detail via GUI** radio button and click **Next**.

  The **Assign New Access Points** window appears, where you can assign a new AP for each old AP.

  - The **Old Devices** area shows details such as the IP address of the old AP, old AP name, site details, platform, and AP series information. Under the **New Devices** area, provide details about the new device.
  - From the **Choose Serial Number** drop-down list, choose the serial number of the new AP.

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

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

    If the serial number of the new AP is not available in the Inventory, the **Serial Number** drop-down list does not contain the serial number. To add a new serial number that is not present in the Inventory, from the **Choose Serial Number** drop-down list, enter the serial number and click **+**.

    Note Cisco DNA Center performs a validation check and displays errors, if any. You must fix those errors before proceeding.

    You must resolve the following dependencies before provisioning new APs:

    - Device EULA acceptance by providing cisco.com credentials.
    - Update the Cisco Wireless Controller software image version. This validation does not stop you from proceeding with the AP refresh.
    - AP Connected SwitchPort: This validation message does not stop you from proceeding with the AP refresh.

Step 7 Click **Next**.

The configuration that is copied from the old AP to the new AP is displayed in the **Configuration Copied from Old Access Point to New** window.

Step 8 Click **Next**.

Step 9 In the **Submit Access Point Refresh Task** window, click **Provision** to start the AP refresh task.

Step 10 In the **Track Replacement Status** window, monitor the AP replacement status.

- Click **View Details** to get more information about the AP replacement status.
  - If the AP replacement succeeds, the **Replacement Status** window shows the **Replacement Status** as **REPLACED**.
  - If the AP replacement fails, the **Replacement Status** shows as **Error**.
  - To delete the replacement entry, under the **Actions** column, click the three blue dots and click **Delete**. In the **Warning** dialog box, click **Yes**.
  - Click **Export** to download the provisioning summary to a CSV file that you can save locally.
  - Click **Download Report** to download the provisioning status report.

  Note If the new AP is not 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, you must resynchronize the Cisco Wireless Controller.

Step 11 Click **Next** to view the summary details.

Step 12 After successful replacement, an AP refresh event is generated in Cisco DNA Assurance for the old and new AP.

You can view the AP refresh event under **Event Viewer** in the **AP View 360** window.

The new APs are automatically updated on the respective floor maps in the **Network Hierarchy** window.

Configure User-Defined Network Workflow

The following sections provide information about configuring the Cisco User-Defined Network service using workflows in Cisco DNA 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 Cisco DNA Center.
- Create nonfabric enterprise SSIDs or guest wireless SSIDs with any security, and map them to the network profile.
- Provision SSIDs.

Configure the User-Defined Network Service

This procedure shows how to configure the Cisco User-Defined Network service from the **Workflows** > **Configure Cisco User Defined Network** window. Alternatively, you can configure the Cisco User-Defined Network service from the **Provision** > **Services** > **Cisco User Defined Network** window.

Step 1 Click the menu icon (≡) and choose **Workflows** > **Configure Cisco User Defined Network**.

Step 2 Click **Let's Do It**.

The **Let's start with configuring the Service** screen appears. You must generate an authentication token using the Cisco DNA Center Cloud portal so that Cisco DNA Center connects with Cisco DNA Center Cloud.

Step 3 Click **Configure Cloud Service**.

The **Cisco DNA Center Cloud** application opens in a new tab.

Step 4 Log in to **Cisco DNA Center Cloud** using your cisco.com account ID and password.

- Click the **Authentication Token** tab in the left menu.

  The **Authentication Token** window appears.

- In the **Authentication Token** window, click **Generate New Token**.

  The authentication token is generated.

- Click **Copy Token** to copy the authentication token.

Step 5 Navigate back to the **Let's start with configuring the Service** screen in Cisco DNA Center.

Step 6 Click **Next** to validate the copied authentication token.

Step 7 In the **Authentication Token** text box, paste the authentication token that you generated and copied in **Cisco DNA Center Cloud**, and click **Connect**.

If the token is validated successfully, a message saying `Connection validated, click Next to proceed` appears.

If the token validation fails, click **Retry**, re-enter the authentication token, and click **Connect**.

Step 8 Click **Next** to select the sites where you want to enable the Cisco User-Defined Network service.

- From the **Select Sites** drop-down list, choose the sites.
- Check the **Disable User Defined Network Service** check box to disable the workflow for all the enabled sites.

Step 9 Click **Next** to select the SSIDs for the sites you selected.

The provisioned nonfabric SSIDs are displayed for all the sites selected in the previous step.

- From the **SSID(s)** drop-down list, choose the SSIDs where the User-Defined Network service will be enabled.
- To limit the unicast traffic for the selected SSID, turn on **Unicast Traffic Containment**.
- Click **Apply Individually** to apply the unicast traffic containment for a specific site.
- Click **Apply to all** to apply the unicast traffic containment for all sites.

Step 10 Click **Next**.

Step 11 Select whether you want to provision the Cisco User-Defined Network service on your network now or schedule it for a later time.

- To provision the service on your network now, click the **Now** radio button and click **Next**.
- To provision the service on your network for a later time, click the **Later** radio button, define the date and time, and click **Next**.

The **Configuration Summary** screen appears.

Step 12 Review the following details and click **Edit** in any of the sections if you want to make a change.

- **Authentication Token**
- **Selected Sites & SSIDs**
- **Scheduling**

Step 13 Click **Configure**.

In the next screen, a check mark is shown next to each step as it is completed.

Step 14 Click **View Provisioning Status**.

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 Cisco DNA 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 Click the menu icon (≡) and choose **Provision** > **Services** > **App Hosting for Switches**.

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**.

The workflow is launched.

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 Click **Next**.

Step 5 In the **Select App** window, click on the application you want to select.

Step 6 Click **Next**.

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

Step 7 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 8 Click **Next**.

Step 9 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 10 In the **Summary** window, review the details before installing the application on the selected switches.

Step 11 Click **Next**.

The **Provisioning Task** window displays the task name that tracks the deployment of the application on the switches.

Step 12 Review the automatically generated task name and click **Provision**.

Step 13 In the **Track Provisioning Status** window, you can track the progress of the deployment.

Step 14 Click **View Details** to view the provisioning status of the individual devices and failures, if any.

Step 15 Click **Next**.

The application is enabled successfully.

The summary of the task result and the success/failure counts are displayed.

Step 16 Click **Manage App**, where you can manage the lifecycle operations of the application to perform Day N tasks.

Enable IoT Services Workflow

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 Cisco DNA 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 Click the menu icon (≡) and choose **Workflows**.

A library of available workflows is displayed. These workflows guide you step-by-step through a particular task.

Step 2 Click **Enable IOT Services**.

Step 3 Click **Let's Do it** to start the installation workflow.

Step 4 In the **Select Site** window, navigate to the floor where you want to enable the IoT service.

Step 5 Click **Next**.

Step 6 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 Cisco DNA Center, see Add an Application.

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

Step 7 In the **Select Access Points** window, check the check box adjacent to the **Device Name** where you want to install the IoT connector application.

Step 8 Click **Next**.

Step 9 In the **Summary** window, review the details before installing the application on the selected APs, and click **Next**.

The **Provisioning Task** window, which displays the task name created to track deployment of any application on APs, is displayed.

Step 10 Review the auto-generated task name and click **Provision**.

Step 11 In the **Track Provisioning Status** window, you can track the progress of the deployment.

Step 12 Click **View Details** to view the provisioning status.

Step 13 Click **Next**.

The **Done! Task Completed** window appears.

Step 14 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 the following details:

- **AP Name**
- **AP Status**
- **IP Address**
- **Health**

Step 4 Click **Tech Support logs** to collect Application Hosting logs.

AP Configuration in Cisco DNA Center

The Configure Access Points workflow allows you to configure and deploy AP-level and radio-level parameters in Cisco DNA Center.

You can configure the following AP-level parameters:

- AP location
- AP admin status
- AP mode
- AP LED status
- AP failover priority
- High availability

You can configure the following radio-level parameters:

- Radio admin status
- Radio power settings
- Radio channel settings

Configure AP Workflow

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

Before you begin

Make sure that the AP is assigned to a site.

Step 1 In the Cisco DNA Center GUI, click the menu icon (☰) and choose **Workflows** > **Configure Access Points**.

Step 2 Click **Let's Do it**.

To skip this window in the future, check the **Don't show this to me again** check box.

The **Get Started** window appears.

Step 3 In the **Task Name** field, enter a unique name for the workflow, and click **Next**.

Step 4 In the **Select Site from the hierarchy** window, navigate to the site where you want to apply AP-related configurations.

The right pane shows the selected floor and the number of APs available on that floor.

Step 5 Click **Next**.

The **Select Access Points** window lists all the APs available in the selected site.

Step 6 In the **Select Access Points** window, check the check boxes of the APs to edit the AP name in bulk.

Step 7 Click **Next**.

The **Modify AP Name** window shows the list of APs selected in the previous window.

Step 8 In the **Modify AP Name** window, enter a new name for the APs using one of the following methods:

- **Create a New Naming Convention**: Click this radio button, enter a name based on your convention, and click **Apply Pattern**. The **Access Points** table shows the new AP names based on the naming pattern 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 9 Click **Next**.

Step 10 In the **Configure AP Parameters** window, configure the following AP parameters:

- **Location**: Check this check box and enter the location details.
- **Admin Status**: To disable the admin status, check this check box and click **Disable**.
- **AP LED Status**: To disable the APs LED 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/Flex**, **Monitor**, **Bridge**, and **Flex+Bridge**.
- **AP Failover Priority**: Check this check box and, from the **AP Failover Priority** drop-down list, choose the failover priority for APs. Valid options are:
  - **Low**: Assigns the AP to level 1 priority, which is the lowest priority level. This is the default value.
  - **Medium**: Assigns the AP to level 2 priority.
  - **High**: Assigns the AP to level 3 priority.
  - **Critical**: Assigns the AP to level 4 priority, which is the highest priority level.
- **Controller Configuration**: Check this check box and configure the primary, secondary, and tertiary controller name and IP address for the AP.

Step 11 Click **Next**.

Step 12 In the **Configure 802.11 a/n/ac/ax Parameters** window, configure the following 802.11 a/n/ac/ax parameters:

- Check the **Admin Status** check box and click the **Disable** button to disable the admin status.
- Check the **Power Assignment** check box, click the **Custom** button, and choose a custom power value from the **Select Custom Power** drop-down list.
- Check the **Channel Assignment** check box, click the **Custom** button, and choose a custom channel number from the **Select Custom Channel** drop-down list.
- Check the **Channel Width** check box and choose one of the channel bandwidth options from the **Select Channel Width** drop-down list:
  - **20 MHz**
  - **40 MHz**
  - **80 MHz**
  - **160 MHz**

- Check the **Antenna Name** check box and choose an antenna name from the **Select Antenna Name** drop-down list. If you choose **Other** as the Antenna name, enter the **Antenna Gain** value in the **Antenna Gain (for Antenna-Other)** field. Enter a number to specify an external antenna's ability 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 is from 0 to 40.
- Check the **Azimuth** check box and enter a value for azimuth orientation, in degrees. The azimuth is the angle of the antenna measured relative to the x-axis. The azimuth range is from 0 to 360.
- Check the **Elevation** check box and enter a value for elevation orientation, in degrees. The elevation orientation range is from 0 to 90.

Step 13 Click **Next**.

Step 14 In the **Configure 802.11 b/g/n Parameters** window, configure the following 802.11 b/g/n parameters:

- Check the **Admin Status** check box and click the **Disable** button to disable the admin status.
- Check the **Power Assignment** check box and click the **Custom** button and choose custom power from the **Select Custom Power** drop-down list.
- Check the **Channel Assignment** check box, click the **Custom** button, and choose custom channel number from the **Select Custom Channel** drop-down list.
- Check the **Antenna Name** check box and choose the antenna name from the **Select Antenna Name** drop-down list.
- If you select **Other** as the Antenna name, enter the antenna gain value in the **Antenna Gain (for Antenna-Other)** field. Enter a number to specify an external antenna's ability to direct or focus radio energy over a region of space. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value is from 0 to 40.
- Check the **Azimuth** check box and enter a value for azimuth orientation in degrees. The azimuth is the angle of the antenna measured relative to the x-axis. The azimuth range is from 0 to 360.
- Check the **Elevation** check box and enter a value for elevation orientation in degrees. The elevation orientation range is from 0 to 90.

Step 15 Click **Next** to view the summary details. In the **Summary** window, review the following AP configuration details, and click **Edit** in any of the sections to make a change.

- Select Site from the hierarchy
- Select Access Points
- Modify AP Name
- Select AP Parameters
- Select 802.11 a/n/ac/ax Parameters
- Select 802.11 b/g/n/ax Parameters

Step 16 Click **Next**.

Step 17 To provision now, click the **Now** radio button and click **Next**. To provision at a later time, click the **Later** radio button, define the date and time, and click **Next**.

Step 18 In the **Track Provision Status** window, view the **AP Configuration Provision** status.

Learn Device Configurations from Brownfield Devices

Cisco DNA Center allows you to learn the configurations from brownfield devices such as Cisco Wireless Controllers and save the configurations at the global level. *Brownfield* refers to devices that belong to existing sites with pre-existing infrastructure.

The following procedure describes how to learn device configurations from brownfield devices in Cisco DNA Center.

Step 1 Click the menu icon (≡) and choose **Workflows**.

A library of available workflows is displayed. These workflows guide you step by step through a particular task.

Step 2 Click the **Learn Device Configuration** workflow.

Step 3 Click **Let's Do it**.

To skip this window in the future, check **Don't show this to me again**.

The **Select WLC to Learn Configuration** window appears.

Step 4 From the device name column, select a wireless controller device whose configurations have not been learned by Cisco DNA Center.

Step 5 Click **Next**.

Step 6 In the **Learned Network Configurations** window, review the network settings. The network servers that appear in this window are saved at the global level.

Step 7 **System Settings**: Shows all the AAA servers that are available on the device. Enter the password in the **Shared Secret** field for the AAA servers, because the passwords are encrypted and Cisco DNA Center cannot learn passwords.

Step 8 To save a AAA server as a Cisco ISE server, click the **Cisco ISE Server** toggle button and then enter the **Username**, **Password**, and **FQDN** details.

> **Note** If the Cisco ISE server is already present in Cisco DNA Center, you cannot save a AAA server as a Cisco ISE server.
>
> After configuring the AAA server as a Cisco ISE server, the certificate from the Cisco ISE server is automatically accepted to establish trust.

a) **AAA Server**: Shows the network servers configured in Cisco DNA 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.

b) **DHCP Server**: Shows all the DHCP servers available on the device.

c) **NTP Server**: Shows all the NTP servers available on the device.

Step 9 Click **Next**.

The **Learned Wireless Configuration** window appears.

Step 10 Review the wireless configuration. The wireless configurations that appear in this window are saved at the global level.

Supported: Shows all the supported **SSIDs**, **RF Profiles**, **Interfaces**, and **Interface Groups**.

- To ignore an SSID, RF profile, interface, or interface group, select it 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.

Unsupported: Shows all the unsupported **SSIDs**, **RF Profiles**, **Interfaces**, and **Interface Groups**. You can address these unsupported or unknown configurations and use CLI templates.

Note: Attributes that are associated with multiple profiles can cause conflicts. However, you can resolve the conflicts in the next step.

Step 11 Click **Next**.

The **Resolve Multiple WLAN Profile Conflict** window appears.

Step 12 Review and resolve the conflicts that appear in the **Resolve Multiple WLAN Profile Conflict** window.

The SSIDs that are saved at the global level and learned with multiple WLAN profiles are listed.

Assign a WLAN profile from SSID to global and another profile to a particular site to resolve the conflict.

Step 13 To assign a WLAN profile to a site, click **Assign Site** in the corresponding SSID row.

Step 14 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 15 Click **Next**.

The **Resolve Configuration Conflicts** window appears.

Step 16 Review and resolve the conflicts displayed in the **Resolve Configuration Conflicts** window.

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 17 Click **Next**.

Step 18 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. Cisco DNA 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:

- Advanced SSID Configuration
- CleanAir Configuration
- Dot11ax Configuration
- Flex Configuration
- Multicast 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 19 (Optional) Click the menu icon (☰) and choose **Tools** > **Model Config Editor** if you want to modify the learned model config designs.

Step 20 Click **Next**.

The **CLI Templates Learned** window appears.

Step 21 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 22 (Optional) To edit the CLI template, choose **Tools** > **Template Editor**.

Step 23 Click **Next**.

The **Network Profiles** window appears.

Step 24 Review the network profiles in the **Network Profiles** window.

Based on the configurations learned, Cisco DNA Center creates the network profiles. You can either use these network profiles or create new ones.

Note SSIDs are learned and grouped when creating network profiles.

Step 25 To create a new network profile, click **Create New Profile**.

Step 26 In the **New Profile** window, enter a name for the network profile in the **Network Profile Name** field, choose SSIDs in the **SSIDs** table, and click **Save**.

Step 27 For each network profile, do the following:

- 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 brownfield device 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 28 Click **Save**.

The **Network Profile - Model Configurations** window appears.

Step 29 Add the model configurations learned by Cisco DNA Center to the network profiles.

a) Expand each network profile and click **Add**.

b) In the **Add Model Configs to Network Profile** window, do the following:

1. Expand the model config design that you want to add.
2. Choose the design.

   For **Advanced SSID Configuration**, for each design, choose SSIDs from the drop-down list in the **Applicable SSID** column.
3. Click **Apply**.

c) To delete a model config added to the network profile, choose the model config and click **Delete**.

Step 30 Click **Next**.

The **Summary** window displays all the configurations learned from the device.

Step 31 To make any changes, click **Edit**. To make any changes to previous steps, click **Back**.

Step 32 Click **Save**.

All these network configurations are saved at the global level.

Step 33 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 the devices when the devices are provisioned.

Replace Device Workflow

The workflow guides you step by step to replace a faulty device.

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 Cisco DNA Center through Plug and Play (PnP).
- The replacement device must not be in a provisioning state while triggering the RMA workflow.

Step 1 Click the menu icon (≡) and choose **Workflows** > **Replace Device**.

Step 2 Click **Let's Do it**.

To skip this window in the future, check the **Don't show this to me again** check box.

Step 3 In the **Get started** window, enter a unique **Task Name** for your workflow and click **Next**.

Step 4 In the **Choose Device Type** window, choose the type of faulty device that you want to replace and click **Next**.

Step 5 In the **Choose Site** window, choose the site in which you have the faulty device and click **Next**.

Step 6 In the **Choose Faulty Device** window, choose one faulty device that you want to replace and click **Next**.

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**.
d) Click **Next**.

Step 8 In the **Choose Replacement Device** window, choose a replacement device from the **Unclaimed** tab or **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**.

Or

a) In the **Choose Replacement Device** window, click **Sync with Smart Account**.
b) In the **Sync with Smart Account** window, click **Sync**.

Step 10 Click **Next**.

Step 11 In the **Schedule Replacement** window, click **Now** to start device replacement immediately or click **Later** to schedule device replacement at a specific time.

If the replacement device is not yet onboarded, the **Now** option is disabled. Click **Later** to schedule the device replacement at a specific time.

Step 12 Click **Review** to the view the chosen device type, faulty device details, and replacement device details.

Step 13 Click **Next** to view the details in the **Summary** window.

Step 14 In the **Summary** window, do the following:

a) (Optional) Click **Edit** if you want to change the device type, faulty device, and replacement device chosen in the previous steps.
b) (Optional) Under **Replacement Device**, click **View** to view the configuration of the replacement device.
c) Click **Replace**.

Step 15 Click **Monitor Replacement Status** to go to the **Mark for Replacement** view in the **Provision** window.

Step 16 Click **Replace Status** for the replacement device to view the status of the RMA workflow progress, as follows:

- 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 17 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 18 (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**.

The **Exiting Workflow** confirmation window appears.

b) Click **Exit** in the confirmation window.

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

c) To resume the work flow from where you left, click the **In Progress** card.

- If a device has **In progress** card and you try to replace the same device from **Inventory** > **Marked for Replacement** window, a confirmation message with the serial number and task name of **In progress** card appears. Click **Yes** to resume the work-flow 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 will be cancelled.

Create a Remote Support Authorization

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

Note The Cisco DNA Center remote support authorization is supported with only LM Console version 0.40.5.

Step 1 Click the menu icon (≡) and choose **Workflows** > **Create a Remote Support Authorization**.

Step 2 Click **Let's Do it**.

Note To skip this screen in the future, check **Don't show this to me again**.

The **Set up the Authorization** window appears.

Step 3 In the **Cisco Specialist Email Address** field, enter the email address of the Cisco specialist.

Step 4 In the **Existing SR Number(s)** field, enter one or more SR numbers separated by a comma.

Step 5 In the **Access Justification** field, enter the access justification and click **Next**.

Step 6 In the **Schedule the Access** window, click **Now** to allow the Cisco specialist to access Cisco DNA Center immediately, or click **Later** to schedule the access for a later date and time.

Step 7 Click **Next**.

Step 8 In the **Access Permission Agreement** window, check **I agree** and click **Next**.

Note You can revoke the authorization at any time before the access.

Step 9 In the **Summary** window, review the details. To make changes, do the following:

- Click **Edit** to make changes in the **Set Up the Authorization** window.
- Click **Edit** to make changes in the **Schedule the Access** window.

Step 10 Click **Create**.

The **Done! Authorization is created** window appears.

Step 11 Click **View All Authorization** to navigate to the **Remote Support Authorization** window. For more information, see View Remote Support Authorization.

Create an Event Notification

Cisco DNA 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 Click the menu icon (≡) and choose **Workflows** > **Create a New Notification**.

Step 2 In the **Create a New Notification window**, click **Let's Do it**.

Note To skip this screen in the future, check the **Don't show this to me again** check box.

Step 3 In the **Select Channels** window, choose the notification channels.

The supported channels are **REST**, **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, **EMAIL**, and custom channels.

Step 4 Click **Next**.

Step 5 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 6 Click either the plus icon next to an event, or click **Add All** to add all the events to the respective notification.

Step 7 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 8 Click **Next**.

Step 9 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. Cisco DNA 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.

2. Click either **Select Existing Instance** to use the existing email instance or **Create New Instance** to create a new email instance.

3. If you click **Select Existing Instance**, from the **Select Instance** drop-down list, choose an email instance.

4. 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:

1. 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.

2. In the **Protocol** field, enter either TCP or UDP.

3. In the **Port** field, enter the port number of the syslog server.

4. In the **Hostname/IP** field, enter the hostname or IP address of the syslog server.

5. 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, 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 10 Click **Save**.

The **Name and Description** window appears.

Step 11 In the **Name** field, enter a unique name for the notification.

Step 12 In the **Description** box, enter a description of the notification.

Step 13 In the **Summary** window, review the configured details.

Step 14 Click **Finish**.

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