



Build and Deploy Workflows

- [AP Refresh Workflow](#), on page 1
- [Configure User-Defined Network Workflow](#), on page 3
- [Enable Application Hosting on Switches](#), on page 5
- [Enable IoT Services Workflow](#), on page 7
- [About AP Configuration from Cisco DNA Center](#), on page 8
- [Replace Device Workflow](#), on page 11

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 AP must be associated with the same wireless controller.

-
- Step 1** In the Cisco DNA Center GUI, 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 screen in the future, check **Don't show this to me again**.
The **Get Started** screen appears.
- Step 3** In the **Task Name** field, enter a unique name for the workflow and click **Next**.
- Step 4** In the **Select Network Sites** screen, 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 APs that are already in provisioned state.

Step 5 In the **Select Access Points** screen, 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** screen, 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 to the drag and drop area.
 - To import the CSV file, click **Choose file** and browse to the location of the CSV, then 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** screen 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 any errors. 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 new AP is displayed in the **Configuration Copied from Old Access Point to New** screen.

Step 8 Click **Next**.

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

Step 10 In the **Track Replacement Status** screen, you can 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.

Introduction to 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.

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 SSDP such as Apple Bonjour, mDNS protocol 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 which belongs 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** In the Cisco DNA Center GUI, 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 helps you to enable docker applications such as ThousandEyes Enterprise Agent, iPerf on 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 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Services > App Hosting for Switches**. Select the application and click **Install** at the bottom of the screen.

Step 2 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 page, you can place your cursor on the blue progress bar and switch back to the previous steps listed there.

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, choose the application.

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, choose the device 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:** Click the **Select Network** drop-down list and choose a VLAN to configure the application.
 - **App IP address:** Choose **Static** or **Dynamic** from the **Address Type** drop-down list. 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 **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** page, 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 any failures.
- 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 helps you to enable IoT technologies such as Bluetooth, Zigbee, and ESL on selected Catalyst 9100 Series Access Points.

- Step 1** In the Cisco DNA Center GUI, 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 details before installing the application on selected APs, and click **Next**.
The **Provisioning Task** window appears which displays the task name which is created to track deployment of any application on APs.
- 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 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.
-

About AP Configuration from 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 screen in the future, check the **Don't show this to me again** check box.
- The **Get Started** screen 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** screen, 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** screen lists all the APs available in the selected site.
- Step 6** In the **Select Access Points** screen, check the check boxes of the APs to bulk edit the AP Name.
- Step 7** Click **Next**.
- The **Modify AP Name** screen shows the list of APs selected in the previous screen.
- Step 8** In the **Modify AP Name** screen, enter a new name for the AP 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** screen, you can 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 AP 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 access point to the level 1 priority, which is the lowest priority level. This is the default value.
 - **Medium:** Assigns the access point to the level 2 priority.
 - **High:** Assigns the access point to the level 3 priority.
 - **Critical:** Assigns the access point to the 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 access point.

Step 11 Click **Next**.

Step 12 In the **Configure 802.11 a/n/ac/ax Parameters** screen, 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 and click the **Custom** button and choose custom power from the **Select Custom Power** drop-down list.
- Check the **Channel Assignment** check box and click the **Custom** button and choose 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 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(in dBi) (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 0–40.
- 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 0–360.
- Check the **Elevation** check box and enter a value for Elevation orientation in degrees. The elevation orientation range is 0–90.

- Click **Next**.

- Step 13** In the **Configure 802.11 b/g/n Parameters** screen, 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 and 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(in dBi) (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 14** Click **Next** to view the summary details. In the **Summary** screen, 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 15** Click **Next**.
- Step 16** Select whether you want to provision now or schedule it for a later time.
- Step 17** To provision now, click the **Now** radio button and click **Next**. To provision for a later time, click the **Later** radio button, define the date and time, and click **Next**.
- Step 18** In the **Track Provision Status** screen, you can view the **AP Configuration Provision** status.
-

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** page. 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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows > Replace Device**.
- Step 2** Click **Let's Do it**.
To skip this screen in the future, check **Don't show this to me again**.
- Step 3** In the **Choose Device Type** screen, choose the type of faulty device that you want to replace and click **Next**.
- Step 4** In the **Choose Site** screen, choose the site in which you have the faulty device and click **Next**.
- Step 5** In the **Choose Faulty Device** screen, choose one faulty device that you want to replace and click **Next**.
- Step 6** In the **Choose Faulty Device** screen, 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 7** 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 through Inventory or Discovery process.
- Step 8** (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 9** Click **Next**.
- Step 10** In the **Schedule Replacement** window, click **Now** to start the device replacement immediately or click **Later** to schedule the device replacement at a specific time.
If the replacement device is not yet onboarded, the **Now** option will be disabled. You can click **Later** to schedule the device replacement at a specific time.
- Step 11** Click **Review** to view the chosen device type, faulty device details, and replacement device details.

Step 12 Click **Next** to view the details in the **Summary** page.

Step 13 In the **Summary** page, 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 14 Click **Monitor Replacement Status** to go to the **Mark for Replacement** view in the **Provision** page.

Step 15 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.

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

Step 16 If an error message appears, click the error link.

Step 17 Click **Retry** to retrigger the workflow with the same set of faulty and replacement devices.

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