Build and Deploy Workflows

Cisco DNA Center Workflow Navigation

Cisco DNA 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.

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 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

- Ensure that the old AP is in unreachable state and assigned to a site.

- The old AP site must be provisioned as managed AP location for the wireless controller to which the new AP is associated.

- The new AP must not be assigned to any site.

- You must connect the new AP to a Cisco Wireless Controller. The new AP must either be available in the Cisco DNA Center Inventory or contact Cisco DNA Center through Plug and Play (PnP). It must be in Reachable state.

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

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 and click **Next**.

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

   a.   In the left pane, check the check box next to the floor where you want to refresh the AP.

   b.   In the right pane, check the check box next to the device name that you want to replace.

Step 5   In the **Assign New APs to Old APs** window, 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. In the **Edit details** window, do the following:

   a.   (Optional) Update the new AP name.

   b.   (Optional) From the **Choose Platform ID** drop-down list, choose the platform of the new AP.

   c.   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, Cisco DNA Center displays the serial number of that AP as **Managed** in the **Choose Serial Number** drop-down list.

      If the new AP has contacted Cisco DNA Center through PnP, Cisco DNA 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 is not available in the Inventory, the **Serial Number** drop-down list doesn't 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 +.

   d.   Click **Save**.

- To add the new AP details using comma-separated value (CSV) file, do the following:

   a.   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.

    b. To import the CSV file, click **Upload CSV**. 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**.

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

    c. Click **Upload**.

Step 6   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 7   If the **Resolve Dependencies** window displays the dependencies, resolve the dependencies for the provisioning of new APs..

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

        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 doesn't stop you from proceeding with the AP refresh.

- AP Connected SwitchPort: This validation message doesn't stop you from proceeding with the AP refresh.

Step 8   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 9   In the **Summary** window, review the summary and click **Provision**.

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, resynchronize the Cisco Wireless Controller.

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

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.

Cisco DNA Center automatically updates the new APs 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 Cisco User Defined Network

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

Step 1   Click the menu icon (☰) and choose **Workflows** > **Configure Cisco UDN**.

Alternatively, you can configure the Cisco UDN from the **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) Cick **Where did I get my token encryption key?** and click **Go to the Portal** in the dialog box.

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

    c) Log in to **Cisco DNA - Cloud** using your Cisco.com account ID and password.

       The **Cisco DNA - Cloud** home window appears which lists the subscribed offers for your region as a card.

Step 3   Generate an authentication token using the Cisco DNA Cloud portal to allow Cisco DNA Center to connect with Cisco DNA Cloud:

    a) In the **Cisco DNA - Cloud** GUI, click the menu icon (☰) and choose **On-Prem Connections** to register Cisco DNA 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   Cisco DNA Center registration fails intermittently on Cisco DNA - Cloud portal: This is an intermittent issue which happens during every alternate deregistration due to communication failure from Cisco DNA - Cloud to Cisco DNA Center in all regions.

    b) Follow these steps to register from the **ALL** tab:

       • Click **Register Product**.

         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**.

       • From the **Region** drop-down list, choose the location of the on-premise Cisco DNA Center.

       • Click **Register**.

       • The **OTP Generated** dialog box appears after successful registration of Cisco DNA Center. To copy the OTP, click **Copy**, and click **close**.

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

       • Click **Register Cisco DNA Center** to securely connect your products to the relevant cloud applications and services offered by Cisco and its partners.

         The **Register Cisco DNA Center** slide-in pane appears.

       • In the **Cisco DNA Center Name** field, enter the name of the on-premise Cisco DNA Center.

       • From the **Region** drop-down list, choose the location of the Cisco DNA Center.

       • In the **OTP Generated** dialog box, click **Copy** to copy the OTP and click **close**.

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

a)   In the Cisco DNA Center GUI, click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Cloud Authentication**.

b)   In the **Cloud Authentication**, click **Add OTP Key**.

c)   In the **OTP Code** field, paste the OTP that you generated and copied in the Cisco DNA - Cloud application, and click **Done**.

d)   The **Success** dialog box appears. Click **OK**.

Step 5   Verify whether the conection has been established between **Cisco DNA Center** and **Cisco DNA - Cloud** on the **Cisco DNA - Cloud** > **On-Prem Connections** 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 Cisco DNA Center.

b)   Click **Next**.

c)   In the **Select Sites** window, do the following:

    • From the **Select Sites** drop-down list, 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.

Click **Next**.

Step 8   In the **Summary** window, review the configuration details.

a)   To edit any configuration, click the corresponding **Edit** button.

b)   Expand the Connection Status area to view the conection status between Cisco DNA Center and Cisco UDN Cloud.

A success message saying Paired with Cisco DNA - Cloud appears after establishing a connection between Cisco DNA Center and Cisco UDN Cloud.

c)   Click **Configure**.

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

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** > **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**.

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 Cisco DNA 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 details before installing the application on the selected switches and click **Next**.

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 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** > **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 Cisco DNA 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 details before installing the application on the selected APs, and click **Next**.

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 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 do the following:

• Configure and deploy AP-level and radio-level parameters in Cisco DNA Center

• Schedule recurring events for AP

You can configure the following AP-level parameters:

• AP location

• AP admin status

• AP mode

• AP LED status

• LED brightness level

• AP height

• AP failover priority

• High availability

You can configure the following radio-level parameters:

• Radio admin status

• Radio power settings

• Radio channel settings

• CleanAir or spectrum intelligence settings

- Antenna settings

- Azimuth

- Elevation

Configure AP Workflow

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

Step 1 Click the menu icon (≡) and choose **Workflows** > **Configure Access Points**.

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 name for the workflow in the **Task Name** field and click **Next**.

Step 4 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 steps that you want to configure:

- **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**

Note Based on the check boxes that you check in this window, Cisco DNA Center displays the corresponding subsequent configuration steps.

c) Click **Next**.

Step 5 In the **Select Access Points** window, complete 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 6 (Optional) In the **Modify AP Name** window, modify the AP name.

Enter a new name for the APs using one of the following methods:

a) **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.

b) **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 7   (Optional) In the **Configure AP Parameters** window, configure the AP parameters.

Configure the following 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**, Cisco DNA Center uses the following settings:

  If **FlexConnect Local Switching** is enabled on any associated SSID, Cisco DNA 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, Cisco DNA Center sets **FlexConnect** mode on the AP:

    - 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 using the **Preview the CLI** link in the **Summary** window of this workflow 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, Cisco DNA 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 **LED Brightness Level**.

- **AP Height**: Check this check box and enter the AP height in feet. Cisco DNA Center allows a minimum height of 3 feet.

  Note   Cisco DNA Center applies the AP height to an AP when it is assigned to a floor. Ensure that the AP height doesn't exceed the floor height.

- **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.

• **High Availability**: Check this check box and configure the primary, secondary, and tertiary controller name and 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 configured as primary and secondary for the floor where the AP is assigned are configured as primary and secondary controller on the AP.

> • For the APs that are not in provisioned state, the current primary, secondary controller information is cleared from the AP.

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

Note	If AP fallback is disabled on the controller, AP doesn't join the newly configured primary, secondary, and tertiary controller.

Note	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.

Step 8   (Optional) In the **Configure 5 GHz Radio Parameters** window, configure the 5 GHz radio parameters.

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 the **Custom** button. 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 one of the channel bandwidth options from the **Select Channel Width** drop-down list:

> • **20 MHz**

> • **40 MHz**

> • **80 MHz**

> • **160 MHz**

• **CleanAir / Spectrum Intelligence**: To disable CleanAir spectrum intelligence, check this check box and click **Disable**.

• **Antenna Name**: To choose an antenna name, check this 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 (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 is from 0 through 40.

• **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.

- **Azimuth**: To specify the azimuth, check this 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 through 360.

- **Elevation**: To specify the elevation, check this check box and enter a value for elevation orientation, in degrees. The elevation orientation range is from 0 through 90. Use the **Up** and **Down** toggle buttons to specify the direction.

Step 9 (Optional) In the **Configure 2.4 GHz Radio Parameters** window, configure the 2.4 GHz radio parameters.

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 the **Custom** button. Choose a custom channel number from the **Select Custom Channel** drop-down list.

- **CleanAir / Spectrum Intelligence**: To disable CleanAir spectrum intelligence, check this check box and click **Disable**.

- **Antenna Name**: To choose an antenna name, check this 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 (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 is from 0 through 40.

- **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.

- **Azimuth**: To specify the azimuth, check this 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 through 360.

- **Elevation**: To specify the elevation, check this check box and enter a value for elevation orientation, in degrees. The elevation orientation range is from 0 through 90. Use the **Up** and **Down** toggle buttons to specify the direction.

Step 10 (Optional) In the **Configure 6 GHz Radio Parameters** window, configure the 6 GHz radio parameters.

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 the **Auto**, **Client-Serving**, or **Monitor** button.

- **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 the **Custom** button. 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 one of the channel bandwidth options from the **Select Channel Width** drop-down list:

  - **20 MHz**

  - **40 MHz**

• **80 MHz**

• **160 MHz**

- **Azimuth**: To specify the azimuth, check this 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 through 360.

- **Elevation**: To specify the elevation, check this check box and enter a value for elevation orientation, in degrees. The elevation orientation range is from 0 through 90. Use the **Up** and **Down** toggle buttons to specify the direction.

Step 11 (Optional) In the **Configure Dual-Band (XOR) Radio Parameters** window, configure the dual-band (XOR) radio parameters.

a) 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 9100 Access Points

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 the **Auto**, **Client-Serving**, or **Monitor** button. 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 custom channel numbers, check this check box and click the **Custom** button. 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 one of the channel bandwidth options from the **Select Channel Width** drop-down list:

  • **20 MHz**

  • **40 MHz**

  • **80 MHz**

  • **160 MHz**

- **CleanAir**: To disable CleanAir spectrum intelligence, check this check box and click **Disable**.

- **Antenna Name**: To choose an antenna name, check this 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 (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 is from 0 through 40.

- **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.

- **Azimuth**: To specify the azimuth, check this 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 through 360.

- **Elevation**: To specify the elevation, check this check box and enter a value for elevation orientation, in degrees. The elevation orientation range is from 0 through 90. Use the **Up** and **Down** toggle buttons to specify the direction.

Step 12   In the **Schedule Task** window, click **Now** or **Later** to indicate when you want to provision the AP.

Step 13   Click **Next** to view the summary details. In the **Summary** window, review the AP configuration details, and click **Edit** in any of the sections to make a change.

Step 14   Click **Configure**.

Step 15   In the **Track Provision Status** window, view the **AP Configuration Provision** status.

Schedule Recurring Events for AP Workflow

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

Step 1   Click the menu icon (≡) and choose **Workflows** > **Configure Access Points**.

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 in the **Task Name** field.

Step 4   In the **How do you want to configure APs?** window, click the **Schedule Recurring Events For AP And Radio Parameters** radio button.

Step 5   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 choose.

Step 6   In the **Select AP and Radio Parameters** window, choose the AP and radio parameters that you want to configure for the recurring events for the selected APs:

- **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**.

- **5 GHz Admin Status**: To disable the 5 GHz admin status, check this check box and click **Disable**.

   Cisco DNA Center applies this setting to slot 1 of the AP.

- **2.4 GHz Admin Status**: To disable the 2.4 GHz admin status, check this check box and click **Disable**.

   Cisco DNA Center applies this setting to slot 0 of the AP.

- **6 GHz Admin Status**: To disable the 6 GHz admin status, check this check box and click **Disable**.

   Cisco DNA Center applies this setting to slot 3 of the 6 GHz-capable AP.

- **Dual-Band (XOR) Admin Status**: To disable the dual-band (XOR) admin status, check this check box and click **Disable**.

Cisco DNA Center applies this setting to slot 0 of the dual-band (XOR)-supported AP.

Step 7   In the **Schedule Provision** window, configure the following:

a.   Specify the start date and time.

b.   Choose a time zone.

c.   For **Recurrence**, click one of the following toggle buttons:

• **None**: Cisco DNA Center runs the AP configuration task only once and doesn't repeat it.

• **Hourly**: Cisco DNA 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 through 48.

• **Daily**: Cisco DNA Center 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 through 14.

• **Weekly**: Cisco DNA Center 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 through 52.

d.   (Optional) If you choose **Hourly**, **Daily**, or **Weekly** recurrence interval, check the **Set Schedule End** check box to complete the recurrence end settings:

• To specify an end date, click the **End Date** radio button and specify the end date.

Note   Cisco DNA Center allows a maximum end date of three years from the start date.

• To end the recurring event after a specified number of occurrences, click the **End After** radio button and specify the number of occurrences.

Note   Cisco DNA Center allows a minimum value of 2 and maximum end date of three years from the start date.

Step 8   In the **Summary** window, review the summary and click **Configure**.

Learn Device Configurations from Devices with Pre-Existing Infrastructure

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

Step 1   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 know 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 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.

• **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 **Native 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. 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:

- 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, Cisco DNA 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 Cisco DNA 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   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 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 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 **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 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 11   Click **Review** to the view the chosen device type, faulty device details, and replacement device details.

Step 12   In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

    a) (Optional) Under **Replacement Device**, click **View** to view the configuration of the replacement device.

    b) Click **Replace**.

Step 13   Click **Monitor Replacement Status** to go to the **Mark for Replacement** view in the **Provision** window.

Step 14   Click **Replace Status** for the replacement device to view the status of the RMA workflow.
After the workflow is completed, the **Replace Status** is updated to **Replaced**.

Step 15   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 16   (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 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   If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Step 3   In the **Set up the Authorization** window, enter the following:

a) **Cisco Specialist Email Address**

b) **Existing SR Number(s)**

c) **Access Justification**

Step 4   In the **Schedule the Access** window, click **Now** or **Later** to indicate when you want to allow the Cisco specialist to access Cisco DNA Center.

Step 5   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 6   In the **Summary** window, review the details. Click **Edit** to make changes in the **Set Up the Authorization** and **Schedule the Access** window.

Step 7   Click **Create**.

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

Step 8   Click **View All Authorization** to navigate to the **Remote Support Authorization** window. For 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   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.

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. 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 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 configured details and click **Finish**.

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

Workflow to Create an IP- and URL-Based Access Control Policy

You can create IP-based and URL-based post authentication access control list (ACL) for your network.

Before you begin

Create an IP-Based Access Control Contract

Step 1 In the Cisco DNA Center GUI, click the menu icon (≡) and choose **Workflows** > **Create IP & URL-Based Access Control Policy** .

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

Step 3 In the **Policy Name and Details** window, complete the following fields:

• **Policy Name**

• **Description**

• **Select ACL Type**: Choose **IP**, **URL** or both as required.

Step 4 In the **Select Site and SSID** window, do the following:

• Choose the site where you want to apply the policy.

- Choose the nonfabric SSID that is already provisioned to the device.

Step 5   In the **IP Access Control List** window, click **Add New Row** and choose the following:

- **Source**

- **Destination**

- **Contracts**

- **Direction**

Note   This window will be visible only if you choose **IP** as the ACL type in the **Policy Name and Details** window.

Step 6   Click **Add**.

Step 7   In the **URL Access Control List** window, do the following:

- Enter the URL.

- Click the **Actions** drop-down list and choose **Permit** or **Deny**.

Note   This window will be visible only if you choose **URL** as the ACL type in the **Policy Name and Details** window.

Step 8   In the **Schedule Task** window, do one of the following:

- To deploy the policy immediately, click the **Now** radio button and click **View Summary**.

- To deploy the policy at a later time, click the **Later** radio button, enter the **Task Name**, define the **Start Date** and **Time**, and click **View Summary**.

- Click **Generate Preview** if you want to create preview which can be later used to deploy on selected devices.

Step 9   In the **Summary** window, review your site configuration.

- Click **Edit** to make any changes.

- If you are satisfied, click **Deploy**.