Design Network Hierarchy and Settings

Design a New Network Infrastructure

The **Design** area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the **Design** workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the **Discovery** feature. For more information, see About Discovery.

You can perform these tasks in the **Design** area:

Step 1 Create your network hierarchy. For more information, see Create a Site in a Network Hierarchy, on page 2.

Step 2 Define global network settings. For more information, see Manage Global Network Settings, on page 78.

Step 3 Define network profiles.

About Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations. Your network hierarchy can contain sites, which in turn contain buildings and areas. You can create site and building IDs to easily identify where to apply design settings or configurations later. By default, there is one site called **Global**.

The network hierarchy has a predetermined hierarchy:

- **Areas** or **Sites** do not have a physical address, such as the United States. You can think of areas as the largest element. Areas can contain buildings and subareas. For example, an area called United States can contain a subarea called California, and the subarea California can contain a subarea called San Jose.

- **Buildings** have a physical address and contain floors and floor plans. When you create a building, you must specify a physical address and latitude and longitude coordinates. Buildings cannot contain areas. By creating buildings, you can apply settings to a specific area.
- **Floors** are within buildings and consist of cubicles, walled offices, wiring closets, and so on. You can add floors only to buildings.

You can change the site hierarchy for unprovisioned devices while preserving AP locations on sitemaps. Note, however, that you cannot move an existing floor to a different building.

The following is a list of tasks that you can perform:

- Create a new network hierarchy. For more information, see Create a Site in a Network Hierarchy, on page 2.
- Upload an existing network hierarchy from Cisco Prime Infrastructure. For more information, see Upload an Existing Site Hierarchy, on page 4.

Guidelines for Image Files to Use in Maps

Follow these guidelines to use map image files:

- Use a graphical application that can save the map image files to any of these formats—.jpg, .gif, .png, .pdf, .dxf, and .dwg.
- Map image files can be of any size. Cisco DNA Center imports the full definition of the original images to its database, but during display, it automatically resizes them to fit the workspace.
- Obtain the horizontal and vertical dimensions of the site in feet or meters before importing. This helps you to specify these dimensions during map import.
- Avoid using floor map images with rotation metadata, because the images might not render correctly when synced to CMX or Cisco DNA Spaces. Although the floor map images might be in formats that are supported by Cisco DNA Center, the ways in which certain tools add the metadata can be rendered differently. For example, an image file with rotation metadata that is opened in three different applications might render horizontally in two applications and vertically in the other.

Manage Sites in Your Network Hierarchy

Create a Site in a Network Hierarchy

Cisco DNA Center allows you to easily define physical sites and then specify common resources for those sites. The **Design** area uses a hierarchical format for intuitive use, while eliminating the need to redefine the same resource in multiple places when provisioning devices. By default, there is one site called **Global**. You can add more sites, buildings, and areas to your network hierarchy. You must create at least one site before you can use the provision features.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Result: A world map appears in the right pane.

Step 2 From the map toolbar, click **+ Add Site** and choose **Add Area**.

Note You can also hover your cursor over the ellipsis ••• next to the parent site in the left pane, and then choose **Add Area**.

Step 3 Enter the site name in the **Area Name** field.

Note The **Area Name** field has the following restrictions:

- The area name cannot exceed 40 characters.
- Special characters & > < ? ' " / [ ] aren't allowed.

Step 4 From the **Parent** drop-down list, choose a parent node.

Note By default, **Global** is the parent node.

Step 5 Click **Add**.

Result: The site is created under the parent node in the left pane.

Export a Site Hierarchy from Cisco Prime Infrastructure and Import into Cisco DNA Center

A network hierarchy is a representation of your network's geographical locations. You create site and building IDs so that later you can easily identify where to apply design settings or configurations. If you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Cisco DNA Center, saving time and effort spent in creating a new network hierarchy.

This is a simple process that requires you to export two files from Cisco Prime Infrastructure as a CSV file that contains location groups or site information, and a map archive file that contains various floor maps in your network hierarchy.

This procedure describes how to export an existing site hierarchy from Cisco Prime Infrastructure to Cisco DNA Center. You can export a site hierarchy from Cisco Prime Infrastructure Release 3.2 and later.

Before you begin

- Make sure that you have Cisco Wireless Controllers and APs in your inventory. If not, discover them using the **Discovery** feature.
- Add and position APs on a floor map.
- If you manually created any sites in Cisco DNA Center that are present in Cisco Prime Infrastructure, you must remove those sites manually before importing them into Cisco DNA Center.

Step 1 Export the location groups from Cisco Prime Infrastructure as a CSV file to your workstation. In Cisco Prime Infrastructure, choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 In the **Device Groups** window, click **Export Groups**.

Step 3 In the **Export Groups** dialog box, click the **APIC-EM** radio button to download the CSV file, and click **OK**.

Note Wait for the CSV file to download. The CSV file contains information about the geographic locations of various sites, buildings, and floors and their hierarchy in the network.

Step 4 Export maps from Cisco Prime Infrastructure by choosing **Maps** > **Wireless Maps** > **Site Maps (New)**.

Note This downloads map information, such as floor dimension, and calibration information, such as the Radio Frequency (RF) attenuation model that has been applied to each floor in Cisco Prime Infrastructure.

Step 5 From the **Export** drop-down list, choose **Map Archive**.

Result: The **Export Map Archive** window appears, and the **Select Sites** window appears by default.

Step 6 Check the check box of a specific site, campus, building, or floor that you want to export. Alternatively, check the **Select All** check box to export all the maps.

Step 7 Check if the **Map Information** and **Calibration Information** are selected. Selecting one option is mandatory. If not, click the **On** button for **Map Information** or **Calibration Information**.

- Selecting **Map Information** exports floor dimensions such as length, width, and height. It also exports details about the APs that have been placed on the floor maps, and the obstacles and areas overlayed on the floor maps within Cisco Prime Infrastructure.
- Selecting **Calibration Information** exports the RF attenuation model that has been applied to each floor in Cisco Prime Infrastructure. It is a good practice to export the existing calibration data from Cisco Prime Infrastructure. Otherwise, you must enter the calibration details manually in Cisco DNA Center.

Step 8 Click **Generate Map Archive**.

Result: A tar file that contains the various floor maps in your network hierarchy is created and saved on your workstation.

Step 9 To import the site hierarchy to Cisco DNA Center, do the following:

a) In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.
b) From the map toolbar, click **Import** and choose **Import Sites**.

Step 10 In the **Import Sites** window, drag and drop the Cisco Prime Infrastructure location groups CSV file.

Step 11 Click **Import**.

Step 12 Import the map archive file that contains floor maps and related map information by clicking **Import** from the map toolbar and choosing **Import Maps**.

Step 13 In the **Import Maps** window, drag and drop the map archive file.

Step 14 Click **Import**.

Upload an Existing Site Hierarchy

You can upload a CSV file or a map archive file that contains an existing network hierarchy. For example, you can upload a CSV file with location information that you exported from Cisco Prime Infrastructure. For information about exporting maps from Cisco Prime Infrastructure, see Export Maps Archive, on page 5.

Note Before importing a map archive file into Cisco DNA Center, make sure that the devices such as Cisco Wireless Controllers and the associated APs are discovered and listed on the Cisco DNA Center inventory page.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 From the tool bar, click **Import** and choose **Import Sites**.

Step 3 Drag and drop your CSV file, or navigate to where your CSV file is located, then click **Import**.

> **Note** If you do not have an existing CSV file, click **Download Template** to download a CSV file that you can edit and upload.

Step 4 To import the Cisco Prime Infrastructure maps tar.gz archive file, choose **Import** > **Map Import**.

Step 5 Drag and drop the map archive file into the boxed area in the **Import Site Hierarchy Archive** dialog box.

Step 6 Click **Save** to upload the file.

Result: The **Import Preview** window appears, which shows the imported file.

Export Maps Archive

You can export maps archive files from Cisco Prime Infrastructure and import them into Cisco DNA Center.

Step 1 From the Cisco Prime Infrastructure user interface, choose **Maps** > **Wireless Maps** > **Site Maps (New)**.

Step 2 From the **Export** drop-down list, choose **Map Archive**.

Step 3 On the **Select Sites** window, configure the following. You can either select map information or calibration information to be included in the maps archive.

- **Map Information**: Click the **On or Off** button to include map information in the archive.
- **Calibration Information**: To export calibration information, click the **On or Off** button. Click the **Calibration Information for selected maps** or the **All Calibration Information** radio button. If you select **Calibration Information for selected maps**, the calibration information for the selected site maps is exported. If you select **All Calibration Information**, the calibration information for the selected map, along with additional calibration information that is available in the system, is also exported.
- In the **Sites** left pane, check one or more check boxes of the site, campus, building floor, or outdoor area that you want to export. Check the **Select All** check box to export all the maps.

Step 4 Click **Generate Map Archive**. A message `Exporting data is in progress` is displayed.

Result: A tar file is created and is saved to your local machine.

Step 5 Click **Done**.

Export a Global Maps Archive

You can export a complete network global hierarchy map, or choose the hierarchy of a site, a building, or a floor that the hierarchy map downloads to an archive file. The map archive file contains data such as date and time, number of floors, and APs.

Note You can export up to 500 floors.

Before you begin

To perform the following task, you must be a **Super Admin** or **Network Admin**.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 To export the complete network map, click **Export** from the upper toolbar and choose **Export Maps**.

Alternatively, click the gear icon next to the desired site, building, or floor in the left pane and choose **Export Maps**.

- If you choose a site and click **Export Maps**, the site map containing all the subsites, buildings, and floors is exported.
- If you choose a building and click **Export Maps**, the building map containing all the floors is exported.
- If you choose a floor and click **Export Maps**, only the chosen floor map is exported.

Step 3 In the **Export Maps** window, do the following:

a) In the **File to be saved to** field, enter a filename.

b) For **Export Format**, choose a format.

c) Click **Export**.

Result: A tar file containing the selected maps archive file is generated and saved to your computer.

Export Site Hierarchy

You can export the complete hierarchy of a site that downloads to a CSV format file. The site hierarchy file contains details such as site names, parent hierarchy, number of floors, location, and site address.

The following procedure explains how to export a site hierarchy:

Before you begin

To perform the following task, your account must be a **SUPER-ADMIN-ROLE** or **NETWORK-ADMIN-ROLE**.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 To export the complete site hierarchy, click **Export** from the map toolbar and choose **Export Sites**.

Step 3 In the **Export Sites** dialog box, click **OK**.

Result: The complete site hierarchy file containing site names, parent hierarchy, number of floors, location, and address is exported in CSV format and saved in your computer.

Search the Network Hierarchy

You can search the network hierarchy to quickly find a site, building, or area. This is particularly helpful after you have added many sites, areas, or buildings.

To search the tree hierarchy, in the **Find Hierarchy** search field in the left pane and enter either the partial or full name of the site, building, or floor name that you are searching.

Result: The tree hierarchy is filtered based on the text you enter in the search field.

Edit a Site

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis ••• next to the site and choose **Edit Area**.

Step 3 In the **Edit Area** pop-up, make the necessary edits.

Step 4 Click **Update** to save your changes.

Delete a Site

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis ••• next to the site and choose **Delete Area**.

Step 3 In the dialog box, click **OK** to confirm the deletion.

Manage Buildings in Your Network Hierarchy

Add a Building

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the **Network Hierarchy** window, click **+Add Site** > **Add Building**.

Note Alternatively, you can hover your cursor over the ellipsis ••• next to the parent site in the left pane, and choose **Add Building**.

Step 3 Add the building details in the **Add Building** pop-up:

a) In the **Building Name** field, enter a name for the building.

Note The **Building Name** field has the following restrictions:

- The building name cannot exceed 40 characters.
- Special characters & > < ? ' " / [ ] aren't allowed.

b) From the **Parent** drop-down list, choose a parent node.

Note By default, **Global** is the parent node.

c) In the **Address** field, enter an address.

Note Alternatively, you can click on the map to input the address. Adding an address causes the **Longitude** and **Latitude** coordinates fields to be automatically populated. You can manually change the longitude and latitude coordinates to change the address.

Step 4 Click **Add**.

Result: The building is created and appears under the parent site in the left pane.

Edit a Building

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis ••• next to the building and choose **Edit Building**.

Step 3 In the **Edit Building** pop-up, make the necessary edits.

Step 4 Click **Update** to save your changes.

Delete a Building

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis ••• next to the building and choose **Delete Building**.

Step 3 In the dialog box, click **OK** to confirm the deletion.

Note Deleting a building deletes all its container maps. APs from the deleted maps are moved to Unassigned state.

Manage Floors in Your Network Hierarchy

Add a Floor to a Building

After you add a building, you will need to create floors for it.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis ••• next to the building of the floor and choose **Add Floor**.

Step 3 In the **Floor Name** field, enter a name for the floor.

Note The **Floor Name** field has the following restrictions:

- The floor name cannot exceed 40 characters.
- Special characters & > < ? ' " / [ ] aren't allowed.

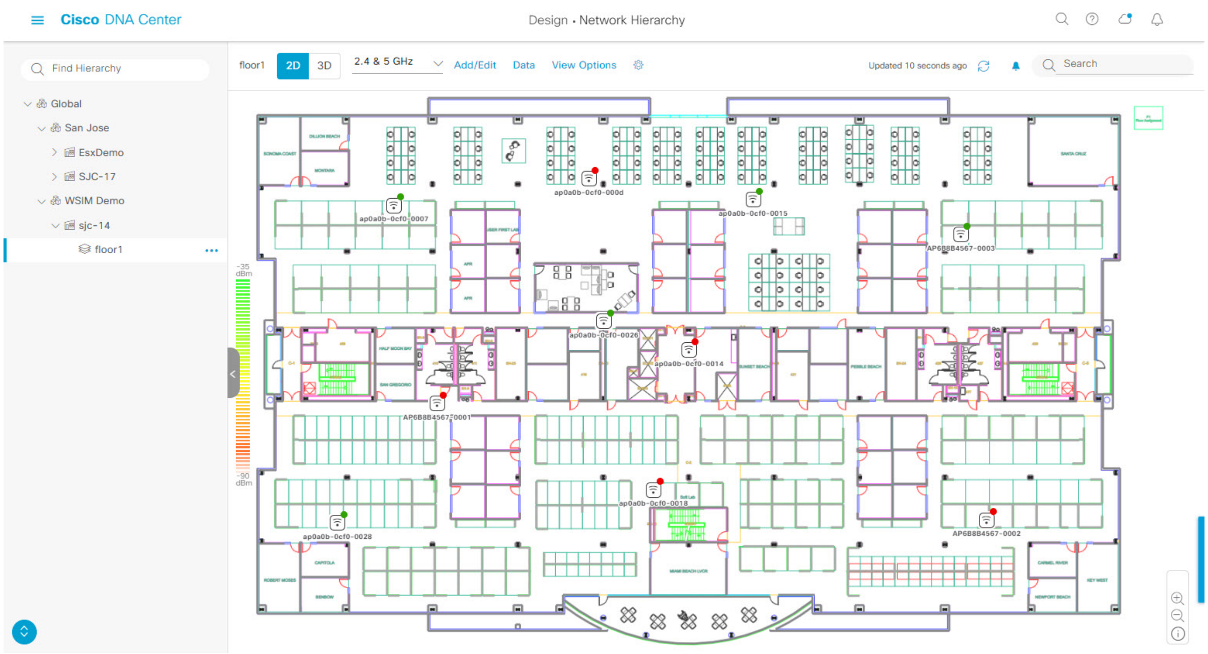
Step 4 For the **Type (RF Model)** drop-down list, choose the RF model to apply for the floor.

Note The RF model determines how the RF is calculated based on the characteristics of the floor.

Step 5 In the **Floor Image** area, drag and drop the floor plan file to upload the floor plan.

Note Cisco DNA Center supports the file types DXF, DWG, JPG, GIF, PNG, and PDF for floor plans.

Figure 1: Example of a Floor Plan



Note After you import a floor plan, make sure that you enable the overlay visibility (From the floor, click **View Options** and enable the overlay toggles in **Overlay Objects**). By default, overlays are not displayed after you import a map.

Step 6 If you upload a CAD file (DXF or DWG file type), use the **Floormap** pop-up to choose the CAD layers that you want to appear as floor elements in the map:

a) For the **2D** column, check the check boxes of the CAD layer that you want to appear in the 2D view.

b) For the **3D Wall/Shelving Type** column, use the drop-down list for a CAD layer to specify the type for the wall or shelving.

Note For a layer to appear in the 3D view, it is required to have a **3D Wall/Shelving Type** value. The wall/shelving type affects attenuation and how the heatmap is calculated.

c) Click **Use Selected Layers**.

Step 7 Enter the floor map dimensions in the **Width**, **Length**, and **Height** fields.

Step 8 Click **Add**.

Edit a Floor

After you add a floor, you can edit the floor map so that it contains obstacles, areas, and APs on the floor.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis ••• next to the floor and choose **Edit Floor**.

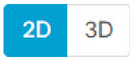
Step 3 In the **Edit Floor** pop-up, make the necessary changes.

Step 4 Click **Update** to save the changes.

View a 2D Wireless Floor Map

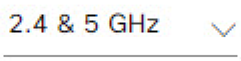
Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, ensure that the **2D** toggle 

is enabled.

Step 4 Use the map toolbar for the following actions and settings:

Item	Description
	2D and 3D Toggle: Use this toggle to view the wireless map in 2D or 3D.
	**Wi-Fi Band Filter**: Use this filter to view the heatmap for the 2.4 GHz and 5 GHz Wi-Fi bands.

Item	Description
Add/Edit	Click to enter add and edit mode which allows to do the following: • Add, position, and delete floor elements such as: • Access points. For details, see Add, Position, and Delete APs, on page 15. • Sensors. For details, see Add, Position, and Delete Sensors, on page 20. • Add, edit, and delete overlay objects such as: • Coverage areas. For details, see Add Coverage Areas, on page 21. • Location regions. For details, see Location Region Creation, on page 23. • Walls. For details, see Add Walls on a Floor, on page 22. • Shelvings. For details, see Add Shelvings on a Floor, on page 23. • Markers. For details, see Place Markers, on page 25. • GPS markers. For details, see Add GPS Markers, on page 25.
Data	Apply filters to the access point, sensor, and client data that appears in the wireless map. For details, see Filter Device Data on a Floor, on page 26.
View Options	Click to open the **View Options** slide-in pane which contains the view options for the map, devices, and floor map elements.
⚙	**Gear Icon**: Hover your cursor over the icon for the following options: • **Recompute**: Recomputes the heatmap. • **Export**: Export the floor map to a PDF or CSV file format. • **Edit Floor**: Edit the floor details such as its name • **Set Scale**: Change the scale by doing the following: **a.** Click on a point and then on another point to specify a known measurement on the map. **b.** In the **New line length (ft)** field, enter the length of the measurement. **c.** Click **OK**. The floor map dimensions are recalculated based on the length of the measurement. • **Measure Distance**: Measure a distance on the floor map. Click on a point and then another point to specify the distance.
🔄	**Refresh Icon**: Click to refresh the device and map data. To the left of the icon is the timestamp for the last refresh
🔍 Search	Use this search field to perform a search for specific floor map elements such as [illegible]ors, clients, and so on.

Step 5 Use the map for the following functionality:

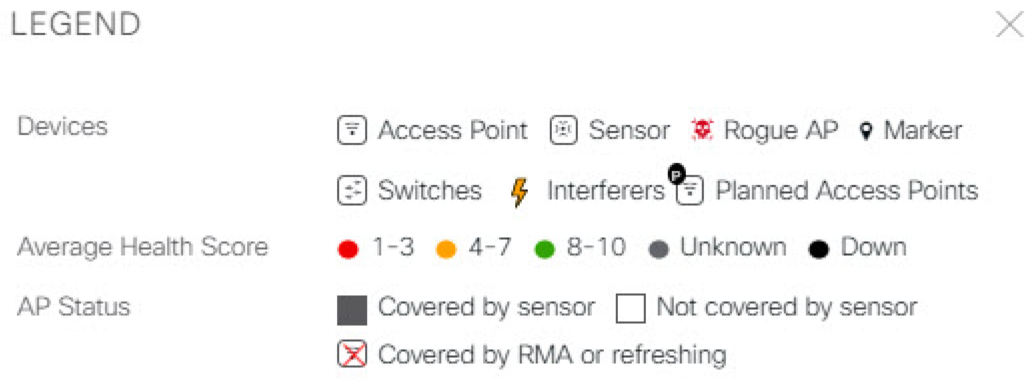
- View the heatmap of the 2D wireless floor map. You can customize the view option settings from the **View Options** slide-in pane.
- View an AP's details by hovering your cursor over an AP icon.

  You can view the basic info, RX neighbors, clients, interferers, and health score for an AP.

  Click **Device 360** to get a 360° view of the AP.

  Note For **Device 360**, the package *Assurance - Base* is required.

- View a sensor's status and test results by hovering your cursor over a sensor icon.
- View a switch's details by hovering your cursor over a switch icon.
- Use the map navigation controls at bottom-right of the map for the following controls:

Map Navigation Controls	**Description**
⛶	**Default Map View**: Click to reset the map view to the default.
⊕ ⊖	**Zoom In / Zoom Out**: Zoom in and out of the map. Alternatively, you can use your mouse wheel to zoom in and out.
ⓘ	**Map Legend**: Click this icon to view the map legend which describes the map icons such as the device type, average health score, and AP status.  LEGEND Devices: Access Point, Sensor, Rogue AP, Marker, Switches, Interferers, Planned Access Points Average Health Score: ● 1-3 ● 4-7 ● 8-10 ● Unknown ● Down AP Status: ■ Covered by sensor □ Not covered by sensor ☒ Covered by RMA or refreshing

Step 6 Click **View Options** from the map toolbar to open the **View Options** slide-in pane. This allows you to configure the view option settings. Expand the categories to view the settings:

- **Map**: Contains various floor map and heatmap settings:

Item	**Description**
Show Grid	Click the toggle to enable or disable a grid on the floor map. The grid provides the dimensions of the floor map.
Map Opacity %	Use this slider to customize the opacity or transparency of the floor map.

Item	Description
Heatmap Type	The heatmap provides a graphical representation of Radio Frequency (RF) wireless data where the values taken by variable are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, antenna orientation, and AP transmit power. Use the drop-down list to choose the heatmap type: • **AP RSSI**: Coverage heatmap, which identifies the strength of wireless signal. • **Client Density**: Density of associated clients. • **IDS**: Heatmap that shows the monitor mode access point coverage provided to the wireless clients on a floor map. • **Planned Heatmap**: Hypothetical heatmap that shows the possible coverage of planned access points on a floor map.
RSSI Cut off (dBm)	Use this slider to set the threshold for the RSSI value to appear on the heatmap. RSSI values that do not meet the threshold are faded.
Heatmap Opacity %	Use this slider to customize the opacity or transparency of the heatmap.
Heatmap Color Scheme	Customize the color scheme for the heatmap. Options are **Legacy** and **Natural**.

- **Access Points**: Click the toggle to enable or disable the AP icons on the floor map.
  - **Display Label**: Use the drop-down list to choose the type of label to appear for APs on the floor map such as the AP's name, MAC address, or IP address, and so on.

- **Planned Access Points**: Click the toggle to enable or disable the appearance of planned access point (PAP) icons on the floor map.
  - **Display Label**: Use the drop-down list to choose the type of label to appear for the PAP icons such as the PAP's name.

- **Switches**: Click the toggle to enable or disable the appearance of switch icons on the floor map.
  - **Display Label**: Use the drop-down list to choose the type of label to appear for switch icons on the floor map such as the switch's name, MAC address, or AP count.

- **Sensors**: Click the toggle to enable or disable the appearance of sensor icons on the floor map.
  - **Display Label**: Use the drop-down list to choose the type of label to appear for sensor icons on the floor map such as the sensor's name, MAC address, or IP address.

- **Overlay Objects**: Contains the settings for the overlay objects:
  - **Coverage Areas**
  - **Location Regions**
  - **Walls 2D & 3D**
  - **Walls 3D only**

    - **Shelvings**
    - **Markers**
    - **GPS Markers**

  Click the toggle for an overlay object to enable or disable the object on the floor map.

- **Clients**: Click the toggle to enable or disable the appearance of client icons on the floor map.
    - **Display Label**: Use this drop-down list to choose the type of label to appear for client icons on the floor map such as client name, IP address, MAC address, and so on.
    - **Show Client Clusters**: Click this toggle to enable or disable clients in close promixity to be grouped together.
- **Interferers**: Click this toggle to enable or disable the appearance of client icons on the floor map.
    - **Show Zone of Impact**: Click this toggle to enable or disable the appearance of the zone of impact from interferers.
- **Map Properties**: Contains the **Auto Refresh** setting.
    - **Auto Refresh**: Use this drop-down list to specify the time interval between each auto refresh for map data to occur.
- **Global Map Properties**: Contains the **Units of Measure** setting.
    - **Units of Measure**: Change the preferred measurement system to imperial system (feet) or metric system (meters). This setting applies to all wireless maps.

Edit Floor Map Elements and Overlays

While viewing a floor map, click **Add/Edit** from the map toolbar to enter edit mode. While in edit mode, you can do the following:

Add, position, and delete the following devices: • Access Points • Sensors
Add, edit, and delete the following overlay objects: • Coverage Areas • Location Regions • Walls • Shelvings • Markers • GPS Markers

About Interactive Floor Planning

Interactive planning helps you plan a floor layout by drawing planned APs or hypothetical APs and obstacles with a raster image or a CAD floor plan as the backdrop. You can export the floor map as a PDF and share it with the technicians who are mounting the APs. The floor drawing helps the technicians to visualize the floor layout and the exact AP mount locations.

With interactive floor planning, you can:

- Create a floor layout with a raster or CAD floor plan as the canvas.
- Place the planned APs or hypothetical APs on the floor map based on the signal coverage requirement. These hypothetical APs or planned APs are not yet installed or discovered by Cisco DNA Center.
- Assign the antenna type and orientation.
- Draw obstacles such as walls and shelvings on the floor which impacts the signal attenuation.
- Plan all APs in sequence.
- Export the floor map as a PDF.

Guidelines for Placing Access Points

Follow these guidelines while placing APs on the floor map:

- Place APs along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. APs placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other APs.
- Location accuracy can be improved by increasing overall AP density and moving APs close to the perimeter of the coverage area.
- In long and narrow coverage areas, avoid placing APs in a straight line. Stagger them so that each AP is more likely to provide a unique snapshot of the device location.
- Although the design provides enough AP density for high-bandwidth applications, location suffers because each AP view of a single device is not varied enough. Therefore, location is difficult to determine. Move the APs to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy.
- For optimal heatmap visibility on floor maps, configure the AP height to approximately 10 feet (3 meters) or lower.

Add, Position, and Delete APs

Cisco DNA Center computes heatmaps for the entire map that show the relative intensity of the Radio Frequency (RF) signals in the coverage area. For 2D wireless maps, the heatmap is only an approximation of the actual RF signal intensity because it does not consider the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Before you begin

Make sure that you have Cisco APs in your inventory. If not, discover APs using the Discovery feature. See About Discovery.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click the building floor.

Step 3 From the map toolbar, click **Add/Edit**.

Step 4 Ensure the **APs** toggle is enabled from the map toolbar.

Step 5 From the map left pane, click **Add APs**.

Step 6 From the **Add APs** slide-in pane, check the check boxes of the access points to select the APs in bulk, and click **Add Selected**. Alternatively click **Add** next to an access point.

> **Note** You can search for access points using the search option available. Use the **Filter** field to search for access points using the AP name, MAC address, model, or Cisco Wireless Controller. The search is case-insensitive. The search result appear in a table. Click **Add** to add one or more of these APs to the floor area.

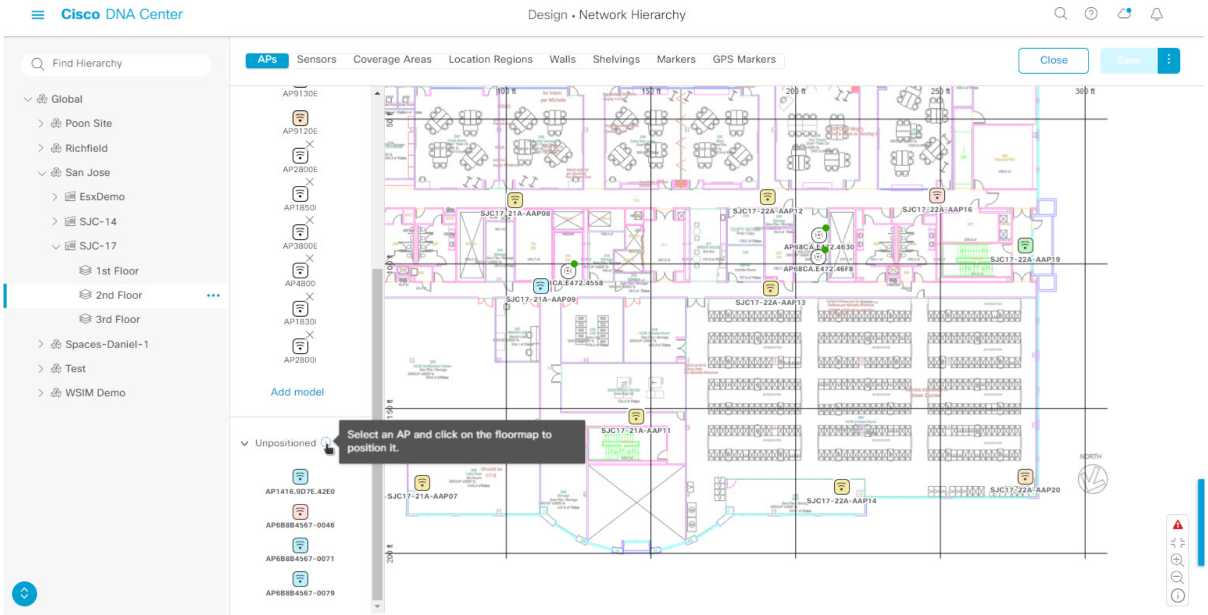
Result: Newly added APs appear in the **Unpositioned** category from the map left pane in edit mode.

Step 7 Close the **Add APs** window after assigning APs to the floor area.

Step 8 From the map toolbar, click **Add/Edit**.

Step 9 From the map left pane, click an AP from the **Unpositioned** category to position the AP.

Figure 2: Unpositioned APs



Select an AP and click on the floormap to position it.

Step 10 To position the AP, do one of the following:

- Click on the location of the floor map to position the AP.
- From the **Edit AP** slide-in pane, enter the x and y coordinates in the corresponding fields.
- You can draw three points on the floor map and position the AP by using the selected points. To do this:

  a. From the **Edit AP** slide-in pane, click **Position by 3 points**.

b. To define the points, click anywhere on the floor map to start drawing the first point. Click again to finish drawing a point. A dialog box appears to set the distance to first point. Enter the distance, in meters, and click **Set Distance**.

c. Define the second and third points similarly, and click **Save**.

- You can define two walls on the floor map and position APs between the defined walls. This helps you to know the position of APs between the two walls. This helps you to understand the AP position between the walls.

  a. From the **Edit AP** slide-in pane, click **Position by 2 walls**.

  b. To define the first wall, click anywhere on the floor map to start drawing the line. Click again to finish drawing a line. A dialog box appears to set the distance to the first wall. Enter the distance in meters and click **Set Distance**.

  c. Define the second wall similarly and click **Save**.

  Result: The AP is placed automatically based on the defined distance between the walls.

Step 11 Use the **Edit AP** slide-in pane to configure details of the AP such as:

- **AP Name**: Shows the AP name.
- **MAC Address**: Displays the MAC address.
- **AP Model**: Indicates the AP model of the selected access point.
- **x**: Indicates the x-axis coordinate of the AP. You can manually enter the value.
- **y**: Indicates the y-axis coordinate of the AP. You can manually enter the value.
- **AP Height**: Indicates the height of the access point. You can manually enter the value.
- **Antenna**: Antenna type for this access point.

  Note For external APs, you must select an antenna, or the AP will not be present in the map.

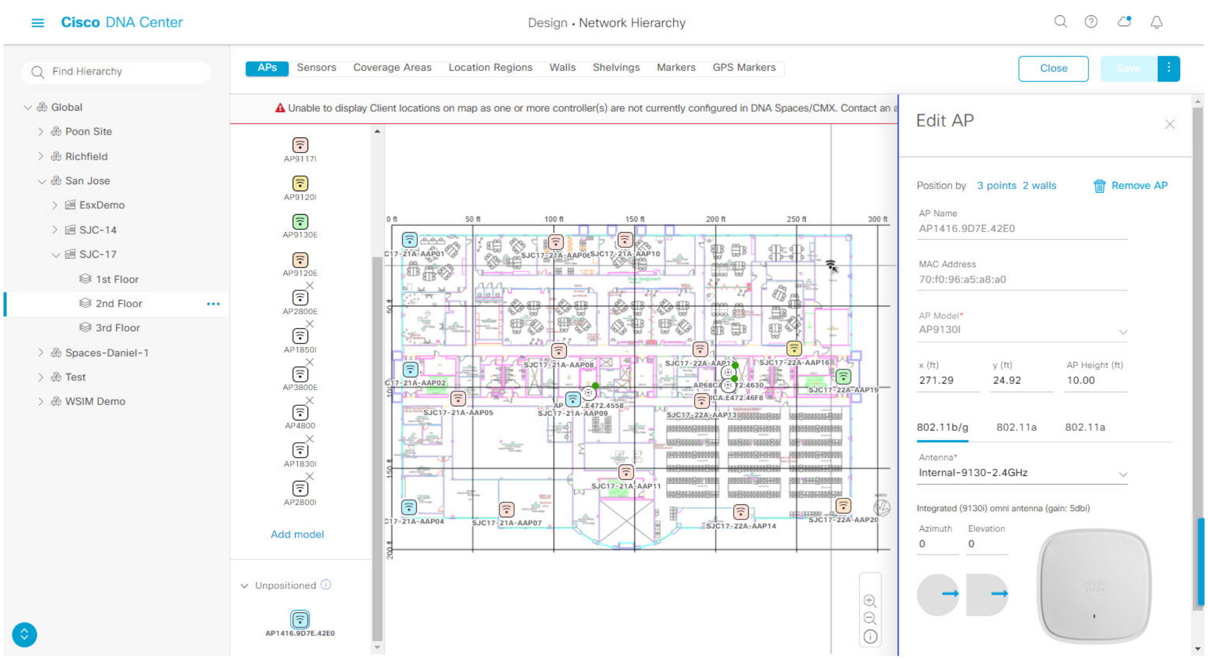
- **Azimuth**: The azimuth is the angle of the antenna measured relative to the x axis. The azimuth range is 0 to 360. In Cisco DNA Center, north is 0 or 360 degrees; east is 90 degrees.

  You can manually enter the value or use the blue arrow under the field to change the value.

  Note This option does not appear for omnidirectional antennas because their pattern is nondirectional in azimuth.

- **Elevation**: Displays the elevation in degrees. You can manually enter the value or use the blue arrow under the field to change the value.

Figure 3: Edit AP Slide-In Pane



Unable to display Client locations on map as one or more controller(s) are not currently configured in DNA Spaces/CMX. Contact an a

AP Name: AP1416.9D7E.42E0

MAC Address: 70:f0:96:a5:a8:a0

AP Model*: AP9130I

x (ft): 271.29 y (ft): 24.92 AP Height (ft): 10.00

Antenna*: Internal-9130-2.4GHz

Integrated (9130I) omni antenna (gain: 5dbi)

Azimuth: 0 Elevation: 0

Step 12 After you have completed placing and configuring access points, click **Save** from the map toolbar.

Note If a Cisco Connected Mobile Experiences (CMX) is synchronized with Cisco DNA Center, you can view the location of clients on the heatmap. See Create Cisco CMX Settings, on page 61.

Result: The heatmap is generated based on the new position of the AP.

Step 13 To delete APs from the floor map, click **Remove APs** from the map left pane while in edit mode.

Step 14 From the **Delete APs** slide-in pane, check the check boxes next to the access points that you want to delete, and click **Delete Selected**.

- To delete all the access points, click **Select All** and then **Delete Selected**.
- To delete an access point from the floor, click the **Delete** icon.
- Use **Quick Filter** and search using the AP name, MAC address, model, or controller. The search is case-insensitive. The search result appears in the table. Click the **Delete** icon to delete the APs from the floor area.

Place Planned Access Points on a Floor Map Using AP Model Catalog

Using the AP Model Catalog feature, you can configure one AP on the floor with the AP model, antenna type, azimuth, and elevation orientation, and then replicate that configuration on rest of the APs that belong to the same model type.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 Design your network hierarchy by adding sites, buildings, and floors.

Step 3 In the left pane, click a building floor.

Note You can draw the planned APs and obstacles on the selected floor.

Step 4 From the map left pane, in the **AP Models** area, click the AP model of the planned AP to add.

Note If the AP model is not listed, click **Add Model** to choose the AP model to add to the list.

Step 5 Using the drawing tool, click the location on the floor map to add the planned AP.

Result: A planned AP of the selected model is added to the floor map and the **Edit Planned AP** slide-in pane appears on the right, with an AP name added to it by default.

Step 6 From the **Edit Planned AP** slide-in pane, click the gear icon, which is located next to the **AP Name** field.

Result: The **Name pattern** dialog box appears.

Step 7 When you add the first AP to the floor, make sure that you enter a valid name pattern, for example SJC-BLD21-FL2-AP####, and then click **Set name pattern**.

Note The planned APs must be unique within Cisco DNA Center, so make sure that the name pattern identifies the floor.

The #### in the name pattern is replaced by numbers in the **AP Name**, for example SJC-BLD21-FL2-AP0001, SJC-BLD21-FL2-AP0002, and so on.

Step 8 From the **Antenna** drop-down list in the **Edit Planned AP** slide-in pane, choose the appropriate antenna type for each of the radio slots of the AP.

Note The antenna image reflects the antenna selected.

Step 9 Depending on the antenna type, enter the **Azimuth** and **Elevation** orientation, in degrees.

Step 10 To add another AP with the same AP properties as that of the AP that you just created, click a location in the floor map where you want to position the new AP.

Result: A new AP icon appears on the map with all of the properties inherited and the AP name appended, for example BLD1-AP0002-TX.

Step 11 To add more APs with the same properties and appended AP Name, click the floor map.

Step 12 To stop adding APs to the floor map, press **Esc** or right-click the floor map.

Step 13 To reposition the APs, drag and drop them to the appropriate location in the floor map.

Step 14 To delete a planned AP, right-click the AP icon and click **Delete**.

Step 15 To edit a planned AP, right-click the AP icon and click **Edit**.

Step 16 After you are finish adding planned APs, click **Save** from the map toolbar.

Export Bulk APs from Prime Infrastructure and Import into Cisco DNA Center

Cisco DNA Center allows you to import, assign and position a collection of access points to the floor map. If you have an existing collection of access points on Cisco Prime Infrastructure, you can import it into Cisco DNA Center, saving time and effort spent in importing, assigning, and positioning access points to the floor map.

This procedure describes how to export an existing collection of access points from Cisco Prime Infrastructure, and import into Cisco DNA Center.

Before you begin

- To perform the following task, you must be a **Super Admin** or **Network Admin**.
- Make sure that you have APs in your inventory. If not, discover them using the **Discovery** feature.
- Add and position APs on a floor map.
- The site, building, and floor must be present in the site hierarchy.

Step 1 Export the bulk AP positions from Cisco Prime Infrastructure as a CSV file to your workstation.

Step 2 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 3 From the left pane, hover your cursor over the ellipsis ••• next to the site and choose **Import Bulk AP**.

Step 4 In the **Import Bulk AP** pop-up window, drag and drop the AP file, or click **Choose a file** to select the file from your workstation.

Note

- To manually create the **AP Positions** CSV file with Prime Template, export a Prime Template to your workstation by clicking **Download Prime Template**. Prime Template does not support nested files.
- To manually create the **AP Positions** CSV file with Cisco DNA Template, export a Cisco DNA Template to your workstation by clicking **Download Template**. Cisco DNA Template supports nested files.

Wait for the CSV file to download. The CSV file contains information about AP positions of various sites in the network.

Step 5 Click **Import**.

Result: The **Import Summary** window appears.

- The **Information** tab shows the list of successfully imported APs.
- Click the **Warning** tab to see the list of warnings.
- Click the **Error** tab to see the list of errors.

Add, Position, and Delete Sensors

Note Make sure you have the Cisco AP 1800S sensor in your inventory. The Cisco Aironet 1800s Active Sensor must be provisioned using Plug and Play for it to show up in the Inventory.

A *sensor device* is a dedicated AP 1800s sensor. The Cisco Aironet 1800s Active Sensor gets bootstrapped using PnP. After it obtains the Assurance server reachability details, it directly communicates with the Assurance server.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click the building floor.

Step 3 From the map toolbar, click **Add/Edit**.

Step 4 From the map toolbar, click the **Sensors** toggle.

Step 5 From the **Add Sensors** slide-in pane, check the check boxes of the sensors that you want to add. Alternatively, click **Add** next to the sensor row to add sensors.

Note You can search for specific sensors using the search option. Use the **Filter** field and search using the name, MAC address, or model of a sensor. The search is case-insensitive. The search results are displayed in the table. Click **Add** to add one or more these sensors to the floor area.

Result: Newly added sensors appear in the **Unpositioned** category from the map left pane in edit mode.

Step 6 Close the **Add Sensors** slide-in pane after assigning sensors to the floor map.

Step 7 From the map toolbar, click **Add/Edit**.

Step 8 From the map left pane, click a sensor in the **Unpositioned** category to position the sensor.

Step 9 Click on the location of the floor map to position the sensor.

- You can use the **x**, **y**, and **sensorHeight** fields in the **Sensor Details** slide-in pane to enter the exact x, y, and z coordinates for the sensor.

Step 10 After you have completed placing and adjusting sensors, click **Save**.

Step 11 To delete a sensor from the floor map, click **Remove APs** from the map left pane while in edit mode.

Step 12 Check the check boxes of the sensors that you want to delete, and click **Delete Selected**.

- To delete all the sensors, click **Select All**, and click **Delete Selected**.
- To delete a sensor from the floor, click the **Delete** icon next to that sensor.
- Use **Quick Filter** and search using the name, MAC address, or model. The search is case-insensitive. The search results are displayed in a table. Click the **Delete** icon to delete one or more sensors from the floor area.

Add Coverage Areas

By default, any floor area or outside area defined as part of a building map is considered as a wireless coverage area.

If you have a building that is nonrectangular or you want to mark a nonrectangular area within a floor, you can use the map editor to draw a coverage area or a polygon-shaped area.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click the building floor.

Step 3 From the map toolbar, click **Add/Edit**.

Step 4 From the map toolbar, click the **Coverage Areas** toggle.

Step 5 From the map left pane, click the **Coverage Area** icon.

Step 6 In the **Coverage Area** pop-up window, enter a name for the coverage area in the field and click **Add Coverage**.

Step 7 Use the drawing tool to create the coverage area shape:

a) Click on the map to create a point and continue creating points to define the coverage area shape.

Note The coverage area shape must have at least 3 points.

b) You can click and drag any points to redefine the coverage area shape.

c) Double-click to exit the drawing tool and finalize the coverage area shape.

Step 8 After you can finish creating the coverage area, click **Save** from the map toolbar.

Step 9 To edit a coverage area, do the following:

a) From the map toolbar, click **Add/Edit**.

b) From the map toolbar, click the **Coverage Areas** toggle.

c) You can click and drag the points of the coverage area to redefine the shape.

d) To edit the coverage area name, right-click a coverage area and choose **Edit**.

e) After finishing making edits, click **Save** from the map toolbar.

Step 10 To delete a coverage area, do the following:

a) From the map toolbar, click **Add/Edit**.

b) From the map toolbar, click the **Coverage Areas** toggle.

c) Right-click the coverage area and choose **Delete**.

d) After finishing deleting, click **Save** from the map toolbar.

Add Walls on a Floor

Add walls on a building floor for a more accurate heatmap. Walls affect the signal attenuation and how the RF is calcuated in the heatmap.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, ensure that the **2D** toggle 2D 3D is enabled.

Step 4 From the map toolbar, click the **Walls** toggle.

Step 5 From the map left pane, click a wall type from the **Others** or **On this floor** categories.

Note If a wall type is not listed, click **Add Wall Type** to create a custom wall type.

Step 6 Use the drawing tool to create the wall area:

- Click on the map to create point and continue creating points until you have created the shape for the wall.
- To finalize a shape, click the wall type of the shape from the left pane to exit drawing mode. Alternatively, you can double-click on the map finalize the shape. If you want to cancel the shape, right-click on the map.
- To change the type of an existing wall, right-click the shape and choose **Change Type**.
- To move an existing wall, drag and drop the shape to the new location.

- To remove an existing wall, right-click the shape and choose **Delete**.

Add Shelvings on a Floor

Shelvings are a type of obstacle that affects signal attenuation. An example of a setting with shelvings would be a high-ceiling warehouse.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, ensure that the **2D** toggle 2D 3D is enabled.

Step 4 From the map toolbar, click the **Shelvings** toggle.

Step 5 From the map left pane, click the shelving type to add.

- In the shelving pop-up, you can edit the name, dimensions, and orientation (the angle of the shelving, example: 0 means that the shelving is vertical and parallel to the y axis) of the shelving type.
- If a shelving type is not in the list, click **Add Shelving Type** to create a new shelving type.

Step 6 Click **Add Shelving**.

Step 7 Drag and drop the shelving to move it to its location on the floor map.

Step 8 Right-click the shelving for the following actions:

- **Edit**: Edit the name, dimensions, and orientation for the shelving.
- **Clone**: Create a copy of the shelving.
- **Array**: Create an array of shelvings by specifying the number of shelvings and the distance between them.
- **Delete**: Remove the shelving from the floor map.

Step 9 After adding the necessary shelvings, click **Save** from the map toolbar.

Location Region Creation

You can create inclusion and exclusion areas to further refine location calculations on a floor. You can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas). For example, you might want to exclude areas such as an atrium or stairwell within a building, but include a work area, such as cubicles, labs, or manufacturing floors.

Guidelines for Placing Inclusion and Exclusion Areas on a Floor Map

- Inclusion and exclusion areas can be any polygon-shaped area and must have at least 3 points.
- You can only define 1 inclusion region on a floor. By default, an inclusion region is defined for each floor area when it is created. The inclusion region is indicated by a solid aqua line, and generally outlines the entire floor area.

- You can define multiple exclusion regions on a floor area.

Define an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are defined within the borders of an inclusion area.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, click **Add/Edit**.

Step 4 From the map toolbar, click the **Location Regions** toggle.

Step 5 From the map left pane, click the **Exclusion** icon.

Step 6 Use the drawing tool to create the exclusion area:

- Click on the map to create point and continue creating points until you have created the shape for the exclusion area.
- To finalize the shape, click the **Exclusion** icon from the left pane to exit drawing mode. Alternatively, you can double-click on the map to finalize the shape. If you want to cancel the shape, right-click on the map.
- To move an existing exclusion area, drag and drop the shape to the new location.
- To remove an existing exclusion area, right-click the shape and choose **Delete**.

Step 7 After you are finish creating exclusion areas, click **Save** from the map toolbar.

Define an Inclusion Region on a Floor

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, click **Add/Edit**.

Step 4 From the map toolbar, click the **Location Regions** toggle.

Step 5 From the map left pane, click the **Inclusion** icon.

Step 6 Use the drawing tool to create the inclusion area:

- Click on the map to create point and continue creating points until you have created the shape for the inclusion area.
- To finalize the shape, click the **Inclusion** icon from the left pane to exit drawing mode. Alternatively, you can double-click on the map to finalize the shape. If you want to cancel the shape, right-click on the map.
- To move an existing inclusion area, drag and drop the shape to the new location.
- To remove an existing inclusion area, right-click the shape and choose **Delete**.

Step 7 After you are finish creating inclusion areas, click **Save** from the map toolbar.

Place Markers

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, click **Add/Edit**.

Step 4 From the map toolbar, click the **Markers** toggle.

Step 5 Enter the name for the marker, and then click **Add Marker**.

Step 6 Use the drawing tool to place the marker:

- Click on the map to place the marker.
- To move the marker,
- To edit an existing marker, right-click the marker and choose **Edit**.
- To remove an existing marker, right-click the marker and choose **Delete**.

Step 7 Click **Save** from the map toolbar.

Add GPS Markers

To increase the accuracy of a client's position, Cisco DNA Center GPS markers enable you to find the actual position of a building space on the world map.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, click **Add/Edit**.

Step 4 From the map toolbar, click the **GPS Markers** toggle.

Step 5 From the map left pane, click the **GPS Markers** icon.

Step 6 Use the drawing tool to place the GPS marker:

a) Click on the map to place the GPS marker.
b) In the **Place Markers** pop-up window, enter the name, latitude, longitude, x and y coordinates in the appropriate fields.
c) Click **Add GPS Marker**.

Step 7 Repeat Step 6 until there are three GPS markers on the floor map in a polygon-shape.

Step 8 To edit an existing GPS marker, right-click the GPS marker and choose **Edit**.

Step 9 To remove an existing GPS marker, right-click the GPS marker and choose **Delete**.

Step 10 Click **Save** from the map toolbar.

Note The GPS marker is an attribute of the building and can be applied to all the floors of the building.

Identify Wireless Interferers on the Floor Map

Cisco DNA Center detects interference and disables the interference source for a specific band on a floor map. Any interference in the 2.4-GHz band disrupts the network traffic of the 802.11 wireless network.

Cisco DNA Center identifies the position, area of impact, and intensity of the interferer.

This procedure shows how to identify network interferers on a floor map.

Before you begin

Ensure that either Cisco Connected Mobile Experiences (CMX) or Cisco DNA Spaces is synchronized with Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 Hover your cursor over the ellipsis icon ••• next to the floor and choose **Sync: DNA Spaces/CMX** to synchronize **DNA Spaces** or **CMX** with the floor.

Note (Optional) In the world map, hover your cursor over the floor and choose **Sync: DNA Spaces/CMX** to synchronize **DNA Spaces** or **CMX** with the floor.

Step 4 In the **Network Hierarchy** window, click **View Options**.

Step 5 In the **View Options** window, scroll down and click the **Interferers** toggle to enable interferers to appear on the floor map.

Step 6 Expand the **Interferers** category and click the **Show Zone of Impact** toggle to enable the zone of impact of interferers to appear on the floor map.

Note By default, **Zone of Impact** is disabled.

Step 7 In the floor map, hover your cursor over the interferer icon and click the impacted channel to view the interferer device details.

Filter Device Data on a Floor

For 2D wireless maps, you can apply various filters to network devices such as access points, sensors, and so on. Based on the filter criteria, the search results appear in a table. Filtering device data is helpful in locating specific devices for floors with many devices.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, ensure that the **2D** toggle 2D 3D is enabled.

Step 4 From the map toolbar, click **Data**.

Step 5 From the **Data** slide-in pane, click the device type that you want to apply a filter.

Step 6 Define the filter rules by using the drop-down lists to choose the parameters.

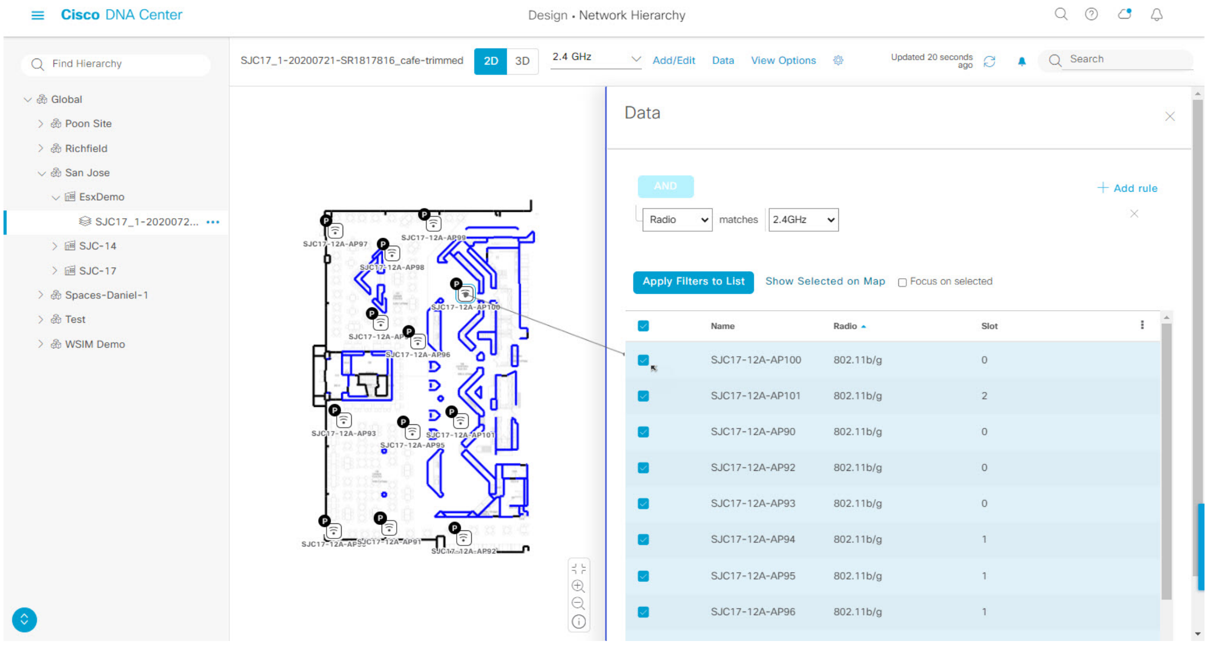
Step 7 To add more filter rules, click the + icon near the top of the slide-in pane.

Step 8 After you are finish defining the filter rules, click **Apply Filters to List**.

Result: The filter results appear in the table at the bottom of the slide-in pane.

Step 9 You can hover your cursor over a device in the table to locate its position on the floor map.

Figure 4: Locating a Device from the Filter Results



Radio matches 2.4GHz

☑	Name	Radio	Slot
☑	SJC17-12A-AP100	802.11b/g	0
☑	SJC17-12A-AP101	802.11b/g	2
☑	SJC17-12A-AP90	802.11b/g	0
☑	SJC17-12A-AP92	802.11b/g	0
☑	SJC17-12A-AP93	802.11b/g	0
☑	SJC17-12A-AP94	802.11b/g	1
☑	SJC17-12A-AP95	802.11b/g	1
☑	SJC17-12A-AP96	802.11b/g	1

Step 10 To remove applied filters, do the following:

a) Close the **Data** slide-in pane.

b) From the map toolbar, click **Data**.

c) Click the filter icon next to the device type to remove the filter.

Create a Floor Map Using an Ekahau Project File

You can create your network hierarchy in Ekahau Pro and import it into Cisco DNA Center for further planning.

Step 1 Plan the floor layout in the Ekahau Pro tool.

- (Optional) Create buildings and floors.
- Import the floor plan.
- Add the planned (or hypothetical) APs.

  The AP name that you provide here will be used to update the AP name on the Cisco Wireless Controller during the wireless controller configuration.
- Add building coordinates.

- Define the site name.
- Add obstacles.
- Export the project.

Note If you're using Ekahau Cloud, make sure to synchronize any local changes to the Ekahau Cloud before exporting the Ekahau project. If the Ekahau project has local changes (such as the removal of an AP or wall) that are out-of-sync with the Ekahau Cloud project, importing the Ekahau project to Cisco DNA Center can fail.

Step 2 Deploy the planned APs at locations designed on the floor layout.

- The physical AP is mounted at the designed location that is specified on the floor layout. The MAC address of the planned AP is updated with the MAC address of the physical AP.
- The physical AP is connected to the VLAN of the intended wireless controller.

Step 3 Configure the Cisco Wireless Controller.

- Discover the Cisco Wireless Controller and APs in your network by running the **Discovery** job, so that the discovered wireless controllers and APs are listed on the **Inventory** window.
- Update the AP name on the wireless controller with the AP name given in the Ekahau Pro project during the floor planning.

Step 4 Import the Ekahau project into Cisco DNA Center.

Step 5 Map the planned APs to real APs in Cisco DNA Center.

Import an Ekahau Project to Cisco DNA Center

Before you begin

Importing an Ekahau Cloud project can fail if the project has local changes (such as removing an AP or wall), that are out-of-sync with the Ekahau Cloud project. To avoid this situation, make sure to synchronize any local changes to the Ekahau Cloud before importing the Ekahau Cloud project to Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 Design your network hierarchy by adding sites, buildings, and floors.

Note For more information, see Create a Site in a Network Hierarchy, on page 2, Add a Building, on page 7, and Add a Floor to a Building, on page 9.

While adding floors, make sure that you create floors with the same name given in the Ekahau project.

Step 3 In the left pane, hover your cursor over the ellipsis ••• icon next to the site where you want to import the Ekahau project and choose **Import Ekahau Project**.

The **Import Ekahau Project** dialog box appears.

Step 4 Drag and drop the ESX file into the boxed area in the **Import Ekahau Project** dialog box, or click the **click to select** link and browse to the ESX file.

> **Note** To import buildings, they need to contain coordinates inside the Ekahau Project. You can add coordinates in Ekahau Pro. After successfully importing an Ekahau Project, each planned AP is mapped to an existing real AP in the inventory using the AP name. The planned AP is displayed with an icon **P** on the floor map. For example, if the name of the planned AP is SJC01-02-AP-B-1, the import process searches for the real AP with the same name.

Step 5 If an AP is not found in the inventory and remains unmapped, the planned AP is retained on the floor.

To see the reason for the mismatch, hover your cursor over the planned AP icon on the floor map, and click **Import History**.

The following attempts are made to map the planned APs to real APs:

- If the newly discovered APs match the planned AP, the planned AP is replaced with the discovered real AP.
- If a planned AP remains unmapped, you can manually replace the planned AP with the real AP, providing reasons for the failure.

Step 6 To manually assign the planned AP to a real AP, hover your cursor over the planned AP icon on the floor map, and click **Assign** > **Assign**.

The **Assign Planned APs** panel appears.

Step 7 In the **Assign Planned APs** panel, map the planned AP to a real AP by AP name, AP type, or All APs.

Step 8 Click the radio button next to the AP Name, and click **Assign** to manually assign the planned AP.

Step 9 Click **Save**.

Export the Ekahau Project from Cisco DNA Center

To augment the preconfigured working floors, the Cisco DNA Center allows you to export the working floors from Cisco DNA Center as an Ekahau project and import the project into the Ekahau Pro Tool.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis ••• icon next to the site, building, or floor and choose **Export Maps**.

Result: The **Export Maps** dialog box appears.

Step 3 Choose the **Ekahau Project** export format.

Step 4 Click **Export**.

Result: A Ekahau project is created as an ESX file type and saved to your local hard drive.

Step 5 Import the ESX file into the Ekahau Pro tool, augment the floor, and save the file.

Step 6 Import the Ekahau project into the Cisco DNA Center under the site.

For more information, see Import an Ekahau Project to Cisco DNA Center.

Visualize Your Wireless Network in 3D

About 3D Wireless Maps

With 3D wireless maps, you can view a 3D visualization of your wireless network. A near real-time predictive model dynamically updates the 3D visualization to show changes in RF coverage.

Here are some of the unique features and functionality that 3D wireless maps offers:

- Navigate through your wireless network in a 3D environment with a first person view or third person view.
- Gain insights into the areas in your wireless network where service-level agreements (SLAs) are not being met.
- View the RF coverage for different elevations and use the **Scanner** tool to view the RF coverage for specific elevations.
- Crop the Key Performance Indicator (KPI) heatmap with the clipping tools.
- Predict the x, y, z coordinates of a specific point on the floor plan with the pin tool to better plan for placement of APs or sensors.
- Visualize floor plan elements, such as walls, in 3D to see how they affect RF coverage and attenuation.

Prerequisite

The system you use to compute and display 3D wireless heatmaps must have a Graphical Processing Unit (GPU) installed and enabled on it. For example, if you're using a Windows virtual machine (VM), you need to make sure that it has a GPU.

Creating the 3D Wireless Map

To view a 3D wireless map, you will need to create a floor plan for the 3D wireless map. There are three ways to create the floor plan for the 3D wireless map:

- **Import a CAD file**: When you use a CAD file (DXF or DWG file type) to import the floor plan, Cisco DNA Center imports the CAD layers and allows you to specify which layers will appear as floor elements in the 3D wireless map.
- **Import a 2D image file**: You can use the file types JPG, GIF, PNG, or PDF to import the floor plan. However, you will need to manually create the floor elements, such as the walls and shelving, in order for them to be represented in the 3D wireless map.
- **Import a Ekahau Pro Project plan**: The data from the Ekahau project, such as the obstacles, APs, and more, are imported into the 3D wireless map.

Create a 3D Floor Map with a CAD File

To view a 3D wireless map, you will need to create a 3D floor map.

You can use CAD files (the DXF or DWG file type) to create a 3D floor map. With CAD files, Cisco DNA Center imports the layers for the walls, shelving, obstacles, and more, to the 3D floor map.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis ••• next to the building of the floor and choose **Add Floor**.

Step 3 In the **Floor Name** field, enter a name for the floor.

Step 4 For the **Type (RF Model)** drop-down list, choose the RF model to apply to the floor.

Note The RF model determines how the RF is calculated based on the characteristics of the floor.

Step 5 Drag and drop the CAD file (the DXF or DWG file type) to the **Floor Image** area.

Step 6 In the **Floormap** pop-up window, choose the CAD layers that you want to appear as floor elements in the map:

a) For the **2D** column, check the check boxes of the CAD layer that you want to appear in the 2D view.

b) For the **3D Wall/Shelving Type** column, use the drop-down list to choose a CAD layer which specifies the type of the wall or shelving.

Note For a layer to appear in the 3D view, it is required to have a **3D Wall/Shelving Type** value. The wall/shelving type affects attenuation and how the heatmap is calculated.

c) Click **Use Selected Layers**.

Step 7 Enter the floor map dimensions in the **Width**, **Length**, and **Height** fields.

Step 8 Click **Add**.

Create a 3D Floor Map with a Non-CAD File

To view a 3D wireless map, you will need to create a 3D floor map.

You can use non-CAD files (a JPG, GIF, PNG, or PDF file type) to create a 3D floor map. However, when using a non-CAD file, the 3D floor elements, such as the walls and shelvings, cannot be imported, and you will have to manually add them.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis ••• next to the building of the floor and choose **Add Floor**.

Step 3 In the **Floor Name** field, enter a name for the floor.

Step 4 For the **Type (RF Model)** drop-down list, choose the RF model to apply to the floor.

Note The RF model determines how the RF is calculated based on the characteristics of the floor.

Step 5 Drag and drop the non-CAD file (a JPG, GIF, PNG, or PDF file type) to the **Floor Image** area.

Step 6 Click **Add**.

Result: The floor map is created.

Step 7 From the map toolbar, click **Add/Edit**.

Step 8 To add walls as a 3D floor element, do the following:

a) From the map toolbar, click the **Walls** toggle to add the appropriate floor element.

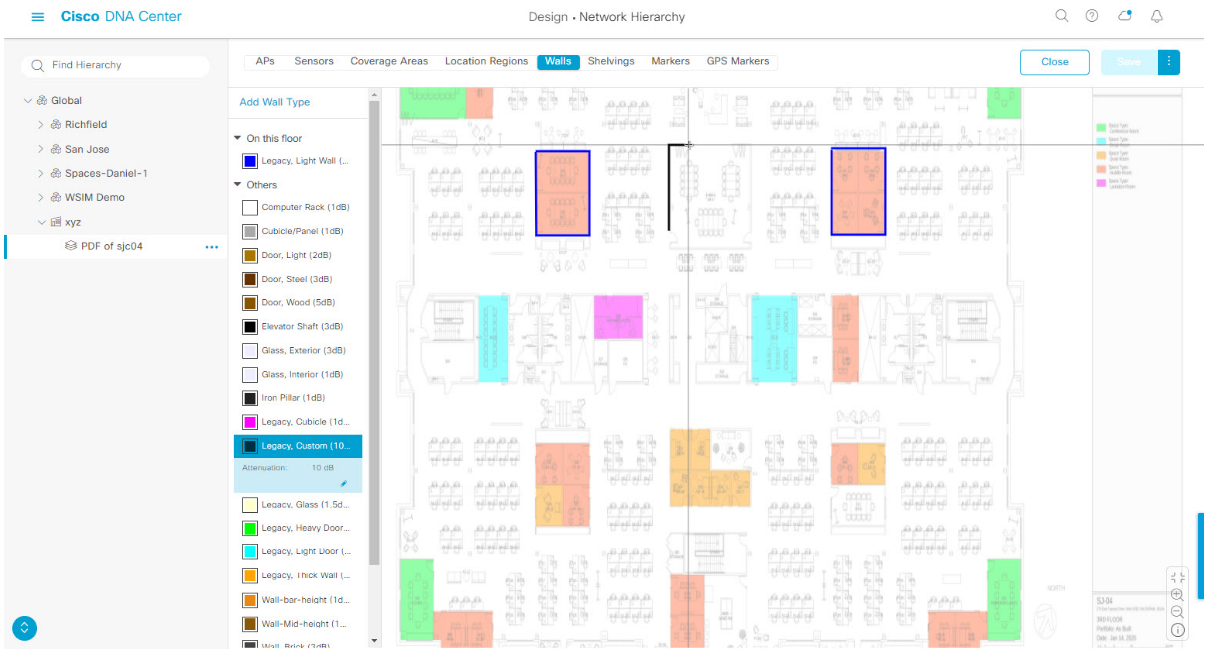
b) From the left pane of the map, click the wall type that you want to add.

- If the wall type is not in the list, click **Add Wall Type** to create a new wall type.

c) Use the drawing tool to create the wall area:

- Click on the map to create a point. Continue creating points until you have created the shape for the wall.
- To finalize a shape, click the wall type of the shape from the left pane to exit drawing mode. Alternatively, you can double-click on the map to finalize the shape. If you want to cancel the shape, right-click on the map.
- To change the type of an existing wall, right-click the shape and choose **Change Type**.
- To move an existing wall, drag and drop the shape to the new location.
- To remove an existing wall, right-click the shape and choose **Delete**.

Figure 5: Adding a Wall with the Drawing Tool



Step 9

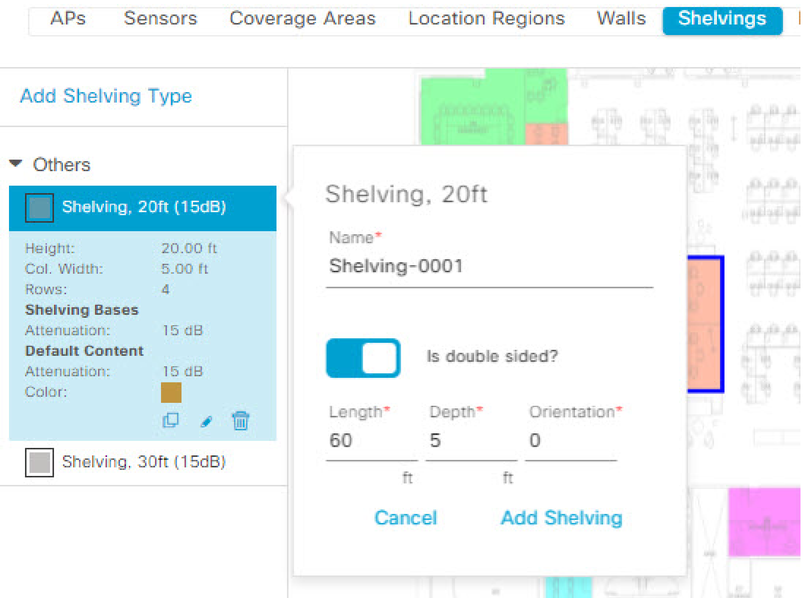
To add shelving as a 3D floor element, do the following:

a) From the map toolbar, click the **Shelvings** toggle.

b) From the left pane of the map, click the shelving type that you want to add.

- In the shelving pop-up window, you can edit the name, dimensions, and orientation of the shelving type. Orientation refers to the angle of the shelving (for example: 0 means that the shelving is vertical and parallel to the y axis).
- If a shelving type is not in the list, click **Add Shelving Type** to create a new shelving type.

Figure 6: Choosing a Shelving Type to Add



Shelving, 20ft (15dB)

Height: 20.00 ft
Col. Width: 5.00 ft
Rows: 4
Shelving Bases
Attenuation: 15 dB
Default Content
Attenuation: 15 dB
Color:

Shelving, 30ft (15dB)

Shelving, 20ft

Name*: Shelving-0001

Is double sided? (enabled)

Length*: 60 ft
Depth*: 5 ft
Orientation*: 0

c) From the shelving pop-up window, click **Add Shelving** to add the shelving to the floor map.

d) Drag and drop the shelving to move it to a location on the floor map.

e) Right-click the shelving for the following actions:

- **Edit**: Edit the name, dimensions, and orientation of the shelving.
- **Clone**: Create a copy of the shelving.
- **Array**: Create an array of shelvings by specifying the number of shelvings and the distance between them.
- **Delete**: Remove the shelving from the floor map.

Step 10 After adding the necessary walls and shelvings, click **Save** from the map toolbar.

View a 3D Wireless Map

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

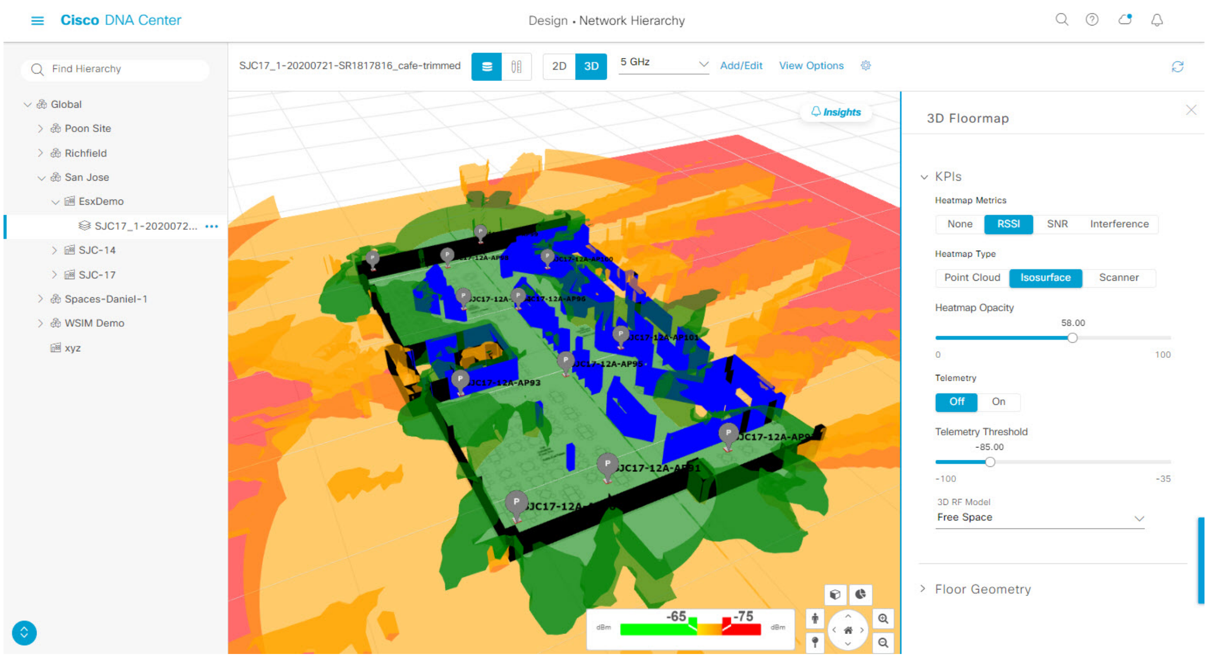
Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, click the **3D** toggle 2D 3D.

Step 4 From the map toolbar, ensure that the **Operation** toggle is enabled.

Result: The 3D wireless map appears in operation mode.

Figure 7: 3D Wireless Map in Operation Mode



Step 5 Use the map toolbar for the following actions and settings:

Item	Description
☰ ▯▯	**Operation and Simulation Toggle**: Use this toggle to switch between Operation mode and Simulation mode.
2D 3D	**2D and 3D Toggle**: Use this toggle to view the wireless map in 2D or 3D.
5 GHz ⌄	**Wi-Fi Band Filter**: Use this filter to view the heatmap for the 2.4 GHz and 5 GHz Wi-Fi bands.
Add/Edit	Click to enter add and edit mode which allows to add and edit map elements.
View Options	Open the **3D Floormap** slide-in pane which contains the KPI, telemetry, and floor element settings.
⚙	**Gear Icon**: Hover your cursor over this icon and choose **Insights Configuration** to customize the conditions for insights.

Step 6 To view the heatmap for one or more APs, select and deselect the APs using one of the following methods:

- To select a single AP, click the AP.
- To select multiple APs, press the `Shift` key while clicking each AP, and then release the `Shift` key.
- To deselect a single AP, click the AP.

Note If no APs are selected, the heatmap includes all APs.

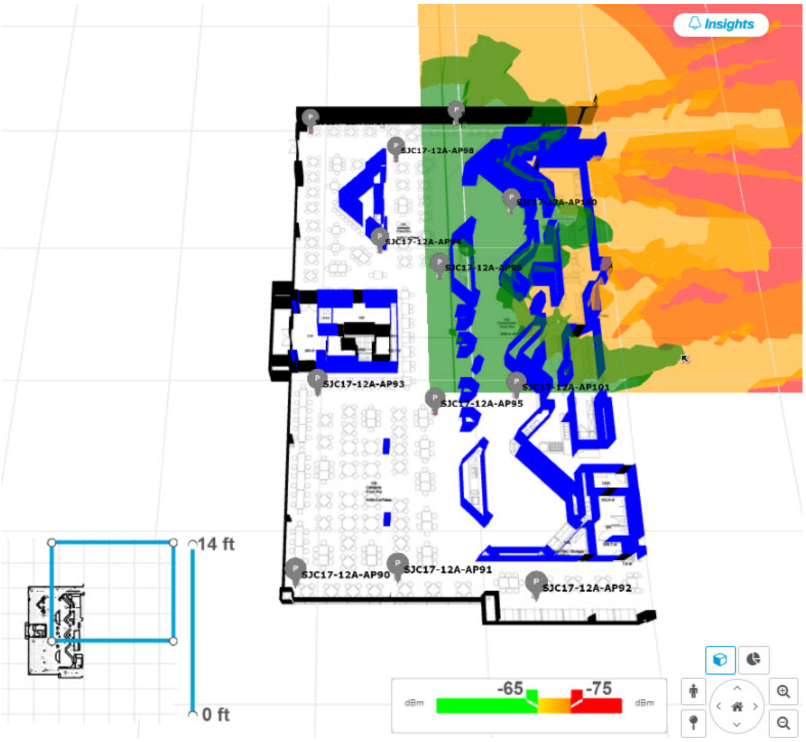
- To deselect all APs, press the **ESC** key or double-click an area of the map that doesn't have any APs.

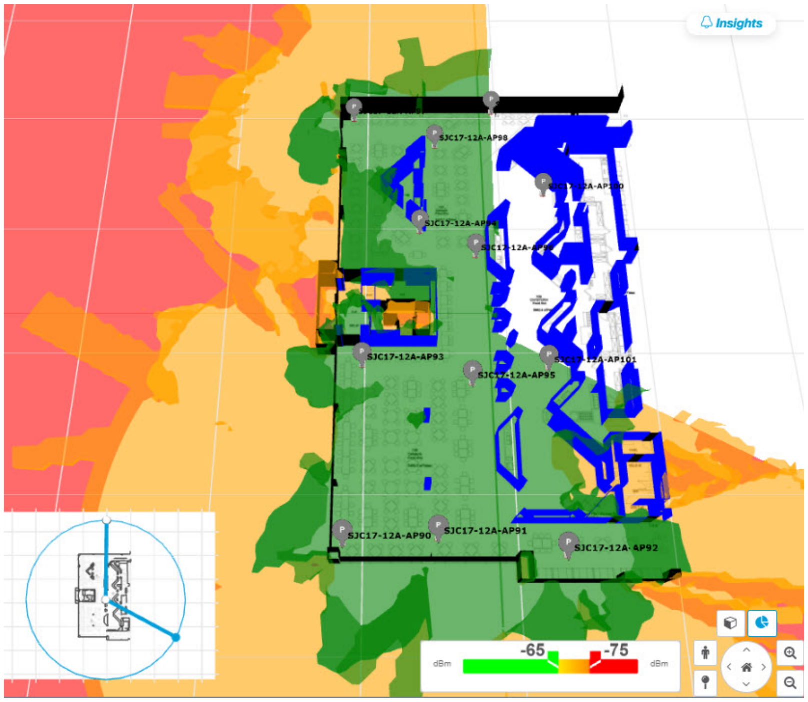
Step 7 At the top-right of the map, click **Insights** to view insights and potential issues in wireless network.

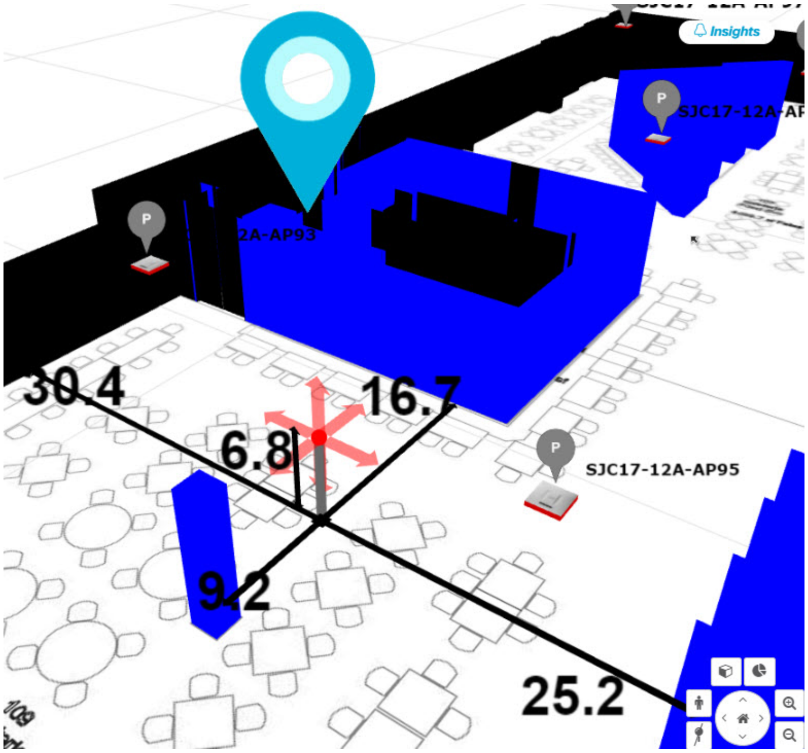
For details, see Gain Insights for a 3D Wireless Map, on page 40.

Step 8 Use the map for the following functionality:

- View the heatmap of the 3D wireless map. You can customize the KPIs, telemetry, and 3D map element settings from the **3D Floormap** slide-in pane.
- When the map is in default map view, you can control the camera angle by:
  - Clicking and dragging with the left mouse button to move the map laterally.
  - Clicking and dragging with the right mouse button to rotate the camera angle.
- Use the map navigation controls at bottom-right of the map for greater control of the map:

Map Navigation Control	Description
⬡	**Use clip box**: Crop the heatmap by using a box shape. Use the clipper at the bottom-left of the map to specify the crop: • Click and drag the 4 circles of the box to change the size of the crop. • Click and drag the 2 circles of the right vertical slider to specify the height range of the crop. *Figure 8: Clip Box*  Insights SJC17-12A-AP98 SJC17-12A-AP100 SJC17-12A-AP96 SJC17-12A-AP93 SJC17-12A-AP95 SJC17-12A-AP101 SJC17-12A-AP90 SJC17-12A-AP91 SJC17-12A-AP92 14 ft 0 ft dBm -65 -75 dBm

Map Navigation Control	Description
◕	**Use clip planes**: Crop the heatmap by using a donut shape. Use the clipper at the bottom-left of the map to specify the crop: - Click and drag the circle in the center of the donut to reposition the donut. - Click and drag the outer 2 circles to change the shape of the crop. ***Figure 9: Clip Planes in Use***  Insights SJC17-12A-AP98 SJC17-12A-AP100 SJC17-12A-AP93 SJC17-12A-AP95 SJC17-12A-AP101 SJC17-12A-AP90 SJC17-12A-AP91 SJC17-12A-AP92 -65 -75 dBm dBm
🧍 / 🧍	**First Person View / Third Person View**: Click the icon to toggle between first person view and third person view. For details, such as the controls for view, see Use First Person and Third Person View for 3D Wireless Maps, on page 41.

Map Navigation Control	Description
📍	**Place a pin**: Receive a predicted measurement (x, y, and z coordinates) of a specific point on the floor map by placing a pin. Click and drag the red arrows around the pin to change the position of the pin. For a video demonstration, click here. *Figure 10: Adjusting a Pin*  Insights SJC17-12A-AP 2A-AP93 30.4 16.7 6.8 SJC17-12A-AP95 9.2 25.2
🔍+ / 🔍−	**Zoom In / Zoom Out**: Zoom in and out on the map. Alternatively, you can use your mouse wheel to zoom in and out.
^ < 🏠 > v	**Map Rotation and Default Map View**: Use the directional arrows to change the camera angle. Use the home icon to reset the map view to the default.

Step 9 Use the **3D Floormap** slide-in pane to configure the KPI and floor map element settings. Expand the following categories to view the settings:

- **KPI Category**: Contains the KPI and telemetry settings:

Item	Description
Heatmap Metrics	Change the KPI to be displayed on the heatmap: • **None**: Disables the heatmap. • **RSSI**: Displays the Received Signal Strength Indication (RSSI) values. • **SNR**: Displays the signal-to-noise ratio (SNR) values. • **Interference**: Displays the SNR that is caused by co-channel interference (CCI) or adjacent channel interference.
Heatmap Type	Change the heatmap type: • **Point Cloud**: Provides a collection of data points in space. Each data point has x, y, and z coordinates. • **Isosurface**: Represents the RSSI with isolines or lines of a contiguous value. • **Scanner**: Displays the RSSI for a specific elevation.
Heatmap Opacity	Use the slider to customize the opacity or transparency of the heatmap.
Telemetry	Use this toggle to enable or disable telemetry. When telemetry is enabled, click a sensor or AP to view its telemetry: • The telemetry for a sensor displays the predicted and measured RSSI values between a sensor AP and other APs. • The telemetry for an AP displays the predicted and measured RSSI values between neighbor APs.
Telemetry Threshold	When telemetry is enabled, use this slider to set the threshold for telemetry sources to appear. Telemetry sources with predicted values that do not meet the threshold are faded.
3D RF Model	Use this drop-down list to choose RF model. The RF model determines how RF is calculated based on the floor type.

- **Floor Geometry Category**: Contains the floor map element settings:

Item	Description
Geometry	Use this toggle to enable or disable the 3D map elements, such as walls.
CAD Layers	Choose the CAD layers that you want to appear on the map.

Create Simulations for 3D Wireless Maps

You can create simulations for 3D wireless maps. Simulations allows you to make changes to device configurations without having to save those changes in Operation mode. You can create multiple simulations and load them at any time.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, click the **3D** toggle 2D 3D.

Step 4 From the map toolbar, click **Add/Edit**.

Step 5 Make the necessary changes to the devices:

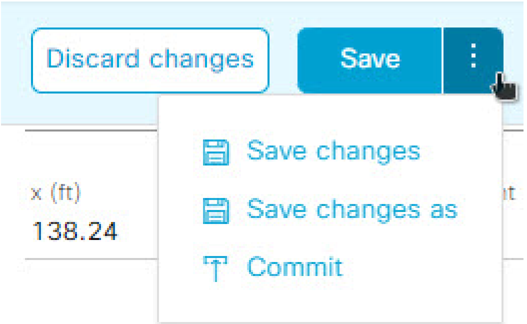
a) Click an AP.

b) Change the AP configuration settings in the slide-in pane.

c) Click **Apply**.

Step 6 From the map toolbar, hover your cursor over the vertical ellipsis and choose **Save changes as**.

Figure 11: Saving as a Simulation



Note Choosing **Save changes** saves your changes to Operation mode.

Choosing **Commit** saves your changes to production devices.

Step 7 In the **Save Simulation** pop-up window, enter a name for the simulation and click **Save**.

Result: The simulation is created.

Step 8 To load a simulation, click the **Simulation** toggle from the map toolbar.

Result: The 3D wireless map enters simulation mode which is indicated by the map toolbar color changing to light blue.

Step 9 Use the drop-down list to the right of the **Simulation** toggle to choose which simulation to load.

Gain Insights for a 3D Wireless Map

Cisco DNA Center actively monitors the network performance of 3D wireless maps and provides insights for areas where service-level agreements (SLA) are not being met.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

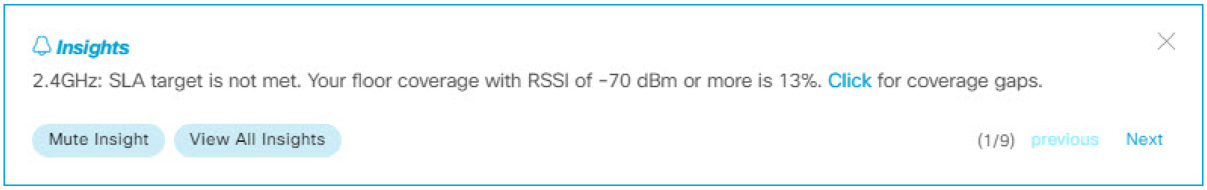
Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, click the **3D** toggle 2D 3D.

Step 4 At the top right of the map, click **Insights**.

Result: The **Insights** area appears.

Figure 12: Insights Area



Insights

2.4GHz: SLA target is not met. Your floor coverage with RSSI of -70 dBm or more is 13%. Click for coverage gaps.

Mute Insight View All Insights (1/9) previous Next

Step 5 From the **Insights** area, you can do the following:

Actions	Details
View insight details.	The **Insights** area displays the insight details. To cycle through the insights, click **Next** and **previous**. An insight reports the percentage of floor coverage area which does not meet a specific KPI threshold (for example, RSSI is ≥ -70 dBm). Click **Click** to view the affected areas.
Get an overview of all insights.	Click **View All Insights** to open the **All Insights** slide-in pane which displays all insights (active and muted).
Customize the insight settings.	Customizing an insight settings allows you to change insight's KPI threshold value. Click **View All Insights** and then click **Edit Configuration** for an insight to customize its settings. Alternatively, you can hover your cursor over the gear icon ⚙ from the map toolbar and choose **Insights Configurations** to customize insight settings.
Mute an insight.	Click **Mute Insight** to stop Cisco DNA Center from reporting the insight. Muted insights appear at the bottom of the list in the **All Insights** slide-in pane.

Use First Person and Third Person View for 3D Wireless Maps

You can use the first person and third person views to gain a different perspective of your wireless network.

Step 1 Click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

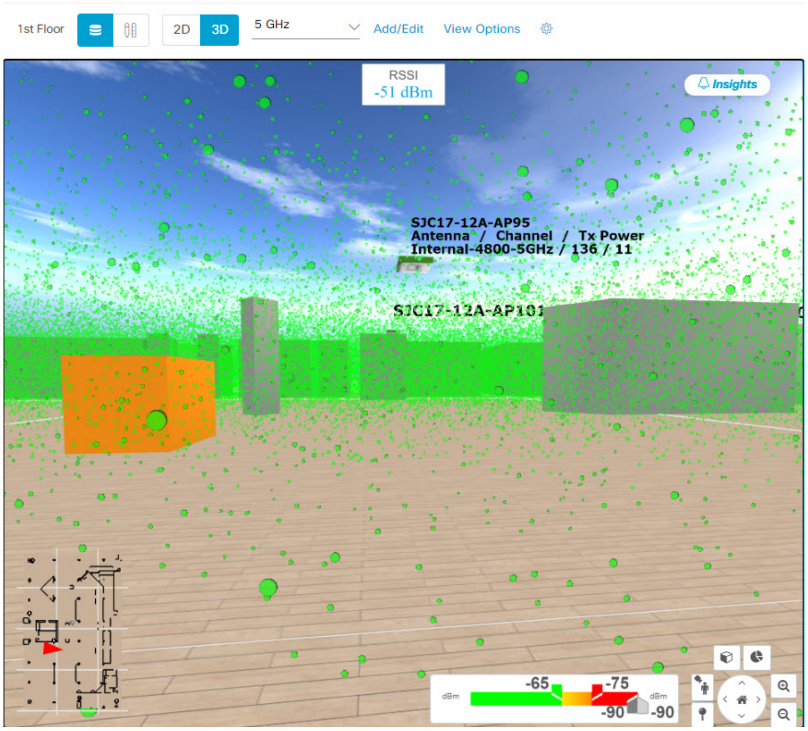
Step 2 In the left pane, click a building floor.

Step 3 From the map toolbar, click the **3D** toggle 2D 3D.

Step 4 To use the first person view, click the first person view icon from the map navigation controls.

Result: The map view changes to the first person view.

Figure 13: First Person View



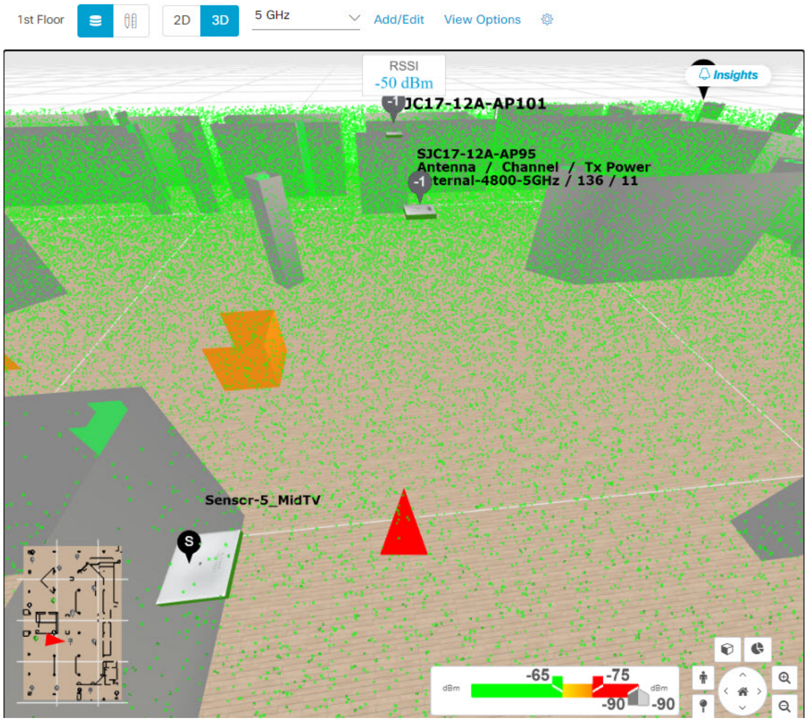
Step 5 You can control the first person view by doing the following:

Action	Controls
Move forward/backward and right/left.	Use the **W**, **A**, **S**, and **D** keys or arrow keys.
Change the camera angle.	Click and drag on the map.
Raise the altitude of the camera angle.	Hold the **Spacebar**.
Lower the altitude of the camera angle.	Hold **Shift** + **Spacebar**.

Step 6 To use the third person view, click the third person icon from the map navigation controls.

Result: The map view changes to the third person view.

Figure 14: Third Person View



Step 7 You can control the third person view by doing the following:

Action	Controls
Move forward/backward and right/left.	Use the **W**, **A**, **S**, and **D** keys or arrow keys.
Change the camera angle.	Click and drag on the map.
Raise the altitude of the camera angle.	Hold the **Spacebar**.
Lower the altitude of the camera angle.	Hold **Shift** + **Spacebar**.

Configure Global Wireless Settings

Global wireless network settings include settings for Service Set Identifier (SSID), wireless interfaces, wireless radio frequency (RF), and sensors.

Note Creating a wireless sensor device profile applies only to Cisco Aironet 1800s Active Sensor devices.

Create SSIDs for an Enterprise Wireless Network

The following procedure describes how to configure SSIDs for an enterprise wireless network.

Note The SSIDs are created at the global level. The site, building, and floor inherit settings from the global level.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, ensure that **Global** is selected.

Step 4 From the **SSID** table, hover over ⊕Add ∨ and choose **Enterprise**.

Result: The **Wireless SSID** workflow appears.

Step 5 Complete the **Basic Settings** step:

a) In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network.

b) For **Wireless Option**, choose the wireless band preference:

- **Dual band operation (2.4 GHz and 5 GHz)**: The WLAN is created for 2.4 GHz and 5 GHz. By default, band select is disabled.
- **Dual band operation with band select**: The WLAN is created for 2.4 GHz and 5 GHz and band select is enabled.
- **5 GHz only**: The WLAN is created for 5 GHz and band select is disabled.
- **2.4 GHz only**: The WLAN is created for 2.4 GHz and band select is disabled.

c) For **Type of Enterprise Network**, choose how the quality of service is provisioned on the wireless network:

- **Voice and Data**: The quality of service is optimized for voice and data traffic.
- **Data Only**: The quality of service is optimized for wireless data traffic only.

d) For **SSID STATE**, customize the following settings:

- **Admin Status**: Use this toggle to enable or disable the admin status.
- **Broadcast SSID**: Use this toggle to enable or disable the visibility of the SSID to all wireless clients within range.

Step 6 Complete the **Security Settings** step:

a) For **Level of Security**, choose the encryption and authentication type for the network:

Note The sites, buildings, and floors inherit settings from the Global hierarchy. You can override the level of security at the site, building, or floor level.

- **Enterprise**: You can configure both **WPA2** and **WPA3** security authentication by checking the respective check boxes. By default, the **WPA2** check box is enabled.

  Note Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP).

  WPA3 is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher-grade security protocols for sensitive data networks.

- **Personal**: If you choose **Personal**, enter the passphrase key in the **Pass Phrase** field. This key is used as the pairwise master key (PMK) between clients and the authentication server.

  Note WPA3-Personal brings better protection to individual users by providing more robust password-based authentication making the brute-force dictionary attack much more difficult and time-consuming.

  For WPA2 personal, you can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floors inherit the new settings. For information, see Preshared Key Override, on page 47.

- **Open Secured**: From the **Assign Open SSID** drop-down list, choose an open SSID to redirect the clients to open secured SSID. The open secured policy provides the least security.

  Note Fast Transition is not applicable for open-secured SSID.

  Since open-secured SSID is dependent on open SSID, you must have enabled anchor on open SSID before enabling it on open-secured SSID.

- **Open**: The open policy provides no security. It allows any device to connect to the wireless network without any authentication.

b) For **Authentication, Authorization, and Accounting Configuration**, click **Configure AAA** to add and configure the AAA servers for the enterprise wireless network SSID.

For more information, see Configure AAA Server for an Enterprise Wireless Network.

c) Check one or more following check boxes:

- **Fast Lane**: Check this check box to enable fastlane capabilities on the network.

  Note By enabling fastlane, you can set the IOS devices to receive an optimized level of wireless connectivity and enhanced Quality of Service (QoS).

- **Identity PSK** (for Personal Layer 2 Security): Check this check box to enable unique preshared keys that can be created for individuals or groups of users in the SSID.

- **MAC Filtering**: Check this check box to enable MAC-based access control or security on the wireless network.

  Note When MAC filtering is enabled, only the MAC addresses that you add to the wireless LAN are allowed to join the network.

- **Deny RCM Clients**: Check this check box to deny clients with randomized MAC addresses.

d) Click **Next**.

Step 7 Complete the **Advance Settings** step:

a) For **Fast Transition (802.11r)**:

- Choose **Adaptive**, **Enable**, or **Disable** mode.

  Note 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

- Check the **Over the DS** check box to enable fast transition over a distributed system.

b) For **MFP Client Protection**, choose a setting: **Optional**, **Required**, or **Disabled**.

Note Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between APs and clients. MFP provides both infrastructure and client support.

By default, **Optional** is selected. If you choose **Required**, the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller, and if the client is also configured for WPA2 and supports CCXv5 MFP).

c) For **11K**:

- **Neighbor List**: Check this check box to all the 11k capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

  Note To facilitate roaming, a 11k capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with the Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for next roam from the response frame.

- **Session Timeout**: Check this check box to set the maximum time for a client session to remain active before reauthorization.

  Note By default, the **Session Timeout** is enabled with a timeout of 1800 seconds.

- **Client Exclusion**: Check this check box to set the client exclusion timer.

  Note When a user fails to authenticate, the wireless controller excludes the client from connecting. The client is not allowed to connect to the network until the exclusion timer expires. By default, the **Client Exclusion** is enabled with a timeout of 180 seconds.

d) For **11v BSS Transition Support**:

- **BSS Max Idle Service**: Check this check box to set the idle period timer value. The idle period timer value is transmitted using the association and reassociation response frame from APs to the client.

  Note The BSS Max idle period is the timeframe during which an AP does not disassociate a client due to nonreceipt of frames from the connected client.

- **Client User Idle Timeout**: Check this check box to set the user idle timeout for a WLAN.

Note If the data sent by the client is more than the threshold quota specified within the user idle timeout, the client is considered to be active and the wireless controller refreshes for another timeout period.

By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

- **Directed Multicast Service**: Check this check box to enable directed multicast service.

Note By default, **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer time and saves the battery power.

e) For **Radius Client Profiling**, use this toggle to enable or disable RADIUS profiling on a WLAN.

Note At least one AAA/PSN server is required to enable this feature.

f) Click **Next**.

Step 8 Complete the **Associate SSID to Profile** step:

a) Click a profile from the left pane.

b) If you do not have a profile, click **Add Profile** and then configure the profile settings:

- **Profile Name**: Enter a name for the wireless profile.
- **Fabric**: Specify whether the SSID is fabric or nonfabric.

Note A fabric SSID is a wireless network, which is part of Software Defined-Access (SD-Access). With fabric SSID, it is mandatory to have SD-Access. Nonfabric is a traditional wireless network that does not require SD-Access.

For a nonfabric SSID, choose the following:

- **Interface**: Click the **Interface Management** drop-down list and choose an interface or click the plus icon + to add a new wireless interface.

Note This is the VLAN ID that is associated with the wireless interface.

- **VLAN Group**: Click the **VLAN Group Name** drop-down list and choose a VLAN group, or click the plus icon + to add a VLAN group.

- **Do you need Anchor for this SSID?**: Choose whether the SSID will be an anchor or not.
- **Flex Connect Local Switching**: Check this check box to enable local switching for the WLAN. When you enable local switching, any FlexConnect AP that advertises this WLAN is able to locally switch data packets.

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

c) Click **Associate Profile** to choose the profile.

d) Click **Next**.

Step 9 Review the **Summary** step. If changes are necessary, click **Edit**.

Step 10 To save the SSID settings, click **Save**.

Result: The SSID is created.

Preshared Key Override

SSIDs are created at the Global hierarchy. The sites, buildings, and floors inherit settings from the Global hierarchy. You can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floor inherits the new setting.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 In the left pane, choose the site, building, or floor to edit the PSK.

Step 3 Under **Enterprise Wireless**, click the **Passphrase** field, and enter a new passphrase for the PSK SSID.

Step 4 Click **Save**.

A success message saying `Passphrase for the SSID(s) updated successfully` is displayed.

Hover your cursor over the inherit icon ≡ next to the SSID to view the origin of this setting.

Step 5 To reset the PSK override, check the check box of the PSK SSID on the site, building, or floor and click **Delete**. The PSK is reset to the global passphrase value.

Configure AAA Server for an Enterprise Wireless Network

Before you begin

- Make sure you have defined the AAA server under **System Settings** > **External Services** > **Authentication and Policy Servers** page.
- You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 Ensure that **Global** is selected from the left pane.

Step 4 From the **SSID** table, in the **Action** column, click **Configure AAA** against an SSID for which you want to configure the AAA server.

The **Configure AAA Server** slide-in pane appears.

Step 5 From the **Server** drop-down list, you can either search for a server IP address by entering its name in the **Search** field or choose the AAA IP address.

Note The **Configure AAA** feature is not supported for Mobility Express devices.

Step 6 Click+ to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of enterprise wireless network for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches.

Step 7 From the **Additional Server** drop-down list, choose the server IP address.

Step 8 (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 9 Click **Configure**.

Note Cisco DNA Center allows you to override the set of AAA server configuration for SSID on the site level. For each set of overridden AAA settings per SSID, Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Cisco DNA Center creates the new WLAN profiles equals to the number of floors.

You must reprovision the device to override the AAA servers on the site level. See Provision Devices.

Create SSIDs for a Guest Wireless Network

This procedure explains how to create SSIDs for a guest wireless network.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, ensure that **Global** is selected.

Step 4 From the **SSID** table, hover over ⊕Add ⌄ and choose **Enterprise**.

Result: The **Wireless SSID** workflow appears.

Step 5 Complete the **Basic Settings** step:

a) In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network.

b) For **Wireless Option**, choose the wireless band preference:

- **Dual band operation (2.4 GHz and 5 GHz)**: The WLAN is created for 2.4 GHz and 5 GHz. By default, band select is disabled.
- **Dual band operation with band select**: The WLAN is created for 2.4 GHz and 5 GHz and band select is enabled.
- **5 GHz only**: The WLAN is created for 5 GHz and band select is disabled.
- **2.4 GHz only**: The WLAN is created for 2.4 GHz and band select is disabled.

c) For **Type of Enterprise Network**, choose how the quality of service is provisioned on the wireless network:

- **Voice and Data**: The quality of service is optimized for voice and data traffic.
- **Data Only**: The quality of service is optimized for wireless data traffic only.

d) For **SSID STATE**, customize the following settings:

- **Admin Status**: Use this toggle to enable or disable the admin status.

- **Broadcast SSID**: Use this toggle to enable or disable the visibility of the SSID to all wireless clients within range.

e) Click **Next**.

Step 6 Complete the **Security Settings** step:

a) For **L2 Security**, choose the L2 encryption and authentication type:

- **Enterprise**: You can configure either **WPA2** or **WPA3** security authentication type by checking the respective check boxes. By default, the **WPA2** check box is enabled.

  Note Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Fast transition is applicable for enterprise WPA2 SSID.

  WPA3 security authentication is the latest version of WPA which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher grade security protocols for sensitive data networks.

- **Personal**: You can configure both **WPA2** and **WPA3** or configure **WPA2** and **WPA3** individually by checking the respective check boxes.

  Note WPA3 personal security authentication brings better protection to individual users by providing more robust password-based authentication. This makes the brute-force dictionary attack much more difficult and time-consuming.

  Enter the passphrase key in the **Pass Phrase** field. This key is used as the pairwise master key (PMK) between the clients and the authentication server.

- **Open Secured**: From the **Assign Open SSID** drop-down list, choose an open SSID to associate with the open SSID. Associating secures the open SSID. You must have an open SSID created before associating it with the open secured SSID.

  Note Fast Transition is not applicable for open-secured SSID.

  Since open-secured SSID is dependent on open SSID, you must have enabled anchor on open SSID before enabling it on open-secured SSID.

- **Open**: The open policy provides no security. It allows any device to connect to the wireless network without any authentication.

b) For **L3 Security**, choose the L3 encryption and authentication type:

- **Web Policy**: Provides a higher level of L3 security.

  For **Authentication Server**, configure the authentication server settings:

Authentication Server Type	Description
ISE Authentication	Use Cisco ISE for authentication which provides central web authentication (CWA).

Authentication Server Type	Description
• **Web Authentication Internal** • **Web Authentication External**	Web authentication or Web Auth is a layer 3 security method that allows a client to pass Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) traffic only until they have passed some form of authentication. For web authentication internal, the page is reconstructed by the Cisco Wireless Controller. For web authentication external, the client is redirected to the specified URL. Enter a redirect URL in the **Web Auth Url** field.
• **Web Passthrough Internal** • **Web Passthrough External**	Web passthrough is a solution that is used for guest access and requires no authentication credentials. In web passthrough authentication, wireless users are redirected to the usage policy page while trying to use the Internet for the first time. After accepting the policy, users are allowed to browse the Internet.

- **Open**: There is no security at the L3 level and any device can connect to the SSID.

c) For **Timeout Settings for sleeping clients**, choose the authentication for sleeping clients:

- **Always authenticate**: Enables authentication for sleeping clients.
- **Authenticate after**: Enter the duration for which sleeping clients are to be remembered before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes and the default duration is 720 minutes.

Note The clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login window. You can configure the duration for which the sleeping clients are to be remembered for before reauthentication becomes necessary. The valid range is from 10 minutes to 43200 minutes; the default is 720 minutes. You can configure the duration on a WLAN and on a user group policy that is mapped to the WLAN. The sleeping timer becomes effective after the idle timeout. If the client timeout is less than the time configured on the sleeping timer of the WLAN, then the lifetime of the client is used as the sleeping time.

d) For **Authentication, Authorization, and Accounting Configuration**, click **Configure AAA** to add and configure the AAA servers for the guest wireless network SSID.

For more information, see Configure AAA Server for a Guest Wireless Network.

e) Check one or more following check boxes:

- **Fast Lane**: Check this check box to enable fastlane capabilities on the network.

  Note By enabling fastlane, you can set the IOS devices to receive an optimized level of wireless connectivity and enhanced Quality of Service (QoS).

- **Identity PSK** (for Personal L2 Security): Check this check box to enable unique preshared keys that can be created for individuals or groups of users in the SSID.
- **MAC Filtering**: Check this check box to enable MAC-based access control or security on the wireless network.

  Note When MAC filtering is enabled, only the MAC addresses that you add to the wireless LAN are allowed to join the network.

- **Deny RCM Clients**: Check this check box to deny clients with randomized MAC addresses.

f) Click **Next**.

Step 7 Complete the **Advance Settings** step:

a) For **Fast Transition (802.11r)**:

- Choose **Adaptive**, **Enable**, or **Disable** mode.

  Note 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

- Check the **Over the DS** check box to enable fast transition over a distributed system.

b) For **MFP Client Protection**, choose a setting: **Optional**, **Required**, or **Disabled**.

Note Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between APs and clients. MFP provides both infrastructure and client support.

By default, **Optional** is selected. If you choose **Required**, the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller, and if the client is also configured for WPA2 and supports CCXv5 MFP).

c) For **11K**:

- **Neighbor List**: Check this check box to all the 11k capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

  Note To facilitate roaming, a 11k capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with the Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for next roam from the response frame.

- **Session Timeout**: Check this check box to set the maximum time for a client session to remain active before reauthorization.

  Note By default, the **Session Timeout** is enabled with a timeout of 1800 seconds.

- **Client Exclusion**: Check this check box to set the client exclusion timer.

  Note When a user fails to authenticate, the wireless controller excludes the client from connecting. The client is not allowed to connect to the network until the exclusion timer expires. By default, the **Client Exclusion** is enabled with a timeout of 180 seconds.

d) For **11v BSS Transition Support**:

- **BSS Max Idle Service**: Check this check box to set the idle period timer value. The idle period timer value is transmitted using the association and reassociation response frame from APs to the client.

  Note The BSS Max idle period is the timeframe during which an AP does not disassociate a client due to nonreceipt of frames from the connected client.

- **Client User Idle Timeout**: Check this check box to set the user idle timeout for a WLAN.

Note If the data sent by the client is more than the threshold quota specified within the user idle timeout, the client is considered to be active and the wireless controller refreshes for another timeout period.

By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

- **Directed Multicast Service**: Check this check box to enable directed multicast service.

  Note By default, **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer time and saves the battery power.

e) Click **Next**.

Step 8 Complete the **Associate SSID to Profile** step:

a) Click a profile from the left pane.

b) If you do not have a profile, click **Add Profile** and then configure the profile settings:

- **Profile Name**: Enter a name for the wireless profile.
- **Fabric**: Specify whether the SSID is fabric or nonfabric.

  Note A fabric SSID is a wireless network, which is part of Software Defined-Access (SD-Access). SD-Access is a solution that automates and simplifies configuration, policy, and troubleshooting of wired and wireless networks. With fabric SSID, it is mandatory to have SD-Access. Nonfabric is a traditional wireless network that does not require SD-Access.

  For a nonfabric SSID, choose the following:

  - **Interface**: Click the **Interface Management** drop-down list and choose an interface or click the plus icon ⊕ to add a new wireless interface.

    Note This is the VLAN ID that is associated with the wireless interface.

  - **VLAN Group**: Click the **VLAN Group Name** drop-down list and choose a VLAN group or click the plus icon ⊕ to add a VLAN group.

- **Do you need Anchor for this SSID?**: Choose whether the SSID will be an anchor or not.
- **Flex Connect Local Switching**: Check this check box to enable local switching for the WLAN. When you enable local switching, any FlexConnect AP that advertises this WLAN is able to locally switch data packets.

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

c) Click **Associate Profile** to choose the profile.

d) Click **Next**.

Step 9 Review the **Summary** step. If any changes are necessary, click **Edit**.

Step 10 To save the SSID settings, click **Save**.

Result: The SSID is created.

Configure AAA Server for a Guest Wireless Network

Before you begin

- Make sure you have defined the AAA server under **System Settings** > **External Services** > **Authentication and Policy Servers** page.
- You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 Ensure that **Global** is selected from the left pane.

Step 4 From the **SSID** table, in the **Action** column, click **Configure AAA** of SSID for which you want to configure the AAA server.

The **Configure AAA Server** slide-in pane appears.

Step 5 From the **Server** drop-down list, you can either search for a AAA IP address by entering its name in the **Search** field or choose AAA IP address.

Note

- You must configure at least one Policy Service Node (PSN) server for Central Web Authentication (CWA) SSIDs of guest wireless network.
- Cisco DNA Center allows you to map AAA server in any combination of identity services engine PSNs and third-party AAA IPs.
- In the **Server** drop-down list, the **AAA** IP addresses, and the PSN IP addresses are grouped in the corresponding sections.
- The **Configure AAA** feature is not supported for Mobility Express (ME) devices.

Step 6 Click+ to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of guest wireless network for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches.

Step 7 From the **Additional Server** drop-down list, choose the server IP address.

Step 8 (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 9 Click **Configure**.

Note Cisco DNA Center allows you to override the set of AAA server configuration for SSID on the site level. For each set of overridden AAA settings per SSID, Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Cisco DNA Center creates the new WLAN profiles equals to the number of floors.

You must reprovision the device to override the AAA servers on the site level. See Provision Devices.

Configure 802.1x Authentication Settings for APs

You can configure the authentication settings for the secure onboarding of APs using PnP. Based on the authentication settings configured at the global or site-level hierarchy in Cisco DNA Center, PnP pushes the 802.1x (Dot1x) supplicant and certificates when claiming the AP. The AP authenticates with Cisco ISE using the 802.1x supplicant.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, ensure that **Global** is selected.

Note The 802.1x authentication which is created at the global level can be overridden at the site level.

Step 4 In the **Access Points Authentication for Plug n Play (PnP)** area, complete the following:

a) Choose the authentication method:

- **NO-AUTH**: By default, NO-AUTH is selected.
- **EAP-TLS**: EAP-Transport Level Security (EAP-TLS) is an authentication method designed to mitigate several weaknesses of EAP. EAP-TLS provides many of the benefits as PEAP but differs from it in the lack of support for legacy authentication methods.
- **EAP-PEAP**: Extensible Authentication Protocol-Protected Extensible Authentication Protocol (PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol.

  If you select **EAP-PEAP**, enter the user name and password. A certificate is generated and applied during the PnP claim process.
- **EAP-FAST**: Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is an authentication protocol that provides mutual authentication and uses a shared secret to establish a tunnel. The tunnel is used to protect weak authentication methods that are based on passwords. The shared secret, referred to as a Protected Access Credentials (PAC) key, is used to mutually authenticate the client and server while securing the tunnel.

  If you select **EAP-FAST**, then enter the user name and password. A certificate is generated and applied during the PnP claim process.

b) Enter the **Username** and **Password**.

c) Click **Save**.

Create a Wireless Interface

You can create wireless interfaces only in nonfabric deployments.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 Ensure that **Global** is selected from the left pane.

Step 4 From the **Wireless Interfaces** table, click **+Add**.

Step 5 Configure the wireless interface settings in the **Create a Wireless Interface** slide-in pane:

a) In the **Interface Name** field, enter the dynamic interface name.

b) In the **VLAN ID** field, enter the VLAN ID for the interface.

Step 6 Click **Save**.

Result: The wireless interface is created and appears in the **Wireless Interfaces** table.

Design and Provision Interface/VLAN Groups to Nonfabric Deployments

Cisco DNA Center allows you to configure networks with multiple broadcast domains through different VLANs. When the same set of APs broadcast the same WLAN, the broadcast domains are controlled through multiple VLANs on the same WLAN through interface groups.

Cisco DNA Center interface groups are logical groups of interfaces that facilitate user configuration, where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface can be part of multiple interface groups. A WLAN can be associated with an interface or interface group.

Note The interface group name and the interface name cannot be the same.

The Cisco DNA Center VLAN group feature maps a WLAN to a single VLAN or multiple VLANs using VLAN groups. VLAN groups can be associated to policy profiles.

The following procedure explains how to design and provision the interface or VLAN groups for nonfabric deployments.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 For the **VLAN Group** table, click **Add**.

The **Add VLAN Group** slide-in pane appears.

Step 4 Enter a valid **VLAN Group Name**, select single or multiple interfaces from the list, and click **Save**.

Note If you select more than 15 interfaces, the selected interfaces might not be displayed correctly onscreen.

Step 5 In the **Edit Network Profile** page, the VLAN group is associated with the SSID.

For information on how to create an SSID, see Create SSIDs for an Enterprise Wireless Network.

Step 6 To add more SSIDs to the VLAN group, click **Add SSID**.

Step 7 Choose **Interface** or **VLAN** group.

Step 8 Click the add icon to create a new interface or VLAN group.

Note Interface or VLAN group is not applicable for FlexConnect local switching.

Step 9 Click **Save**.

Step 10 In **Configure Interface and VLAN**, you can view the list of interface names, interface groups names, and other parameters required to configure the interface and VLAN.

Note An interface group cannot contain more than 64 interfaces.

Step 11 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Network Devices** > **Inventory**.

Step 12 Select the device.

Step 13 From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

Step 14 Review the details in the **Assign Site**, **Configuration**, **Model Configuration**, **Advanced Configuration**, and **Summary** screens. From each screen, click **Next** to advance to the next screen.

Step 15 Click **Deploy**.

Result: The **Provision Device** dialog box appears.

Step 16 Choose **Now** and click **Apply**.

Result: The message **Task Scheduled view status in Tasks** appears.

Create a Wireless Radio Frequency Profile

You can either use the default radio frequency profiles (LOW, TYPICAL, HIGH), or create custom radio frequency profiles.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the **Wireless Radio Frequency Profile** table, click **Add**.

Result: The **Wireless Radio Frequency Profile** window appears.

Step 4 In the **Profile Name** field, enter the RF profile name.

Step 5 Click the toggle next to **2.4 GHz** or **5 GHz** to enable or disable the radio band.

Note If you have disabled one of the radios, the base radio of the AP that you are going to configure this AP profile into will be disabled.

Step 6 Configure the following for the **2.4 GHz** radio type:

- Under **Parent Profile**, select **High**, **Medium (Typical)**, **Low**, or **Custom**. (The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates the profile configurations available in the device for 2.4 GHz. If you change any settings in the populated **Data Rate** and **Tx Configuration**, the **Parent Profile** automatically changes to **Custom**.) Note that a new RF profile is created only for the select custom profiles.

  Note Low, Medium (Typical), and High are the default RF profiles. If you select a default RF profile, the respective RF profile on the device is used and the new RF profile is not created on Cisco DNA Center.

- **DCA** dynamically manages channel assignment for an RF group and evaluates the assignments on a per-AP radio basis.

- Check the **Select All** check box to select DCA channels **1**, **6**, and **11**. Alternatively, check the individual check boxes next to the channel numbers.
- Click **Show Advanced** to select the channel numbers under the **Advanced Options**. Check the **Select All** check box to select DCA channels that are under **Advanced Options**, or check the check box next to the individual channel numbers. The channel numbers that are available for B profile are **2**, **3**, **4**, **5**, **7**, **8**, **9**, **10**, **12**, **13**, and **14**.

  Note You must configure these channels globally on Cisco Wireless Controllers.

- Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.
- Under **Tx Power Configuration**, set the power level and power threshold for an AP.
  - **Power Level**: To determine whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 to 30 dBm and the default is -10 dBm.
  - **Power Threshold**: Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm to 80 dBm and the default threshold is -70 dBm.
  - **RX SOP**: Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High**, **Medium**, **Low**, or **Auto** threshold values for each 802.11 band.

Step 7 Configure the following for the **5 GHz** radio type:

- From the **Parent Profile** drop-down list, choose **High**, **Medium (Typical)**, **Low**, or **Custom**. (The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates the configurations available in the device for 2.4 GHz. If you change any settings in the populated **Data Rate** and **Tx Configuration** fields, the **Parent Profile** automatically changes to **Custom**.) Note that a new RF profile is created only for select custom profiles.

  Note **Low**, **Medium (Typical)**, and **High** are the default RF profiles. If you select a default RF profile, the respective RF profile that is already present in the device is used and the new RF profile is not created on Cisco DNA Center.

- From the **Channel Width** drop-down list, choose one of the channel bandwidth options: **Best**, **20 MHz**, **40 MHz**, **80 MHz**, or **160 MHz**.
- Set the **DCA Channel** to manage channel assignments:

  Note You must configure the channels globally on Cisco Wireless Controllers.

  - **UNNI-1 36-48**: The channels available for UNII-1 band are **36**, **40**, **44**, and **48**. Check the **UNII-1 36-48** check box to include all channels, or check an individual check box.
  - **UNII-2 52-144**: The channels available for UNII-2 band are **52**, **56**, **60**, **64**, **100**, **104**, **108**, **112**, **116**, **120**, **124**, **128**, **132**, **136**, **140**, and **144**. Check the **UNII-2 52-144** check box to include all channels, or check an individual check box.

    - **UNII-3 149-165**: The channels available for UNII-3 band are **149**, **153**, **157**, **161**, and **165**. Check the **UNII-3 149-165** check box to include all channels, or check an individual check box.

- Use the **Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.
- Under **Tx Power Configuration**, set the power level and power threshold for an AP.
    - **Power Level**: Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 to 30 dBm and the default is -10 dBm.
    - **Power Threshold**: Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm to 80 dBm and the default threshold is -70 dBm.
    - **RX SOP**: Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an AP's radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High**, **Medium**, **Low**, or **Auto** threshold values for each 802.11 band.

Step 8 Click **Save**.

Step 9 To mark a profile as the default RF profile, check the **Profile Name** check box and click **Mark Default**.

Step 10 In the **Warning** window, click **OK**.

Provision a Cisco Sensor SSID for Nonfabric Deployment

- The Cisco DNA Center sensor uses the Cisco sensor provisioning Service Set Identifier (SSID) to communicate with the Plug and Play (PnP) server and obtain day-0 configurations for running tests.

Note The Cisco sensor provisioning SSID is not applicable for APs working as sensors.

- For fabric deployments, the Cisco sensor provisioning SSID is mapped to an Infrastructure Virtual Network Access Point (INFRA VN–AP) pool to communicate with Cisco DNA Center.
- The following platforms support the Cisco sensor provisioning SSID:
    - Cisco AireOS Controller
    - Cisco Catalyst 9800 Series Wireless Controller (both fabric and nonfabric deployments)
- The Cisco sensor provisioning SSID supports the following network controllers:
    - Cisco Catalyst 9800 Wireless Controllers for Cloud
    - Cisco Catalyst 9800 Series Wireless Controller
    - Cisco AireOS Controller

The following procedure enables you to configure the Cisco sensor provisioning SSID for nonfabric deployments.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the **SSID** table, hover over ⊕Add ∨ and choose **Enterprise**.

Result: The **Wireless SSID** workflow appears.

Step 4 Toggle the **Sensor** field and click **Next**.

Note The parameters for the SSID are automatically populated and cannot be edited.

Step 5 Click **Next**.

Step 6 In the **Wireless Profiles** screen, check a profile from the **Profiles** table.

Result: The **Edit Wireless Profile** dialog box appears.

Step 7 In Fabric, select **Yes** and click **Save**.

Result: The **Success Profile sensorProfile selected** message appears.

Step 8 Click **Finish**.

Step 9 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Network Devices** > **Inventory**.

Step 10 Check a device and from the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

Step 11 Review the details under **Assign Site**, **Configuration**, **Model Configuration**, **Advanced Configuration**, and **Summary**. Click **Next** after each screen.

Step 12 Click **Deploy**.

Result: The **Provision Device** dialog box is displayed.

Step 13 Choose **Now** and click **Apply**.

Result: The message **Task Scheduled view status in Tasks** appears at the bottom-right corner.

Manage Backhaul Settings

Use this procedure to view, create, and manage backhaul configurations for wireless sensors. A wireless sensor requires a backhaul SSID to communicate with Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Assurance** > **Manage** > **Sensors**.

Result: The **Sensor List** window appears.

Step 2 Hover your cursor over the **Settings** tab and choose **Backhaul Settings**.

Step 3 You can add and manage backhaul SSIDs by doing the following:

a) Click **+ Add Backhaul**.

The **Create Sensor Backhaul SSID Assignment** window appears with two areas: **Wired Backhaul** and **Wireless Backhaul**.

b) In the **Settings Name** field, enter a name for the backhaul SSID.

c) In the **Wired Backhaul** area, configure the following:

- **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:
    - **802.1x EAP**: Standard used for passing Extensible Authentication Protocol (EAP) over wired LAN.
    - **Open**: No security or authentication is used.
- **EAP Method**: If you choose **802.1x EAP**, you must choose one of the following EAP methods for user authentication from the drop-down list:
    - **EAP-FAST**: Enter the username and password in the fields provided.
    - **PEAP-MSCHAPv2**: Enter the username and password in the fields provided.
    - **EAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

      If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.
    - **PEAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

      If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.

d) In the **Wireless Network Name (SSID)** area, select the wireless network (SSID) and configure the following.

- **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:
    - **WPA2 Enterprise**: Provides a higher level of security using Extensible Authentication Protocol (EAP) (802.1x) to authenticate and authorize network users with a remote RADIUS server.
    - **WPA2-Personal**: Provides a good security using a passphrase or a preshared key (PSK). This allows anyone with the passkey to access the wireless network.

      If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.
    - **PSK Format**:The available preshared key formats are:
        - **ASCII**: Supports ASCII PSK passphrase.
        - **HEX**: Supports 64-character HEX key PSK password.
    - **Open**: No security or authentication is used.

e) Click **Save**.

Step 4 You can edit the existing backhaul configurations by doing the following:

a) Check the check box of the backhaul configuration.

b) Hover your cursor over the **Actions** drop-down list and choose **Edit**.

Step 5 You can delete a backhaul configuration by doing the following:

a) Check the check box of the backhaul configuration.
b) Hover your cursor over the **Actions** drop-down list and choose **Delete**.

About Cisco Connected Mobile Experiences Integration

Cisco DNA Center supports the integration of Connected Mobile Experiences (CMX) for wireless maps. With the CMX integration, you can get the exact location of your wireless clients, rogue access points and interferers on the floor map within the Cisco DNA Center user interface.

Depending on your requirements, you can create CMX settings either at the global level or at the site, building, or floor level. For a small enterprise, you can assign CMX at the global level, which is the parent node. All children inherit their settings from the parent node. For a medium enterprise, you can assign CMX at the building level and for a small enterprise, you can assign CMX at the floor level.

Note CMX should be anonymized for security purposes.

Create Cisco CMX Settings

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System** > **Settings**.

Step 2 From the **External Services** section, click **DNA Spaces/CMX Servers**.

Result: The **DNA Spaces/CMX Servers** window appears.

Step 3 From the **CMX Servers** table, click **Add**.

Step 4 Complete the fields in the **Add CMX Server** slide-in pane:

- **IP Address**: Enter the valid IP address of the CMX web GUI.
- **User Name**: Enter the CMX web GUI username.
- **Password**: Enter the password credentials.
- **SSH User Name**: Enter the CMX admin username.
- **SSH Password**: Enter the CMX admin password credentials.

Note Make sure that CMX is reachable.

Step 5 Click **Add**.

Result: The CMX server is added successfully.

Step 6 To assign a CMX server to a site, building, or a floor, click the **Menu** icon and choose **Design** > **Network Settings**.

Step 7 Click the **Wireless** tab.

Step 8 In the left tree view menu, select either Global or the area, building, or floor that you are interested in.

Step 9 In the **DNA Spaces/CMX Servers** section, use the drop-down list, choose the CMX server.

Step 10 Click **Save**.

Result: The **Create CMX Settings** page appears.

After the CMX is added, if you make any changes to the floor on the **Network Hierarchy** page, the changes are synchronized automatically with the CMX.

When the CMX is synced, Cisco DNA Center starts querying the CMX for the client location and displays the location on the floor map.

Step 11 From the floor map, you can do the following:

- View the location of the client, which is shown as a blue dot.
- Hover your cursor over an AP. A dialog box is displayed with **Info**, **Rx Neighbor**, and **Clients** tabs. Click each tab for more information. Click **Device 360** to open the Device 360 window and view issues. Click an issue to see the location of the issue and the location of the client device.
- Click an AP to open a side bar with details about the AP.
- Perform real-time client tracking when Intelligent Capture and CMX are integrated.

Step 12 If the CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** page, hover your cursor over the ellipsis ••• next to the building or floor on which you made the changes in the left tree pane, and then choose **Sync: DNA Spaces/CMX** to push the changes manually.

Step 13 To edit the CMX server details or delete a CMX server, do the following:

a) In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System** > **Settings**.
b) From the **External Services** section, click **DNA Spaces/CMX Servers**.
c) Select the CMX server that you want to edit, make any changes, and click **Update**.
d) Select the CMX server that you want to delete and click **Delete**.
e) Click **OK** to confirm the deletion.

For CMX Authentication Failure

- Check if you are able to log in to the CMX web GUI with the credentials that you provided at the time of CMX settings creation on Cisco DNA Center.
- Check if you are able to log in to the CMX console using SSH.
- Check if you are able to exercise CMX REST APIs using the API Documentation link on the CMX GUI.

If Clients Do Not Appear on the Cisco DNA Center Floor Map

- Check if the Cisco wireless controller on the particular floor is configured with CMX and is active.
- Check if the CMX GUI shows clients on the floor map.
- Use the Cisco DNA Center Maps API to list the clients on the floor: `curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor group id>/clients?associated=true`

About Cisco DNA Spaces Integration

Enterprises operating in the physical world have limited to no visibility into the behavior of people and connected assets within their buildings. Cisco DNA Spaces solves this physical blind-spot problem using location-sensing intelligence from all underlying Cisco wireless networks and translating the data into business-ready insights.

Cisco DNA Center supports the integration of Cisco DNA Spaces. With the Cisco DNA Spaces integration, you can get the exact location of your wireless clients, rogue APs, and interferers on the floor map in the Cisco DNA Center GUI. Depending on your requirements, you can create Cisco DNA Spaces settings either at the global level or at the site, building, or floor level.

Note The Cisco DNA Center and Cisco DNA Spaces integration is currently limited to only automatic map exports and synchronization for the location hierarchy. The integration does not support captive portal-based authentication features.

Integrate Cisco DNA Spaces with Cisco DNA Center

Use this procedure to integrate Cisco DNA Spaces with Cisco DNA Center.

Step 1 Onboard the Cisco DNA Spaces client:

a) Log in to Cisco DNA Spaces using your email ID, and click **Continue**.

The **Select Customer** dialog box is displayed.

b) From the **Select Customer** drop-down list, choose the Spaces tenant for the Cisco DNA Center instance (for example, dna-center-dev-US), and then click **Proceed**.

c) In the Cisco DNA Spaces GUI, click the **Menu** icon and choose **Setup** > **Wireless Networks**.

The **Connect your wireless network** window is displayed.

d) In the **Connect your wireless network** window, complete Steps 1 to 3 as documented in the *Cisco DNS Configuration Guide* to onboard the Cisco DNA Spaces client.

You can access the *Cisco DNS Configuration Guide* from the right pane under **Need Help?**. Choose **View Configuration Steps**.

Step 2 Register Cisco DNA Center with Cisco DNA Spaces:

a) Log in to Cisco DNA Spaces using your email ID, and click **Continue**.

Result: The **Select Customer** dialog box appears.

b) From the **Select Customer** drop-down list, choose the Spaces tenant for the Cisco DNA Center instance (for example, dna-center-dev-US), and then click **Proceed**.

c) In the Cisco DNA Spaces GUI, click the **Menu** icon and choose **Integrations** > **DNA Center**.

Result: The **DNAC Integration** window appears.

d) In the **DNAC Integration** window, click **Create Token**.

Result: The **Create new token** dialog box appears.

e) In the **Instance Name** field, enter a unique name for the instance, and then click **Create Token**.

Result: A new token for the instance opens.

f) Scroll to the right of the token and choose **Copy Token**.

g) To paste the token in to the Cisco DNA Center GUI, log in to Cisco DNA Center.

h) In the Cisco DNA Center GUI, click the **Menu** icon and choose **System** > **Settings**.

i) In the left navigation pane, scroll down and choose **DNA Spaces/CMX Servers**.

Result: The **DNA Spaces/CMX Servers** window appears.

j) From the **DNA Spaces** area, choose **Activate**.

Result: The **Integrate DNA Spaces** dialog box appears.

k) In the **Tenant Token** text box, press **Ctrl V** to paste the token that you copied from Cisco DNA Spaces, then click **Connect**.

Result: The **Success** dialog box is displayed with the following information:

```
This cluster is integrated with Cisco DNA Spaces successfully.
```

The DNA Spaces/CMX Servers window displays a green ✓ **Activated** status, and the tenant that you selected in Cisco DNA Spaces (for example, dna-center-dev-US) is displayed in the **Tenant** field.

Step 3 Assign Cisco DNA Spaces to sites in Cisco DNA Center:

a) In the Cisco DNA Center GUI, click the **Menu** icon ≡ and choose **Design** > **Network Settings**.

b) Click the **Wireless** tab.

c) In the left tree view menu, select either **Global** or the area, building, or floor to which you want to assign Cisco DNA Spaces.

d) From the **DNA Spaces/CMX Servers** section, use the drop-down list to select a site (for example, DNA Spaces - dna-center-dev-US).

e) Click **Save**.

Step 4 Monitor sites in Cisco DNA Center using Cisco DNA Spaces:

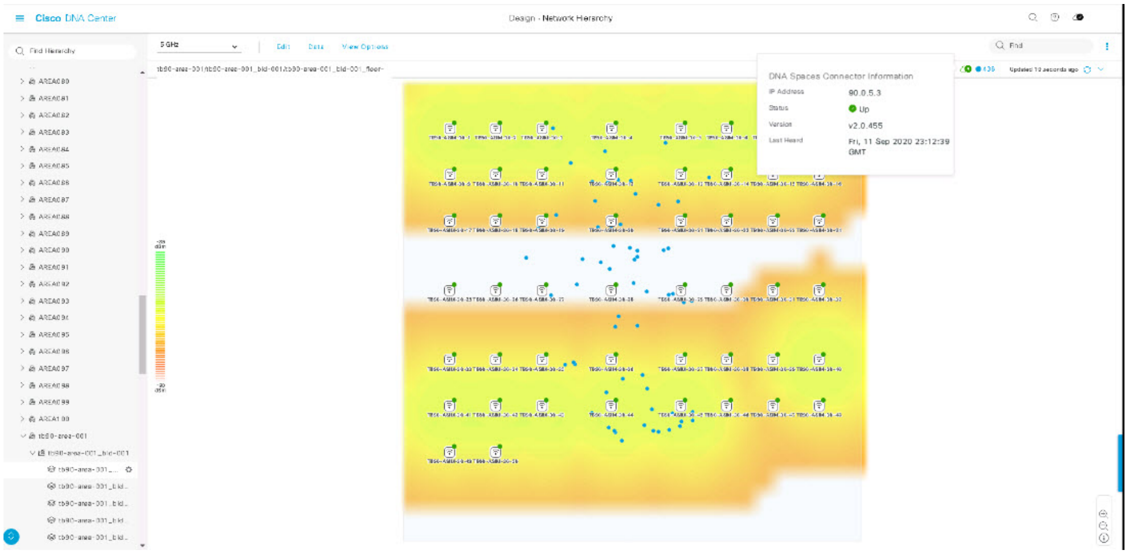
a) In the Cisco DNA Center GUI, click the **Menu** icon ≡ and choose **Design** > **Network Hierarchy**.

b) In the left tree view menu, select either **Global** or the area, building, or floor that you want Cisco DNA Spaces to monitor.

Cisco DNA Center deploys the site information to Cisco DNA Spaces automatically.

c) To confirm that the Cisco DNA Spaces is operational, verify that the Cisco DNA Spaces/CMX status icon displays on the floor that you want to monitor, as shown in the following figure.

Figure 15: Cisco DNA Spaces Status Icon



DNA Spaces Connector Information

IP Address 90.0.5.3

Status Up

Version v2.0.455

Last Heard Fri, 11 Sep 2020 23:12:39 GMT

Configure a FlexConnect VLAN

You can configure the following FlexConnect VLAN settings:

- **Native VLAN**: Allows a FlexConnect group to carry the management traffic between APs and Cisco Wireless Controllers.
- **AAA Override VLAN**: Provides dynamic VLAN assignment of locally switched clients.

You can apply these settings at the global level and override them at the site, building, or floor level.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, choose the appropriate scope:

- **Global**: Configures the VLAN at the global level for all sites.
- **Site**, **Building**, or **Floor**: Configures the VLAN at the chosen level only.

Step 4 In the **Native VLAN ID** field, enter a value for the VLAN ID. The valid range is from 1 to 4094.

Step 5 For **AAA Override VLAN**, enter a VLAN ID and VLAN name mapping in the corresponding **VLAN ID** and **VLAN Name** fields. To add more mappings, click the Add icon.

Note The maximum VLAN mappings that you can define for a FlexConnect deployment is 16. However, for Cisco Catalyst 9800 Wireless Controllers, this number includes default WLAN VLANs and VLANs pushed by AAA.

Step 6 Click **Save**.

Step 7 Create a wireless network profile *or* configure an SSID:

- **Wireless Network Profile**: If you decide to create a wireless network profile, make sure that the **FlexConnect Local Switching** check box is checked. For more information, see Create Network Profiles for Wireless, on page 75.
- **SSID**: For information, see Create SSIDs for an Enterprise Wireless Network, on page 43 and Create SSIDs for a Guest Wireless Network, on page 48.

Step 8 For the saved FlexConnect VLAN settings to get configured on the wireless controller, you must provision the wireless controller on the **Provision** window.

For more information, see Provision a Cisco AireOS Controller or Configure and Provision a Cisco Catalyst 9800 Series Wireless Controller.

Step 9 After provisioning the wireless controller, you must provision the AP that is associated with the controller. To override the FlexConnect VLAN settings at the site, building, or floor level, in the left tree view menu, choose a site, building, or floor.

About Wireless Mesh Networks

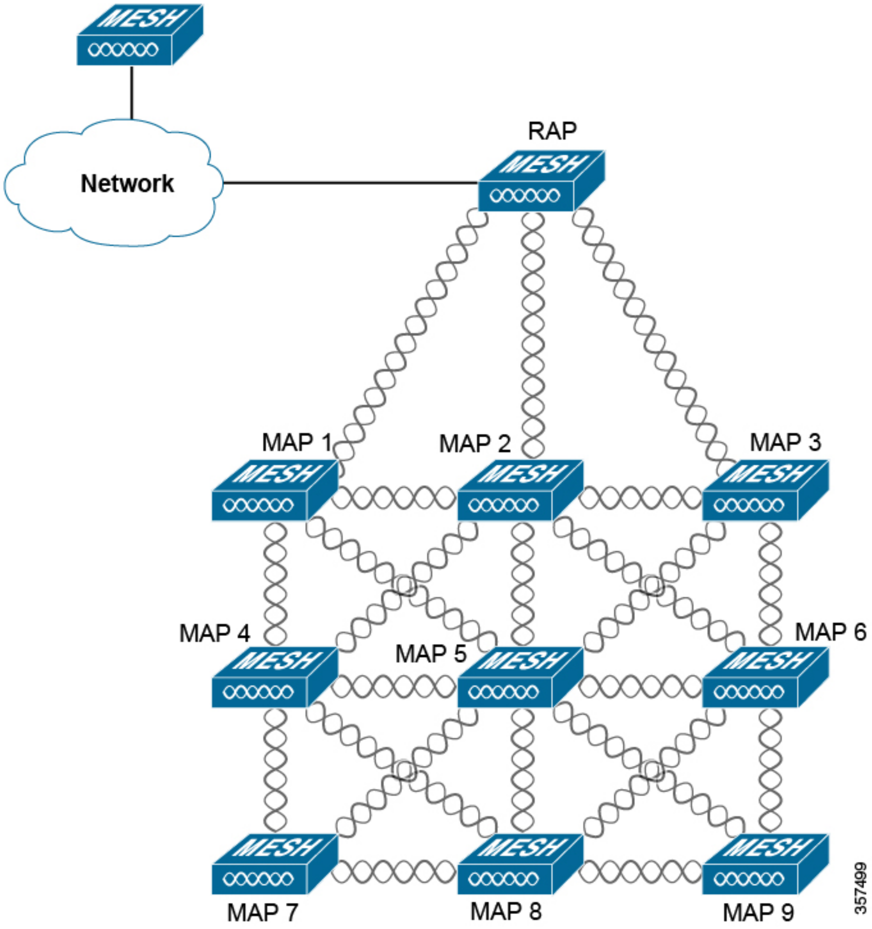
In a Cisco wireless mesh network, multiple mesh access points comprise a network that provides secure, scalable wireless LAN.

Access points within a mesh network operate in one of the following two ways:

- Root access point (RAP)
- Mesh access point (MAP)

Note All access points are configured and shipped as mesh access points. To use an access point as a root access point, you need to reconfigure the mesh access point as a root access point. In all mesh networks, make sure that there is at least one root access point.

RAPs are connected to the wired network at each location. All the downstream access points operate as MAPs and communicate using wireless links.



Both MAPs and RAPs can provide WLAN client access; however, typically the location of RAPs is often not suitable for providing client access.

Some buildings have onsite controllers to terminate CAPWAP sessions from the mesh access points but it is not a mandatory requirement because CAPWAP sessions can be back hauled to a controller over a wide-area network (WAN).

In a Cisco wireless backhaul network, traffic can be bridged between MAPs and RAPs. This traffic can be from wired devices that are being bridged by the wireless mesh or CAPWAP traffic from the mesh access points. This traffic is always AES encrypted when it crosses a wireless mesh link such as a wireless backhaul.

For more information about Mesh Networks, see the latest Cisco Wireless Mesh Access Points, Design and Deployment Guide.

AP Configuration

If you have existing APs that you want to use in mesh network mode, you first need to change the AP Mode to Bridge or Flex+Bridge using the **Configure Access Point** workflow. For information, see Configure AP Workflow.

After an AP is configured for Bridge or Flex+Bridge mode, the **AP 360** page shows the mesh configuration. At this point, you need to provision the APs with the new configuration. Provision a Cisco AP—Day 1 AP Provisioning.

WLC Configuration

For mesh networks, you need to configure a list of authorized access points on the controllers. A controllers responds only to requests from MAPs that are present in its authorization list.

Note Cisco DNA Center supports the configuration of authorization lists on Cisco Catalyst 9800 Wireless Controllers running Cisco IOS Release 17.5 and higher.

On both AireOS and Catalyst 9800 Wireless Controllers, you can use Cisco DNA Center to configure the Bridge Group Name (BGN) and RAP downlink backhaul mesh settings. On Catalyst 9800 Wireless Controllers, you can also configure the maximum range of the MAPs, backhaul client access, and backhaul data rates.

These settings are configured at the floor level on the Wireless Network Settings page. For information, see Configure Mesh Settings on WLCs, on page 68 .

Configure Mesh Settings on WLCs

You can configure mesh settings on AireOS and Catalyst 9800 Wireless Controllers.

Note Range, Backhaul Client Access, and Backhaul Data Rates cannot be applied on AireOS Controllers through Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 In the left pane, choose a floor.

Note Mesh settings are configured per floor only.

Step 4 Under **Authorized Access Points**, click **Manage Authorized Access Points**.

Step 5 In the **Manage Authorized Access Points** pane, enter the MAC addresses of Mesh APs (MAPs) that are allowed to join the controller. The controller responds only to those CAPWAP requests from MAPs that are in its authorization list.

Enter the MAC addresses in one of the following ways:

- **Upload a CSV File**: Download the CSV template file and add your MAC addresses 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.
- **Manually Add MAC Addresses**: If you have only a couple of MAC addresses to configure, click **Add** and in the field that appears under **MAC Address**, enter the MAC address. To add more MAC addresses, click **Add**.

Step 6 Click **Save**.

Step 7 Under **Mesh Settings**, configure the following parameters:

- **Bridge Group Name**: Controls the association of mesh access points. A Bridge Group Name (BGN) can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one Root Access Point (RAP) in your network in the same sector (area). BGN is a string of 10 characters maximum.

A BGN of *NULL VALUE* is assigned by default. Although not visible to you, it allows MAPs to join the network before you assign a network-specific BGN.

- **Range (in Ft)**: Maximum range (in feet) of all MAPs in the network.
- **Backhaul Client Access**: Allows wireless client association over the backhaul radio. Generally, the backhaul radio is a 5-GHz radio for most of the MAPs. This means that a backhaul radio can carry both backhaul traffic and client traffic.

  When **Backhaul Client Access** is disabled, only backhaul traffic is sent over the backhaul radio, and client association is only over the secondary radio(s).
- **RAP Downlink Backhaul**:
- **Backhaul Data Rates**: Backhaul is used to create a wireless connection between the access points. Valid backhaul interface rates are **802.11abg**, **802.11n**, **802.11ac**, **802.11ax**, and **Auto**, depending on the access point. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices.

  With the **Auto** data rate, the access point picks the highest rate where the next higher rate cannot be used because of conditions not being suitable for that rate and not because of conditions that affect all rates. That is, once configured, each link is free to settle down to the best possible rate for its link quality.

  We recommend that you configure the mesh backhaul data rate to **Auto**.

Step 8 Click **Save**.

Create Network Profiles

In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Profiles**, and click **Add Profile** to create network profiles for:

- Routing and NFV
- Firewall
- Switching
- Wireless

Create Network Profiles for NFVIS

This workflow shows how to:

1. Configure the router WAN.
2. Configure the ENCS integrated switch.

Note This option is available only on ENCS 5400 devices.

3. Create custom configurations.
4. View the profile summary.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Profiles**.

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

Step 3 The **Router WAN Configuration** window appears.

- Enter the profile name in the **Name** text box.
- Select the number of **Service Providers** and **Devices** from the drop-down list. Up to three service providers and two devices are supported per profile.
- Select the **Service Provider Profile** from the drop-down list. For more information, see Configure Service Provider Profiles, on page 95.
- Select the **Device Type** from the drop-down list.
- Enter a unique string in the **Device Tag** to identify the different devices, or select an existing tag from the drop-down list. Select the appropriate tag, because your selection is used as part of the matching criteria for Day-0 and Day-N templates applied to the network profile.
- To enable at least one line link for each device to proceed, click **O** and check the check box next to **Connect**. Select the **Line Type** from the drop-down list. Click **OK**.
- Click **+Add Services** to add services to the profile. The **Add Services** window appears. Click on a **Router**, **Firewall**, or **Application** icon and drag it onto the diagram. Based on your selection, the default network connections are automatically created. You can also select **Custom- Net** to add custom services or networks to the profile.

  To configure the router, click on the router and select **Configuration**. Select the **Type**, **Image** and **Profile** from the drop-down list. For more information, see Import a Software Image. Set the **vNIC Mapping** fields as required.

  To configure the firewall, click on the firewall and select **Configuration**. Select the **Type**, **Image** and **Profile** from the drop-down list. The drop-down list for **Type** is populated based on the firewall plugins installed on the system. Set the **vNIC Mapping** fields as required.

  To configure the application, click on the application and select **Configuration**. Select the **Type**, **Image** and **Profile** from the drop-down list. The drop-down list for **Type** is populated based on the application plugins installed on the system. Set the **vNIC Mapping** fields as required.

  To configure custom networks, click on custom-net interface. Select **Connect from** and click on the node you want to add the custom network to and select **Connect to**. Click on custom-net and select **Add Configuration**. Select the **Network Mode** and enter the VLAN ID in **VLAN**.

  Click **Save**.
- Click **Next**.

Step 4 If you have selected an ENCS device, the **ENCS Integrated Switch Configuration** page appears.

- Click **+Add Row**. Select **Type** from the drop-down list and enter the **VLAN ID/Allowed VLAN** and the **Description**.
- Click **Next**.

Step 5 The **Custom Configuration** page appears.

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

If you choose to add the custom configurations:

- Select the **Onboarding Template(s)** or **Day-N Templates** tab, as required.
- Select the Template from the drop-down list. The templates are filtered by the **Device Type** and **Tag Name**.
- Click **Next**.

Step 6 The **Summary** page appears.

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

- Click **Save**.

Step 7 The **Network Profiles** page appears.

Click **Assign Sites** to assign a site to the network profile. For more information, see Create a Site in a Network Hierarchy, on page 2.

Create Network Profiles for Routing

This workflow shows how to:

1. Configure the router WAN.
2. Configure the router LAN.
3. Configure the integrated switch configuration.
4. Create custom configurations.
5. View the profile summary.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Profiles**.

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

Step 3 The **Router WAN Configuration** window appears.

- Enter the profile name in the **Name** text box.
- Select the number of **Service Providers** and **Devices** from the drop-down list. Up to three service providers and ten devices are supported per profile.
- Select the **Service Provider Profile** from the drop-down list. For more information, see Configure Service Provider Profiles, on page 95.
- Select the **Device Type** from the drop-down list.
- Enter a unique string in the **Device Tag** to identify the different devices, or select an existing tag from the drop-down list. Use the device tag if two or more devices are of the same type. If all the devices are of a different type, the

device tag is optional. Select the appropriate tag, because your selection is used as part of the matching criteria for Day-0 and Day-N templates applied to the network profile.

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

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

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

- Click **Next**.

Step 4 The **Router LAN Configuration** page appears.

- Click the **Configure Connection** radio button and choose L2, L3, or both.
- If you choose **L2**, select the **Type** from the drop-down list and enter the **VLAN ID/Allowed VLAN** and the **Description**.
- If you choose **L3**, select the **Protocol Routing** from the drop-down list and enter the **Protocol Qualifier**.

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

- Click **Next**.

Step 5 The **Integrated Switch Configuration** page appears.

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

- To add one or more new VLANs, click **+**.
- To delete a VLAN, click **x**.
- Click **Next**.

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

Step 6 The **Custom Configuration** page appears.

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

If you choose to add custom configurations:

- Click the **Onboarding Template(s)** or **Day-N Templates** tab, as required.
- Choose a template from the drop-down list. The templates are filtered by **Device Type** and **Tag Name**.
- Click **Next**.

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

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

Step 8 The **Network Profiles** page appears.

Click **Assign Sites** to assign a site to the network profile. For more information, see Create a Site in a Network Hierarchy, on page 2.

Create Network Profiles for Firewall

This workflow shows how to:

1. Create custom configurations.
2. Create Firepower Threat Defense (FTD) configurations.
3. View the profile summary.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Profiles**.

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

The **Firewall Type** page appears.

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

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

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

Note You can choose up to 10 devices per profile.

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

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

e) Click **Next**.

The **Custom Configuration** page appears.

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

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

g) Click **Next**.

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

h) Click **Save**.

The **Network Profiles** page appears.

i) To assign a site to the network profile, click **Assign Sites**. For more information, see Create a Site in a Network Hierarchy, on page 2.

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

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

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

   Note You can choose up to 10 devices per profile.

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

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

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

f) Click **Next**.

   The **FTD Configuration** page appears.

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

h) Click **Next**.

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

i) Click **Save**.

   The **Network Profiles** page appears.

j) To assign a site to the network profile, click **Assign Sites**. For information, see Create a Site in a Network Hierarchy, on page 2.

Create Network Profiles for Switching

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

- Onboarding template
- Day N template

Before you begin

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

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Profiles**.

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

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

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

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

- Select the **Device Type** from the drop-down list.
- Select a **Template** from the drop-down list. You can select the Onboarding Configuration template that you have already created.

Step 4 Click **Save**.

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

Create Network Profiles for Wireless

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Profiles**.

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

Before assigning a wireless network profile, make sure that you have created wireless SSIDs under **Design** > **Network Settings** > **Wireless** tab.

Step 3 In the **Add a Network Profile** window, enter a valid profile name in the **Profile Name** text box.

Step 4 Click **+ Add SSID**.

The SSIDs that were created are populated.

Step 5 From the **SSID** drop-down list, choose the SSID.

The SSID type is displayed.

Step 6 Specify whether the SSID is fabric or nonfabric by selecting **Yes** or **No**.

Step 7 If you are creating a nonfabric SSID, select **No**, and configure the following parameters.

Step 8 From the **Interface Name** drop-down list, choose an interface name for the SSID, or click **+ create a new wireless interface** to create a new wireless interface.

Step 9 In the **Do you need Anchor for this SSID?** area, click **Yes** to add an anchor to SSID.

Note: **No** is chosen by default.

Step 10 Check the **Flex Connect Local Switching** check box to enable local switching for the WLAN.

If you have chosen to add anchor to SSID, you cannot enable **Flex Connect Local Switching**.

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

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

Step 11 The VLAN ID that is associated with the wireless interface is autopopulated based on the interface name selected.

If you want to change the VLAN ID, in the **Local to VLAN** text box, enter a new value for the VLAN ID.

Step 12 Click **+ Add Model Config** to add model config designs to a network profile.

The **Add Model Config** window appears.

Step 13 From the **Device Type(s)** drop-down list, select the device type.

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

Step 14 Expand **Wireless** and select the model config design that you are attaching to this wireless profile.

Step 15 From the **Tags** drop-down list under **APPLICABILITY**, select the applicable tags.

Step 16 Click **Add**.

The attached model config appears under the **Attach Model Config** area in the **Add a Network Profile** window.

Step 17 To associate a template with the network profile, click **Add** under the **Attach Template(s)** area.

Step 18 From the **Device Type(s)** drop-down list, choose the device type.

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

Step 19 You can choose the device tag and template from the **Device Tag** and **Template** drop-down lists.

You can use tags on templates only when you have to push different templates for the same device type based on the device tag.

Step 20 Click **Add**.

The created profile appears in the **Wireless Profiles** window.

Step 21 Click **Save** to add a network profile.

The newly added network profile appears on the **Design** > **Network Profiles** page.

Step 22 To assign this profile to a site, click **Assign Sites**.

Step 23 In the **Add Sites to Profile** window, check the check box next to the site to associate to this profile.

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

Step 24 Click **Save**.

Preprovision the AP Group, Flex Group, and Site Tag in a Network Profile

Cisco DNA Center allows you to preprovision the AP group, flex group, and site tag in a network profile. Preprovisioning saves time during AP provisioning by eliminating the need to make repetitive configuration changes and ensures consistency across your devices.

- AP group configuration is applicable to Wireless LAN controllers running an AireOS image.
- Flex group configuration is applicable to Wireless LAN controllers running an AireOS image.
- Site tag configuration is applicable to Catalyst 9800 series wireless controllers.

Before you begin

You must create a network profile and assign a site (floor) to the network profile to enable AP group, flex group, and site tag creation.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Profiles**.

Step 2 Click **Edit**.

Step 3 Click **Show Advanced Settings**.

Step 4 To create an AP group in the network profile, expand **AP Group** and click **+ Create an AP Group**.

The **Create an AP Group** window appears.

Step 5 In the **AP Group Name** field, enter the AP group name.

Step 6 From the **RF Profile** drop-down list, choose the RF profile.

The options are **High**, **Typical**, **Low**, **custom_rf_profile2**, and **rf_prof1_custom**.

Step 7 In the **Select Sites** field, you can either search for a site by entering its name or expand **Global** to select the site.

Step 8 (Optional) Click **Save & Add another** to add another AP group.

Step 9 Click **Save**.

The AP group is created based on the selected RF profile under the **AP Group** area in the **Edit Network Profile** window.

Step 10 To enable the flex group in the network profile, check the **Flex Connect Local Switching** check box and define the VLAN ID in the **Local to VLAN** text box to mark the nonfabric SSID as a flex-based SSID.

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

The **Flex Group** option is enabled under **View Advanced Settings**.

Step 11 To create a flex group in the network profile, expand **Flex Group** and click **+ Create Flex Group**.

The **Create Flex Group** window appears.

Step 12 In the **Flex Group** field, enter the flex group name.

Step 13 In the **Select Sites** field, you can either search for a site by entering its name or expand **Global** to select the site.

Step 14 (Optional) Click **Save & Add another** to add another flex group.

Step 15 Click **Save**.

The flex group is created under the **Flex Group** area in the **Edit Network Profile** window.

Step 16 To create a site tag in the network profile, expand **Site Tag** and click **+ Create a Site Tag**.

The **Create a Site Tag** window appears.

Step 17 In the **Site Tag** field, enter the site tag name.

Step 18 In the **Flex Profile Name** name field, enter the flex profile name.

Note To enable the **Flex Profile Name** name field, check the **Flex Connect Local Switching** check box in the **Edit Network Profile** window.

Step 19 In the **Select Sites** field, you can either search for a site by entering its name or expand **Global** to select the site.

Step 20 (Optional) Click **Save & Add another** to add another site tag.

Step 21 Click **Save**.

The site tag is created under the **Site Tag** area in the **Edit Network Profile** window.

Create Network Profile for Cisco DNA Traffic Telemetry Appliance

Before you begin

Define the template that you want to apply to the telemetry appliances. See Create Templates to Automate Device Configuration Changes.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Profiles**.

Step 2 Click **+Add Profile** and choose **Telemetry Appliance**.

Step 3 In the **Telemetry Appliance Type** window, complete the following:

a) Enter the profile name in the **Name** text box.

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

c) From the **Device Tag** drop-down list, choose an existing device tag defined in Cisco DNA Center or enter a new tag. This step is optional. If the tag that you selected has already been associated with a template, only that template is available in the Template drop-down list.

d) Click **Next**.

Step 4 In the **Custom Configuration** window, choose the template. The chosen template will be applied to the device once it is managed in Cisco DNA Center inventory.

Step 5 Click **Next**.

Step 6 In the **Summary** window, click **Save.**

Manage Global Network Settings

You can create network settings that become the default for your entire network. There are two primary areas from which you can define the settings within your network:

- **Global settings**: Settings defined here affect your entire network and include settings for servers such as DHCP, DNS, AAA, NTP, and so on; IP address pools; Device Credential profiles; Telemetry settings such as Syslog, Traps, and Netflow.
- **Site settings**: Settings define here override global settings and can include settings for servers, IP address pools, and device credential profiles.

Note Changes in network settings that are being used by the active fabric are not supported. These network settings include site hierarchy, renaming IP pools, and several other features.

Note Certain network settings can be configured on devices automatically using the Device Controllability feature. When Cisco DNA Center configures or updates devices, the transactions are captured in the Cisco DNA Center audit logs. You can use the audit logs to help you track changes and troubleshoot issues.

You can define the following global network settings by choosing **Design** > **Network Settings** and clicking the appropriate tab.

- Network servers, such as AAA, DHCP, and DNS—For more information, see Configure Global Network Servers, on page 95.
- Device credentials, such as CLI, SNMP, and HTTP(S)—For more information, see Configure Global CLI Credentials, on page 81, Configure Global SNMPv2c Credentials, on page 82, Configure Global SNMPv3 Credentials, on page 83, and Configure Global HTTPS Credentials, on page 85.
- IP address pools—For more information, see Configure IP Address Pools, on page 90.
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—For more information, see Configure Global Wireless Settings, on page 42.
- Configure global telemetry settings, such as syslog, SNMP, and NetFlow Collector servers using telemetry.

About Device Credentials

Device credentials refer to the CLI, SNMP, and HTTPS credentials that are configured on network devices. Cisco DNA Center uses these credentials to discover and collect information about the devices in your network. In Cisco DNA Center, you can specify the credentials that most of the devices use so that you do not have to enter them each time you run a discovery job. After you set up these credentials, they are available for use in the **Discovery** tool.

CLI Credentials

You need to configure the CLI credentials of your network devices in Cisco DNA Center before you can run a Discovery job.

These credentials are used by Cisco DNA Center to log in to the CLI of a network device. Cisco DNA Center uses these credentials to discover and gather information about network devices. During the discovery process, Cisco DNA Center logs in to the network devices using their CLI usernames and passwords and runs **show** commands to gather device status and configuration information, and **clear** commands and other commands to perform actions that are not saved in a device's configuration.

Note In Cisco DNA Center's implementation, only the username is provided in cleartext.

SNMPv2c Credentials

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language to monitor and manage network devices.

SNMPv2c is the community string-based administrative framework for SNMPv2. SNMPv2c does not provide authentication or encryption (noAuthNoPriv level of security). Instead, it uses a community string as a type of password that is typically provided in cleartext.

Note In Cisco DNA Center's implementation, SNMP community strings are not provided in cleartext for security reasons.

You must configure the SNMPv2c community string values before you can discover your network devices using the Discovery function. The SNMPv2c community string values that you configure must match the SNMPv2c values that have been configured on your network devices. You can configure up to 10 read community strings and 10 write community strings in Cisco DNA Center.

If you are using SNMPv2 in your network, specify both the Read Only (RO) and Read Write (RW) community string values to achieve the best outcome. If you cannot specify both, we recommend that you specify the RO value. If you do not specify the RO value, Cisco DNA Center attempts to discover devices using the default RO community string, *public*. If you specify only the RW value, Discovery uses the RW value as the RO value.

For Plug and Play, both SNMPv2c Read Only and Read Write credentials must be provided.

SNMPv3 Credentials

The SNMPv3 values that you configure to use Discovery must match the SNMPv3 values that have been configured on your network devices. You can configure up to 10 SNMPv3 values.

The security features provided in SNMPv3 are as follows:

- Message integrity: Ensures that a packet has not been tampered with in transit.
- Authentication: Determines if a message is from a valid source.
- Encryption: Scrambles a packet's contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and a user's role. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv: Security level that does not provide authentication or encryption
- AuthNoPriv: Security level that provides authentication, but does not provide encryption
- AuthPriv: Security level that provides both authentication and encryption

The following table describes the security model and level combinations:

Table 1: SNMPv3 Security Models and Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	User Name	No	Uses a username match for authentication.

Level	Authentication	Encryption	What Happens
AuthNoPriv	Either: • HMAC-MD5 • HMAC-SHA	No	Provides authentication based on the Hashed Message Authentication Code-Secure Hash Algorithm (HMAC-SHA).
AuthPriv	Either: • HMAC-MD5 • HMAC-SHA	Either: • CBC-AES-128 • CBC-AES-192 • CBC-AES-256	Provides authentication based on HMAC-MD5 or HMAC-SHA. Provides Advanced Encryption Standard (AES) 128-bit encryption, 192-bit encryption, or 256-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) mode AES for encryption.

The security level must be the same for the SNMPv3 user and the SNMPv3 groups to which that user belongs. If the SNMPv3 user and that user's SNMPv3 groups have different security levels, when Cisco DNA Center configures the SNMPv3 trap host, device SNMP reachability could become impaired.

HTTPS Credentials

HTTPS is a secure version of HTTP that is based on a special PKI certificate store.

About Global Device Credentials

"Global device credentials" refers to the common CLI, SNMP, and HTTPS credentials that Cisco DNA Center uses to discover and collect information about the devices in your network. Cisco DNA Center uses global credentials to authenticate and access the devices in a network that share these configured device credentials. You can add, edit, and delete global device credentials. You can also associate credentials to the Global site or a specific site.

Configure Global CLI Credentials

You can configure and save up to 10 global CLI credentials.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, in the **CLI Credentials** area, click **Add**.

Step 3 Enter information in the following fields:

Table 2: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.

Field	Description
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 4 Click **Save**.

To apply the credential to a site, click on the site in the hierarchy on the left, select the button next to the credential, then click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Configure Global SNMPv2c Credentials

You can configure global SNMPv2c credentials to monitor and manage your network devices.

Note For Plug and Play, both SNMPv2c Read Only and Read Write credentials must be provided.

Before you begin

You must have your network's SNMP information.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, in the **SNMP Credentials** area, click **Add**.

Step 3 For the Type, click **SNMP v2c** and enter the following information:

Table 3: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 4 Click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Configure Global SNMPv3 Credentials

You can configure global SNMPv3 credentials to monitor and manage your network devices.

Before you begin

You must have your network's SNMP information.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, in the **SNMP Credentials** area, click **Add**.

Step 3 For the Type, click **SNMP v3** and enter the following information:

Table 4: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.

Field	Description
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 4 Click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Configure Global HTTPS Credentials

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, in the **HTTPS Credentials** area, click **Add**.

Step 3 Enter the following information:

Table 5: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

Field	Description
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

Step 4 Click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update, and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Guidelines for Editing Global Device Credentials

The following are guidelines and limitations for editing existing global device credentials:

- Cisco DNA Center uses the following process when you edit, save, and then apply a global device credential:

  1. Cisco DNA Center pushes the credential to the device that has local authentication. With local authentication, credential changes are applied and Cisco DNA Center manages the devices using these credentials.

     (Cisco DNA Center does not push CLI credential changes to a device that is under a site with an inherited or configured AAA server. With AAA authentication, credential changes are not applied. Cisco DNA Center manages the devices using these credentials only if the same credentials exist on the AAA server.)

2. After successfully pushing the credential to the device, Cisco DNA Center confirms it can reach the device using the new credential.

   Note If this step fails, Inventory uses the old credentials to manage the device even though Cisco DNA Center pushed the new credentials to the device. In this case, the **Provision** > **Inventory** window might indicate that the device is Unmanaged if you updated an existing credential.

3. After successfully reaching the device using the new credential, the Cisco DNA Center Inventory starts managing the device using the new credential.

- Sites can contain devices that use SNMPv2c and SNMPv3 credentials. When you edit and save global SNMPv2c or SNMPv3 credentials, Cisco DNA Center pushes those changes to devices and enables that credential. For example, if you have a device that uses SNMPv2c, but you edit and save the SNMPv3 global credential, Cisco DNA Center pushes the new SNMPv3 credential to all devices in the associated site and enables it, meaning that all devices will be managed using SNMPv3, even the devices that previously had SNMPv2c enabled.
- To avoid any possible disruptions, modify the **User Name** when you edit CLI credentials. This creates a new CLI credential and leaves any existing CLI credentials unchanged.

Edit Global Device Credentials

You can edit and save global device credentials without Cisco DNA Center applying those credential changes until you're ready. When you decide to apply the changes, Cisco DNA Center searches all sites that reference the device credential you changed and pushes the change to all the devices.

You can update or create new global device credentials, but Cisco DNA Center never removes any credentials from devices.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, click **Manage Credentials**, check the check box for the device credential that you want to change, and choose **Actions** > **Edit**.

Step 3 In the **Edit Credentials** dialog box, make any changes, and click **Save**.

Note The CLI password credentials support only *ASCII-printable characters* (character code 32-127; see https://en.wikipedia.org/wiki/ASCII#Printable_characters).

Step 4 In the credential tile, click **Apply**.

Step 5 In the **Apply Credentials** dialog box, select whether to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update and click **Apply**.

  Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

A status message indicates whether the device credential change succeeded or failed.

Step 6 To view the status of the credential change, choose **Provision** > **Network Devices** > **Inventory**.

The **Credential Status** column displays one of the following statuses:

- Success: Cisco DNA Center successfully applied the credential change.
- Failed: Cisco DNA Center was unable to apply the credential change. Hover over the icon to display additional information about which credential change failed and why.
- Not Applicable: The credential is not applicable to the device type.

If you edited and saved more than one credential (for example, CLI, SNMP, and HTTPS), the **Credential Status** column displays **Failed** if Cisco DNA Center was unable to apply *any* of the credentials. Hover over the icon to display additional information about which credential change failed.

Associate Device Credentials to Sites

The sites you create under the Global site can inherit the global device credentials, or you can create different device credentials specific for a site.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 Select a site from the hierarchy in the left pane.

Step 3 Select the credential you want to associate with the selected site, then click **Save**.

A success message appears at the bottom of the screen indicating the device credential was successfully associated with the site.

Step 4 Click **Reset** to clear the entries on the screen.

Manage Device Credentials

The Manage Credentials workflow allows you to create, edit, assign, and apply credentials to devices.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 In the left pane, choose Global, site, or buildings, as required.

Step 3 Click **Manage Credentials**.
The **Manage Credentials** window opens.

Step 4 From the **Add** drop-down list, select any of the following credentials:

- **CLI**
- **HTTP(S) Read**
- **HTTP(S) Write**
- **SNMPv2c Read**
- **SNMPv2c Write**

- **SNMPv3**

Step 5 In the **Add New Credentials** window, do the following:

a. Complete the required fields.

b. Check the **Assign credential to site** check box.

Note If the box is not checked, the credential will get created but not assigned to any site.

c. Click **Save**.

The newly created credential appears in the **Manage Credentials** window.

Step 6 Choose the credential that you want to assign and click **Assign**.

Note
- The credential is assigned to Global, site, or building as chosen in the left pane.
- If you assign the credentials at the Global level, the site, building, and floor inherit settings from the Global level.

Step 7 To apply the credentials, do any one of the following:

- To apply a credential across the entire site hierarchy, go to **Manage Credentials**, hover your mouse over the desired credential's **Actions** ellipsis menu, and choose **Apply**.
- To apply a credential only to a specific site, choose the desired site in the left pane and click **Apply** on the card corresponding to that credential.

Step 8 In the **Apply Credentials** window, do the following:

- To apply the new credentials now, click the **Now** radio button and click **Apply**.
- To apply the new credentials at a later time, click the **Later** radio button. Then define the date and time of the update and click **Apply**.
- Click **Apply**.

The chosen credential will be applied to all the applicable sites.

You can reschedule the Apply credentials job that has not yet started.

Note If you want to apply the credentials to a specific site, navigate to the required site in the left pane and click Apply in the corresponding credential card.

Step 9 To view the status, do any one of the following:

- In the **Device Credentials** page, click the refresh icon at the top right corner. Hover your mouse over the icon next to the heading in the credential card.
- Go to **Provision** > **Inventory**. The **Credential Status** column shows the status.
- Go to **Activities** > **Audit Log**.

Step 10 To edit the credentials, do the following:

a. Click the edit icon for the credential. In the **Edit Information** window, click **OK**.

Alternatively, in the **Manage Credentials** window, hover your cursor over the ellipsis icon next to the credential name and choose **Edit**.

b. In the **Edit Credentials** window, make the required changes.

c. Click **Save**.

Step 11 To reschedule the **Start** time of a credential application, do the following:

a) (Job scheduled globally) In the **Manage Credentials** window, hover your cursor over the horizontal ellipsis icon next to the credential name and choose **Apply** and **Apply** again.

b) (Job scheduled from the main page for a non-global site) Return to the site for which the application was originally scheduled, click **Apply** on the corresponding credential tile window.

Note You cannot change the time zone.

Configure IP Address Pools

Cisco DNA Center supports IPv4 and IPv6 dual-stack IP pools.

You can manually create IPv4 and IPv6 address pools.

You can also configure Cisco DNA Center to communicate with an external IP address manager. For more information, see the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Click **Add** and complete the required fields in the **Add IP Pool** window.

If you have configured Cisco DNA Center to communicate with an external IP address manager, you cannot create an IP pool that overlaps an existing IP address pool in the external IP address manager.

Step 3 Click **Save**.

The newly added pool appears in the IP Address Pools table. You can click the **IPv4** or **IPv6** option in the **SUBNET TYPE** area if you prefer to view only the IPv4 or IPv6 address pools.

Note When you edit an IP address pool and make DHCP changes, you do not need to reprovision devices using that IP address pool.

Import IP Address Pools from an IP Address Manager

You can import IP address pools from Bluecat or Infoblox.

Note The IP address pools cannot have subpools and cannot have any assigned IP addresses from the IP address pool.

You must configure Cisco DNA Center to communicate with an external IP Address Manager (IPAM). For more information, see the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the **Actions** drop-down list, choose **Import from IPAM Server** and complete the required fields.

Step 3 Enter a CIDR and then click **Retrieve** to get the list of IP pools available to import.

Step 4 Click **Select All** or choose the IP address pools to import, then click **Import**.

Import IP Address Pools from a CSV File

You can import IP address pools from a CSV file.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the **Actions** drop-down list, choose **Import from CSV File**.

Step 3 Click **Download Template** to download the latest sample file.

Step 4 Add the IP address pools to the file and save the file.

Step 5 Upload the CSV file by doing one of the following actions:

a) Drag and drop the file to the drag and drop area.

b) Click where it says "**click** to select" and select the file.

Step 6 Click **Import**.

Reserve an IP Pool

Before you begin

Ensure that one or more IP address pools have been created.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Expand the hierarchy pane and choose a site.

Step 3 Click **Reserve** and complete the following fields to reserve all or part of an available global IP address pool for the specific site:

- **IP Address Pool Name**: Unique name for the reserved IP address pool.
- **Type**: Type of IP address pool. For LAN automation, choose **LAN**. Options are:
  - **LAN**: Assigns IP addresses to LAN interfaces for applicable VNFs and underlays.
  - **Management**: Assigns IP addresses to management interfaces. A management network is a dedicated network that is connected to VNFs for VNF management.
  - **Service**: Assigns IP addresses to service interfaces. Service networks are used for communication within VNFs.
  - **WAN**: Assigns IP addresses to NFVIS for UCS-E provisioning.
  - **Generic**: Used for all other network types.

- **IP Address Space**: IPv4 and IPv6 address pool from which you want to reserve all or part of the IP addresses.
- **CIDR Prefix/Number of IP Addresses**: IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses you want to reserve. If you choose \64 as the **CIDR Prefix** for an IPv6 IP pool, the **SLAAC** option is checked. (When **SLAAC** is selected, the devices automatically acquire IP addresses without the need for DHCP servers.)
- **Gateway**: Gateway IP address.
- **DHCP Servers**: DHCP server IP address(es).
- **DNS Servers**: DNS server address(es).

Step 4 Click **Reserve**.

If you reserve both IPv4 and IPv6 address pools, which means the fabric is provisioned with a dual-stack IP pool, you cannot switch back to a single-stack IP pool if the IPv6 pool is already attached to a VN.

However, if the IPv6 pool is not attached to a VN, you can downgrade it from a dual-stack IPv6 to a single-stack IPv4 pool. To downgrade to a single stack, in the IP Address Pools window, click **Edit** for the dual-stack IP pool. In the **Edit IP Pool** window, uncheck the **IPv6** check box and click **Save**.

Edit IP Pools

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Choose the Global site or expand the hierarchy tree and choose the desired site.

Step 3 To edit all the IP pools in bulk, do the following:

a) From the **Actions** drop-down list, choose **Edit All**.
b) Click **Yes** in the **Warning** message.
c) In the **Edit IP Pool** window make the desired changes and click **Save**.

Step 4 To edit only the desired IP pools, do the following:

a) Choose the desired IP pools and from the **Actions** drop-down list, click **Edit Selected**.

   You can also click **Edit** corresponding to the chosen IP pools.

b) In the **Edit IP Pool** window make the desired changes and click **Save**.

Delete IP Pools

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Choose the Global site or expand the hierarchy tree and choose the desired site.

Step 3 To delete all the IP pools in bulk, do the following:

a) From the **Actions** drop-down list, choose **Delete All**.
b) Click **Yes** in the **Warning** message.

Step 4 To delete only the desired IP pools, do the following:

a) Choose the desired IP pools and from the **Actions** drop-down list, click **Delete Selected**.

You can also click **Delete** corresponding to the chosen IP pools.

b) Click **Yes** in the **Warning** message.

Clone an IP Pool

You can clone an existing IP pool at the site level. When you clone an IP pool, the DHCP server and DNS server IP addresses are automatically filled.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Expand the hierarchy tree, and then choose a site.

Step 3 Locate the desired IP pool and, in the **Actions** area, click **Clone**.

Step 4 In the **Clone IP Pool** window, do the following:

a) Optionally, edit the pool name. (You cannot edit the Type, IP Address Space, or Global Pool values, which are inherited from the pool from which you are cloning.)

b) Edit the CIRD prefix values as necessary.

c) Click **Clone**.

Release IP Pools

You can release single-stack and dual-stack pools that are reserved at the site level.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Choose the Global site or expand the hierarchy tree and choose the desired site.

Step 3 To release all the IP pools in bulk, do the following:

a) From the **Actions** drop-down list, choose **Release All**.

b) Click **Yes** in the **Warning** message.

c) At the prompt, click **Release**.

Step 4 To release only the desired IP pools, do the following:

a) Choose the desired IP pools and from the **Actions** drop-down list, click **Release Selected**.

b) At the prompt, click **Release**.

View IP Address Pools

This procedure shows how to view 10 or more IP address pools in table view and tree view.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Select a site from the hierarchy in the left pane.

Step 3 Use the Toggle button to switch between the Table view and Tree view.

- When the view contains 10 or more IP pools, by default the GUI displays the pools in table view.
- When the view contains fewer than 10 IP pools, by default the GUI displays the pools in tree view.

Note Toggling between the table and tree map view is based on the pool count not on the user selection on the UI.

Tree view applies to the Global pool as well as to the site pool.

Step 4 The **IP Address Pools** table view displays list of IP address pools based on **Name**, **Type**, **IPv4 Subnet**, **IPv4 Used**, **IPv6 Subnet**, **IPv6 Used**, and **Actions**.

Note

- Hover your cursor over the **i** icon next to the **IPv4 Used** and **IPv6 Used**. A tooltip appears that displays more information about **IPv4 Used**, **IPv6 Used**, **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP address pool.
- In the **IPv4** and **IPv6** columns, hover your cursor over the **i** icon next to the corresponding used percentage of **IPv4** and **IPv6** for a given IP address pool. A tooltip displays the percentage of **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP addresses.

Step 5 In the Table view, click the **IPv4 only** or **Dual-Stack** option in the **Subnet Type** area if you prefer to view only the **IPv4** or **Dual-Stack** address pools.

Step 6 In the Tree view, hover your cursor over the IP address pool that you are interested in, and click to view the slide-in pane which contains the following information:

- Subnet type of an IP address pool.
- Percentage of available IP addresses along with **Pool CIDR**, **Gateway**, **DHCP Server(s)**, and **DNS Server(s)** under the respective pool.
- Percentage of used IP addresses under the respective pool.

Step 7 In the **Used** area, click **Assigned** to view the list of assigned IP addresses to a device filtered based on **Device Name**, **IP Address**, and **Site**.

Step 8 Click **Unassignable** to view the list of unassigned IP addresses which cannot be assigned to a device filtered based on **Device Name**, **IP Address**, and **Site**.

Step 9 Click **Edit** to edit an IP address pool.

Step 10 Click **Release** to release an IP address pool.

Note

- In the side bar for a global pool, you can view the usage of a given pool across all the child pool.
- Global and site IP address pool can have blocklisted IP addresses.
- Subpools cannot have blocklisted IP addresses.
  - Cisco DNA Center rejects the IP address pool creation request of a CIDR address pool if it contains blocklisted IP addresses.
  - In the next free IP address pools request, Cisco DNA Center skips the blocklisted IP addresses to find the next IP address free pool.

Step 11 (Optional) In the side bar click **Export** to export the table data.

Configure Service Provider Profiles

You can create a service provider (SP) profile that defines the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class service models. After you create an SP profile, you can assign it to an application policy and to the WAN interfaces in the application policy scope, including setting the subline rate on the interface, if needed.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **SP Profiles**.

Step 2 In the **QoS** area, click **Add**.

Step 3 In the **Profile Name** field, enter a name for the SP profile.

Step 4 From the **WAN Provider** drop-down list, enter a new service provider, or choose an existing one.

Step 5 From the **Model** drop-down list, choose a class model: **4 class**, **5 class**, **6 class**, and **8 class**.

For a description of these classes, see Service Provider Profiles.

Configure Global Network Servers

You can define global network servers that become the default for your entire network.

Note You can override global network settings on a site by defining site-specific settings.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **Network**.

Step 2 In the **DHCP Server** field, enter the IP address of a DHCP server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DHCP server in order to create IP address pools.

Step 3 In the **DNS Server** field, enter the domain name of a DNS server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DNS server in order to create IP address pools.

Step 4 Click **Save**.

Add Cisco ISE or Other AAA Servers

You can define Cisco Identity Services Engine (ISE) servers or other, similar AAA servers for network, client, and endpoint authentication at the site or global level. For network authentication, RADIUS and TACACS protocols are supported. For client and endpoint authentication, only RADIUS is supported. Only one Cisco ISE is supported per Cisco DNA Center.

You can configure the source interface under the RADIUS or TACACS server group to support multi-ISE configuration, wherein each Cisco ISE cluster has its own server group. The source interface used for RADIUS and TACACS servers is determined in the following way:

- If the device has a Loopback0 interface configured, Loopback0 is configured as the source interface.
- Otherwise, the interface that Cisco DNA Center uses as the management IP is configured as the source interface.

After you configure a Cisco ISE server for a site, the devices that are assigned to the site are automatically updated on the corresponding Cisco ISE server with a /32 mask. Subsequently, any changes to those devices in Cisco ISE are sent automatically to Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **Network**.

Step 2 Click **Add Servers** to add a AAA server.

Step 3 In the **Add Servers** window, check the **AAA** check box, and click **OK**.

Step 4 Set the AAA server for network users, client/endpoint users, or both.

Step 5 Check the **Network** and/or **Client/Endpoint** check boxes and configure servers and protocols for the AAA server.

Step 6 Choose the **Servers** for authentication and authorization: **ISE** or **AAA**.

- If you choose **ISE**, configure the following:
  - From the **Network** drop-down list, choose the IP address of the Cisco ISE server. The **Network** drop-down list contains all the IP addresses of the Cisco ISE servers that are registered in **System Settings** on the Cisco DNA Center home page. Selecting a Cisco ISE IP populates the primary and additional IP address drop-down lists with Policy Service Nodes (PSN) IP addresses for the selected Cisco ISE. You can either enter an IP address for the AAA server or choose the PSN IP address from the **IP Address (Primary)** and **IP Address (Additional)** drop-down lists.
  - Choose the **Protocol**: **RADIUS** or **TACACS**.

    Note AAA settings for a physical and managed site for a particular WLC must match, or provisioning fails.

- If you choose **AAA**, configure the following:
  - Enter an IP address for the AAA server or choose the IP addresses from the **IP Address (Primary)** and **IP Address (Additional)** drop-down lists. These drop-down lists contain the non-Cisco ISE AAA servers registered in the **System Settings**.

Step 7 Click **Save**.