



Design Network Hierarchy and Settings

- [Design a New Network Infrastructure, on page 1](#)
- [About Network Hierarchy, on page 2](#)
- [Monitor a Floor Map, on page 10](#)
- [Edit Floor Elements and Overlays, on page 10](#)
- [Floor View Options, on page 22](#)
- [Data Filtering, on page 26](#)
- [Create a Floor Map Using an Ekahau Project File, on page 28](#)
- [About Interactive Floor Planning, on page 30](#)
- [Configure Global Wireless Settings, on page 33](#)
- [Create Network Profiles, on page 56](#)
- [About Global Network Settings, on page 65](#)
- [About Device Credentials, on page 66](#)
- [About Global Device Credentials, on page 68](#)
- [Guidelines for Editing Global Device Credentials, on page 73](#)
- [Edit Global Device Credentials, on page 74](#)
- [Associate Device Credentials to Sites, on page 75](#)
- [Configure IP Address Pools, on page 76](#)
- [Import IP Address Pools from an IP Address Manager, on page 76](#)
- [Import IP Address Pools from a CSV File, on page 76](#)
- [Reserve an IP Pool, on page 77](#)
- [Edit IP Pools, on page 78](#)
- [Delete IP Pools, on page 78](#)
- [Clone an IP Pool, on page 79](#)
- [Release IP Pools, on page 79](#)
- [View IP Address Pools, on page 79](#)
- [Configure Service Provider Profiles, on page 81](#)
- [Configure Global Network Servers, on page 81](#)
- [Add Cisco ISE or Other AAA Servers, on page 82](#)

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 3](#).
 - Step 2** Define global network settings. For more information, see [About Global Network Settings, on page 65](#).
 - 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 3](#).
- Upload an existing network hierarchy from Cisco Prime Infrastructure. For more information, see [Upload an Existing Site Hierarchy, on page 5](#).

Guidelines for Image Files to Use in Maps

- Use a graphical application that can save the map image files to any of these formats: .jpg, .gif, .png, .dxf, and .dwg.
- Ensure that the dimension of an image is larger than the combined dimension of all the buildings and outside areas that you plan to add to the campus map.
- Map image files can be of any size. Cisco DNA Center imports the original image to its database at a full definition, 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.

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**.
A world map is displayed in the right pane.
- Step 2** In the **Network Hierarchy** window, click + **Add Site > Add Area** or click the gear icon ⚙ next to the parent site in the left pane, and then click **Add Area**.
- Step 3** Enter a name for the site in the **Area Name** field.
- Step 4** From the **Parent** drop-down list, choose a parent node.
By default, **Global** is the parent node.
- Step 5** Click **Add**.
The site is created under the parent node in the left pane.
You can also upload an existing hierarchy.
-

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 Access Points 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**.
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. 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.
To export maps, choose **Maps > Wireless Maps > Site Maps (New)**.
- Step 5** From the **Export** drop-down list, choose **Map Archive**.
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. Alternately, 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 overlaid 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**.
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, in the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Hierarchy**, and then choose **Import > Import Sites**.
A world map is displayed in the right pane.
- Step 10** In the **Import Sites** window, drag and drop the Cisco Prime Infrastructure location groups CSV file. Alternately click **Select CSV from your computer** to navigate to where the file is located, and click **Import** to import the Cisco Prime Infrastructure location groups CSV file.
- Step 11** Import the map archive file that contains floor maps and related map information. Choose **Design > Network Hierarchy**, and then choose **Import > Import Prime Maps**.
- Step 12** In the **Import Prime Maps Archive** window, drag and drop the map archive file, or click **click to select** to select the file from your workstation.
- Step 13** Click **Save**.
-

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** and then choose **Import > Import Sites**.
A world map is displayed in the right pane.
- Step 2** Drag and drop your CSV file, or navigate to where your CSV file is located, then click **Import**.
If you do not have an existing CSV file, click **Download Template** to download a CSV file that you can edit and upload.
- Step 3** To import the Cisco Prime Infrastructure maps tar.gz archive file, choose **Import > Map Import**.
- Step 4** Drag and drop the map archive file into the boxed area in the **Import Site Hierarchy Archive** dialog box, or click the **click to select** link and browse to the archive file.
- Step 5** Click **Save** to upload the file.
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. 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, choose **Export > 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 Archive window, do one of the following:
- In the **File Name** field, enter a filename, click **Export**, and click **OK**.
A new tar file containing the selected maps archive file is created and saved on your computer.
 - In the **File Name** field, enter an existing filename and click the **Click to select** link to choose the existing file from your computer. Click **OK**.
The maps are archived in the chosen file and saved in 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, 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 site hierarchy, choose **Export > Export Sites**. Alternatively, click more icon next to **Global** and choose **Export Sites**.
- Step 3** In the **Export Sites** dialog box, click **OK**.
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. The tree hierarchy is filtered based on the text you enter in the search field.

Edit Sites

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, navigate to the corresponding site that you want to edit.
- Step 3** Click the gear icon ⚙ next to the site and select **Edit Site**.
- Step 4** Make the necessary changes, and click **Update**.
-


Delete Sites

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, navigate to the site that you want to delete.
- Step 3** Click the gear icon ⚙ next to the corresponding site and select **Delete Site**.
- Step 4** Confirm the deletion.
-



Add Buildings

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Hierarchy**.
A world map is displayed in the right pane.
- Step 2** In the **Network Hierarchy** window, click **+Add Site > Add Building**, or click the gear icon ⚙ next to the parent site in the left pane and select **Add Building**.
-


You can also upload an existing hierarchy.

- Step 3** In the **Building Name** field, enter a name for the building.
The building name can contain all special characters except for " & ? ' / < > are allowed.
- Step 4** From the **Parent** drop-down list, choose a parent node.
By default, **Global** is the parent node.
- Step 5** In the **Address** field, enter an address. If you are connected to the Internet, as you enter the address, the Design Application narrows down the known addresses to the one you enter. The user can move the marker to change the position on the map. When you see that the correct address appears in the window, select it. When you select a known address, the **Longitude** and **Latitude** coordinates fields are automatically populated.
- Step 6** Click **Add**.
The building that you created is added under the parent site in the left menu.
- Step 7** To add another area or building, in the hierarchy frame, click the gear icon  next to an existing area or building that you want to be the parent node.
-

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 tree pane, navigate to the building that you want to edit.
- Step 3** Click the gear icon  next to the building and select **Edit Building**.
- Step 4** Make the necessary changes in the **Edit Building** window, and click **Update**.
-


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, navigate to the building that you want to delete.
- Step 3** Click the gear icon next to the building and select **Delete Building**.
- Step 4** Confirm the deletion.
- Note** Deleting a building deletes all its container maps. APs from the deleted maps are moved to Unassigned state.
-

Add a Floor to a Building

After you add a building, create floors and upload a floor map.

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

- Step 2** Expand the **Global** site and the previously created area to see all the previously created buildings.
- Step 3** Click the gear icon  next to the building to which you want to add a floor, and then click **Add Floor**.
- Step 4** Enter a name for the floor. The floor name contain upto 21 characters. has a 21.

The floor name can contain all special characters except for & > < ? ' / [] are not allowed.

The floor name can start with a letter or a hyphen (-) and the string following the first character can include one or more of the following:

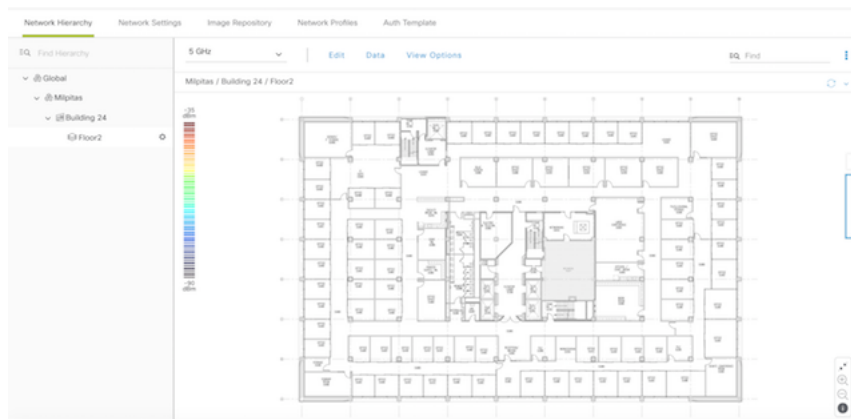
- Upper or lower case letters or both
- Numbers
- Underscores (_)
- Hyphens (-)
- Periods (.)
- Spaces ()

- Step 5** Define the type of floor by choosing the Radio Frequency (RF) model from the **Type (RF Model)** drop-down list: **Indoor High Ceiling**, **Outdoor Open Space**, **Drywall Office Only**, and **Cubes And Walled Offices**. This defines if the floor is an open space or a drywall office, and so on. Based on the RF model selected, the wireless signal strength and the distribution of heatmap is calculated.

- Step 6** You can drag a floor plan on to the map or upload a file. Cisco DNA Center supports the following file types: .jpg, .gif, .png, .dxf, and .dwg.

After you import a map, make sure that you mark the Overlay Visibility as **On (Floor > View Option > Overlays)**. By default, overlays are not displayed after you import a map.


Figure 1: Example of a Floor Plan



- Step 7** 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** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Design > Network Hierarchy**.
- Step 2** Expand the network hierarchy to find the floor that you want to edit, or enter the floor name in the **Search Hierarchy** text field in the left pane.
- Step 3** Make the necessary changes in the **Edit Floor** dialog window, and click **Update**.
-

Monitor a Floor Map

The floor view navigation pane provides access to multiple map functions like:

- Use the **Find** feature located at the top-right corner of the floor map window to find specific floor elements such as APs, sensors, clients, and so on. The elements that match the search criteria are displayed on the floor map along with a table in the right pane. When you hover your mouse over the table, it points to the search element on the floor map with a connecting line.
- Click the  icon at the top-right corner of the floor map window to:
 - Export a floor plan as a PDF.
 - Measure the distance on the floor map.
 - Set the scale to modify the floor dimensions.
- Click the  icon at the bottom-right of the floor map window to zoom in on a location. The zooming levels depend upon the resolution of an image. A high-resolution image might provide more zoom levels. Each zoom level comprises of a different style map shown at different scales, each one showing the corresponding details. Some maps are of the same style, but at a smaller or larger scale.
- Click the  icon to see a map with fewer details.
- Click the  icon to view the map icon legend.

Edit Floor Elements and Overlays

Using the **Edit** option available on the floor area, you can:

- Add, position, and delete the following floor elements:
 - Access Points
 - Sensors
- Add, edit, and delete the following overlay objects:
 - Coverage Areas
 - Obstacles
 - Location Regions

- Rails
- Markers
- GPS Markers

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. 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.

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

Cisco DNA Center supports the following 802.11ax APs:

- Cisco Catalyst 9120 Access Points
- Cisco Catalyst 9117 Access Points
- Cisco Catalyst 9115 Access Points
- Cisco Catalyst 9100 Access Points

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Floor Elements** panel, next to **Access Points**, click **Add**.

Access points that are not assigned to any floors appear in the list.

Step 5 On the **Add APs** window, 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.

Step 6 Close the **Add APs** window after assigning APs to the floor area.

Step 7 Newly added APs appear on the top-right corner of the floor map.

Step 8 In the **Floor Elements** pane, next to Access Points, click **Position** to position the APs correctly on the map.

- To position the APs, click an AP and drag and drop it to the appropriate location on the floor map. Alternatively you can update the x and y coordinates and AP Height in the **Selected AP Details** window. When you drag an access point on the map, its horizontal (x) and vertical (y) position appears in the text field. When selected, the access point details are displayed in the right pane. The **Selected AP Details** window displays the following:

- **Position by 3 points:** You can draw three points on the floor map and position APs using the points created. To do this:

- Click **Position by 3 points**.
- 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**.
- Define the second and third points similarly, and click **Save**.

- **Position by 2 Walls:** 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.

- Click **Position by 2 walls**.
- 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**.
- Define the second wall similarly and click **Save**.

The AP is placed automatically as per the defined distance between the walls.

- **AP Name:** Shows the AP name.
- **AP Model:** Indicates the AP model for the selected access point.
- **MAC Address:** Displays the MAC address.
- **x:** Indicates the horizontal span of the map, in the selected unit of measurement (either feet or meters).
- **y:** Indicates the vertical span of the map, in the selected unit of measurement (either feet or meters).
- **AP Height:** Indicates the height of the access point, in the selected unit of measurement (either feet or meters).

For each of the access point's radios:

- **Protocol:** Protocol for a radio: 802.11a/n/ac, 802.11b/g/n, or 802.11a/b/g/n.
- **Antenna:** Antenna type for a radio.
 - Note** While internal radios have only one antenna type, there may be several external antenna types to choose from.
- **Antenna Image:** Shows the antenna image (or AP image for an internal antenna).
- **Antenna Orientation:** Indicates the Azimuth and the Elevation orientations, in degrees.
- **Azimuth:** Horizontal angle of the antenna, measured clockwise relative to the x axis (so 0 azimuth indicates that the antenna is pointing right). The azimuth range is from 0 to 360.
 - Note** While most directional antennas reach maximum gain facing the azimuth, some antennas attain it by facing 90 degrees away from the azimuth. In those cases, if you configure an AP's azimuth to 0 (pointing right), the highest gain of the generated heatmap will point down. And if you configure the azimuth to 270 (pointing up), the highest gain of the generated heatmap will point right.
- **Elevation:** Vertical angle of the antenna. In wall-mounted antennas, elevation is measured relative to the horizontal axis. So, 45 degrees indicates that the antenna is pointing 45 degrees up, and -45 degrees means that the antenna is pointing 45 degrees down. In ceiling-mounted antennas, elevation is measured relative to the vertical axis. So, 45 degrees indicates that the antenna is pointing 45 degrees towards the azimuth, and -45 degrees means that the antenna is pointing 45 degrees in the opposite direction. The elevation range is -90 to 90 degrees.

Step 9 After you have completed placing and adjusting access points, click **Save**.

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

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 51](#).

Step 10 In the **Floor Elements** panel, next to **Access Points**, click **Delete**.

The **Delete APs** window appears, listing all the assigned and placed access points.

Step 11 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.

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**.

A world map is displayed in the right pane.

Step 3 You can either import the bulk APs by selecting the desired site in the left pane and from the **Import** drop-down list, choose **Import Bulk AP**, or click the gear icon next to the desired site in the left pane and choose **Import Bulk AP**.

Step 4 In the **Import Bulk AP** 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**.

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.

Quick View of APs

Hover your cursor over the AP icon on the floor map to view AP details, Rx neighbor information, client information, and Device 360 information.

- Click **Info** to view the following AP details:
 - **Associated**: Indicates whether an AP is associated or not.
 - **Name**: AP name.
 - **MAC Address**: MAC address of the AP.

- **Model:** AP model number.
 - **Admin/Mode:** Administration status of the AP mode.
 - **Type:** Radio type.
 - **OP/Admin:** Operational status and AP mode.
 - **Channel:** Channel number of the AP.
 - **Antenna:** Antenna name.
 - **Azimuth:** Direction of the antenna.
- Click the **Rx Neighbors** radio button to view the immediate Rx neighbors for the selected AP on the map with a connecting line. The floor map also shows whether the AP is associated or not along with the AP name.
 - Click **Device 360** to get a 360° view of a specific network element (router, switch, AP, or Cisco wireless controller).




Note For Device 360 to open, you must have the Assurance application installed.

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, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan.
- Step 4** In the **Floor Elements** panel, next to **Sensors**, click **Add**.
- Step 5** On the **Add Sensors** window, 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.
- Step 6** Close the **Add Sensors** window after assigning sensors to the floor map. Newly added sensors appear on the top-right corner of the floor map.

- Step 7** To position the sensors correctly, in the **Floor Elements** pane, next to **Sensors**, click **Position** to place them correctly on the map.
- Step 8** After you have completed placing and adjusting sensors, click **Save**.
- Step 9** To delete a sensor, in the **Floor Elements** pane, next to **Sensors**, click **Delete**. The **Delete Sensors** window lists all the assigned and placed sensors.
- Step 10** 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, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Overlays** panel, next to **Coverage Areas**, click **Add**. The **Coverage creation** dialog-box appears.
- Step 5** To draw a coverage area, from the **Type** drop-down list, choose **Coverage Area**.
- a. Enter the name of the area you are defining, and click **Add Coverage**. The coverage area must be a polygon with at least 3 vertices.
 - b. Move the drawing tool to the area you want to outline.
 - c. Click the tool to start and stop a line.
 - d. After you have outlined the area, double-click the area, which results in the area getting highlighted.
- Note** The outlined area must be a closed object for it to be highlighted on the map.
- Step 6** To draw a polygon-shaped area, from the **Type** drop-down list, choose **Perimeter**.
- a. Enter the name of the area you are defining, and click **Ok**.
 - b. Move the drawing tool to the area you want to outline.
 - Click the tool to start and stop a line.
 - After you have outlined the area, double-click the area, which results in area getting highlighted on the page.

- Step 7** To edit a coverage area, in the **Overlays** panel, next to **Coverage Areas**, click **Edit**.
The available coverage areas are highlighted on the map.
- Step 8** Make the changes and click **Save** after the changes.
- Step 9** To delete a coverage area, in the **Overlays** panel, next to **Coverage Areas**, click **Delete**.
The available coverage areas are highlighted on the map.
- Step 10** Hover your cursor over the coverage area and, click delete.
- Step 11** Click **Save** after the deletion.
-

Create Obstacles

You can create obstacles so that they can be considered while computing Radio Frequency (RF) prediction heatmaps for access points.

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (**≡**) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Overlays** panel, next to **Obstacles**, click **Add**.
- Step 5** In the **Obstacle Creation** dialog box, choose an obstacle type from the **Obstacle Type** drop-down list. The type of obstacles that you can create are **Thick Wall**, **Light Wall**, **Heavy Door**, **Light Door**, **Cubicle**, and **Glass**.
The estimated signal loss for the obstacle type you selected is automatically populated. The signal loss is used to calculate RF signal strength near these objects.
- Step 6** Click **Add Obstacle**.
- Step 7** Move the drawing tool to the area where you want to create an obstacle.
- Step 8** Click the drawing tool to start and stop a line.
- Step 9** After you have outlined the area, double-click the area to highlight it.
- Step 10** In the **Obstacle Creation** window, click **Done**.
- Step 11** Click **Save** to save the obstacle on the floor map.
- Step 12** To edit an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Edit**.
All the available obstacles are highlighted on the map.
- Step 13** Click **Save** after the changes.
- Step 14** To delete an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Delete**.
All the available obstacles are highlighted on the map.
- Step 15** Hover your cursor over the obstacle and click to delete.
- Step 16** Click **Save**.
-

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 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, select the floor.
- Step 3** In the **Overlays** panel, next to **Location Regions**, click **Add**.
- Step 4** In the **Location Region Creation** dialog window, from the **Inclusion Type** drop-down list, choose an option.
- Step 5** Click **Add Location Region**.
- A drawing icon appears to outline the inclusion area.
- Step 6** To begin defining the inclusion area, move the drawing tool to a starting point on the map and click once.
- Step 7** Move the cursor along the boundary of the area you want to include and click to end a border line.
Click again to define the next boundary line.
- Step 8** Repeat Step 7 until the area is outlined and then double-click the drawing icon.
A solid aqua line defines the inclusion area.
- Step 9** Click **Save**.
-

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, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Overlays** panel, next to **Location Regions**, click **Add**.

- Step 5** In the **Location Region Creation** window, from the **Exclusion Type** drop-down list, choose a value.
- Step 6** Click **Location Region**.
- A drawing icon appears to outline the exclusion area.
- Step 7** To begin defining the exclusion area, move the drawing icon to a starting point on the map and click once.
- Step 8** Move the drawing icon along the boundary of the area that you want to exclude.
- Click once to start a boundary line, and click again to end the boundary line.
- Step 9** Repeat the preceding step until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is fully defined.
- Step 10** To define more exclusion regions, repeat Step 5 to Step 9.
- Step 11** When all the exclusion areas are defined, click **Save**.
-

Edit Location Regions

- Step 1** In the **Overlays** panel, next to **Location Regions**, click **Edit**.
The available location regions are highlighted on the map.
- Step 2** Make the necessary changes, and click **Save**.
-


Delete Location Regions

- Step 1** In the **Overlays** panel, next to **Location Regions**, click **Delete**.
The available location regions are highlighted on the map.
- Step 2** Hover your cursor over the region that you want to delete, and click **Delete**.
- Step 3** Click **Save**.
-

Create a Rail

You can define a rail line on a floor that represents a conveyor belt. Also, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or outside of the snap-width area (minority).

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Overlays** panel, next to **Rails**, click **Add**.

- Step 5** Enter a snap-width (feet or meters) for the rail, and click **Add Rail**.
A drawing icon appears.
- Step 6** Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.
- Step 7** Click the drawing icon twice when the rail line is drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.
- Step 8** Click **Save**.
- Step 9** In the **Overlays** panel, next to **Rails**, click **Edit**.
The available rails are highlighted on the map.
- Step 10** Make changes, and click **Save**.
- Step 11** In the **Overlays** panel, next to **Rails**, click **Delete**.
All the available rail lines are highlighted on the map.
- Step 12** Hover your cursor over the rail line that you want to delete, and click **Delete**.
- Step 13** Click **Save**.
-

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, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Overlays** panel, next to **Markers**, click **Add**.
A drawing icon appears.
- Step 5** Enter the name for the markers, and then click **Add Marker**.
- Step 6** Click the drawing icon and place the marker on the map.
- Step 7** Click **Save**.
- Step 8** In the **Overlays** panel, next to **Markers**, click **Edit**.
The available markers are highlighted on the map.
- Step 9** Make changes, and click **Save**.
- Step 10** In the **Overlays** panel, next to **Markers**, click **Delete**.
All the available markers are highlighted on the map.
- Step 11** Hover your cursor on the marker that you want to delete, and click delete.
- Step 12** Click **Save**.
-

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, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **GPS Markers**, click **Add**.

A location icon appears.

Step 5 Locate the location icon on the floor map

- Note**
- You must locate the GPS markers a minimum threshold distance of 25 feet from each other.
 - You must not locate the GPS markers in a straight line.

A **Place Marker** dialog box appears to specify a physical address, latitude, and longitude coordinates of GPS marker on the floor map.

Step 6 Click **Add GPS Marker**.

Note You must add a minimum of three GPS markers to the floor map in a polygon-shape.

Step 7 Click **Save**.

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

Edit GPS Markers

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

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **GPS Markers**, click **Edit**.

Step 5 Click the GPS marker on the map that you want to edit.

A **Place Marker** dialog box appears to modify the physical address, latitude, and longitude coordinates of GPS marker on the floor map.

Step 6 Click **Edit GPS Marker**.

Step 7 Click **Save**.

Delete GPS Markers

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Overlays** panel, next to **GPS Markers**, click **Delete**.
- Step 5** Click the GPS marker on the map that you want to delete.
- Step 6** Click **Save**.
-

Floor View Options

Click the **View Options**, which is located above the floor plan in the middle pane. The floor map along with these panels appear in the right pane: **Access Points**, **Sensor**, **Overlay Objects**, **Map Properties**, and **Global Map Properties**.

You can modify the appearance of the floor map by selecting or unselecting various parameters. For example, if you want to view only the access point information on the floor map, check the **Access Point** check box. You can expand each panel to configure various settings available for each floor element.

View Options for Access Points

To view access points on a map, click the **On/Off** button next to **Access Points**. Expand the **Access Points** panel to configure these settings:

- **Display Label:** From the drop-down list, choose a text label that you want to view on the floor map for the AP. The available display labels are:
 - **None:** No labels are displayed for the selected access point.
 - **Name:** AP name.
 - **AP MAC Address:** AP MAC address.
 - **Controller IP:** IP address of Cisco Wireless Controller to which the access point is connected.
 - **Radio MAC Address:** Radio MAC address.
 - **IP Address**
 - **Channel:** Cisco Radio channel number or **Unavailable** (if the access point is not connected).
 - **Coverage Holes:** Percentage of clients whose signal has become weaker until the client lost its connection. It shows **Unavailable** for access points that are not connected and **MonitorOnly** for access points that are in monitor-only mode.
 - **TX Power:** Current Cisco Radio transmit power level (with 1 being high) or **Unavailable** (if the access point is not connected). If you change the radio band, the information on the map changes accordingly.

The power levels differ depending on the type of access point. The Cisco Aironet 1000 Series Lightweight Access Point accepts a value between **1** and **5**; the Cisco Aironet 1230AG Series Access Point accepts a value between **1** and **7**; and the Cisco Aironet 1240AG Series Access Point and Cisco Aironet 1100 Series Access Point accept a value between **1** and **8**.

- **Channel and Tx Power:** Channel and transmit power level (or **Unavailable** if the access point is not connected).
- **Utilization:** Percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays **Unavailable** for disassociated access points and **MonitorOnly** for access points in monitor-only mode.
- **Tx Utilization:** Transmitted (Tx) utilization for the specified interface.
- **Rx Utilization:** Received (Rx) utilization for the specified interface.
- **Ch Utilization:** Channel utilization for the specified access point.
- **Assoc. Clients:** Total number of clients associated.
- **Dual-Band Radios:** Identifies and marks the XOR dual-band radios on the Cisco Aironet 2800 and 3800 Series Access Points.
- **Health Score:** AP health score.
- **Issue Count**
- **Coverage Issues**
- **AP Down Issues**

- **Heatmap Type:** Heatmap is 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. From the **Heatmap Type** drop-down list, select the heatmap type:
 - **None**
 - **AP RSSI:** Coverage heatmap, which identifies the strength of wireless signal in the specific band.
 - **RSSI Cut off (dBm):** Drag the slider to set the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.
 - **Heatmap Opacity (%):** Drag the slider between 0 to 100 to set the heatmap opacity.
 - **Heatmap Color Scheme:** The color green indicates good heatmap coverage, and the color red indicates poor heatmap coverage.
 - **Client Density:** Density of associated clients.
 - **Map Opacity (%):** Drag the slider to set the map opacity.
 - **IDS:** Heatmap that shows the monitor mode access point coverage provided to the wireless clients on a floor map.
 - **Planned Heatmap:** A planned heatmap is a hypothetical heatmap that shows the possible coverage of planned access points on a floor map.

- **Coverage:** Heatmap that excludes monitor-mode access points. (Available only if monitor-mode access points are on the floor plan.)

The AP details are reflected on the map immediately. Hover your cursor over the AP icon on the map to view AP details, RX neighbors details, client details, and switch information.

View Options for Sensors

Click the **Sensors** button to view sensors on the map. Expand the **Sensors** panel to configure these settings:

- **Display Label:** From the drop-down list, choose a text label that you want to view on the floor map for the selected access point. The available display labels are:
 - **None**
 - **Name:** Sensor name.
 - **Sensor MAC Address:** Sensor MAC address.

View Options for Overlay Objects

Expand the **Overlay Objects** panel to configure these settings. Use the **On/Off** buttons to view these overlay objects on the map.

- **Coverage Areas**
- **Location Regions**
- **Obstacles**
- **Rails**
- **Markers**

View Options for Switches

Click the **On/Off** button next to **Switch** to view the list of APs available for that particular switch on the map.

Expand the **Switch** panel to configure the display label setting.

- **Display Label:** From the drop-down list, choose a text label that you want to view on the floor map for the selected switch. The available display labels are:
 - **None**
 - **Name**
 - **Switch MAC Address**
 - **APs Count**
 - **Clients Count**
 - **SSIDs Count**

The AP details for the selected switch are reflected on the map immediately. Hover your cursor over the switch icon on the map to view switch details.

Click the switch name to view the following details:

- Switch MAS Address
- APs count
- Clients count
- SSIDs count
- Heatmap: You can view heatmap for all the APs, APs which belong to a particular switch, or APs which belong to other switches by clicking the respective radio buttons.
- APs owned: Shows the list of APs which belongs to this particular switch.

Configure Map Properties

Expand the **Map Properties** panel to configure:

- **Auto Refresh**—Provides an interval drop-down list to set how often you want to refresh maps data from the database. From the **Auto Refresh** drop-down list, set the time intervals: **None**, **1 min**, **2 mins**, **5 mins**, or **15 mins**.

Configure Global Map Properties

Expand the **Global Map Properties** panel to configure:

- **Unit of Measure**—From the drop-down list, set the dimension measurements for maps to either **Feet** or **Meters**.

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**.

A world map is displayed in the right pane.

In the left pane, navigate to the floor on which you want to identify the interferer.

Step 2 In the site hierarchy pane, click the gear 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 3 In the **Network Hierarchy** window, click **View Options**.

Step 4 In the **View Options** window, scroll down and click the **On/Off** toggle button next to **Interferers** to view interferers on the floor map.

Step 5 Expand **Interferers** and click the **On/Off** toggle button next to **Show Zone of Impact** to view the zone of impact of interferers on the floor map.

Note By default, **Zone of Impact** is turned off.

Step 6 In the world map, hover your cursor over the interferer and click the impacted channel to view the interferer device details.

The **Interferer** window shows the following attributes of the identified interferer:

- Type
- State
- Name
- Interferer reported by either CMX or Cisco DNA Spaces
- MAC address
- Detecting AP(s)
- Duty cycle
- Affected channels
- Zone of impact
- First detected
- Last reported

Data Filtering

Filter Access Point Data

Click **Access Point** under the **Filters** panel in the right pane.

- Choose the radio type from the drop-down list, located above the floor map in the middle pane: **2.4 GHz**, **5 GHz**, or **2.4 GHz & 5 GHz**.
- Click + **Add Rule** to add a query:
 - Choose the access point identifier you want to view on the map.

- Choose the parameter by which you want to filter access points.
- Enter the specific filter criteria in the text box for the applicable parameters, and click **Go**. The search results appear in a tabular format.
- Click **Apply Filters to List** to view the filter results on the map. To view a particular access point on the map, check the check box of the access point in the table that is displayed, and click **Show Selected on Maps**.

When you hover your mouse cursor over the search result in the table, the location of the AP is marked by a line on the map.


Filter Sensor Data

Click **Sensor** under the **Filters** panel in the right pane.

- Choose the radio type from the drop-down list, located above the floor map in the middle pane: **2.4 GHz**, **5 GHz**, or **2.4 GHz & 5 GHz**.
- Click + **Add Rule** to add a query:
 - Choose the sensor identifier you want to view on the map: **Name** and **MAC Address**.
 - Choose the parameter by which you want to filter sensors.
 - Enter the specific filter criteria in the text box for the applicable parameters, and click **Go**. The search results appear in a tabular format.
 - Click **Apply Filters to List** to view the filter results on the map. To view a particular sensor on the map, check the check box of the sensor in the table that is displayed, and click **Show Selected on Maps**.

When you hover your mouse cursor over the search result in the table, the location of the sensor is marked by a line on the map.

Filter Client Data

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Design > Network Hierarchy**.
 - Step 2** In the left pane, select a floor.
 - Step 3** Click **Data**, which is located above the floor plan in the middle pane.
 - Step 4** In the **Filters** panel, click **Clients**.
 - Step 5** Click + icon to add a rule.
 - Step 6** From the filtering criteria drop-down list, choose the client identifier you want to view on the map.
 - Step 7** Choose the respective parameter for the chosen client identifier.
 - Step 8** Enter the specific filter criteria in the text box for the applicable parameters.
 - Step 9** Click **Apply Filters to List** to narrow down the clients list based on the following filter results on the map: **User Name**, **Average Health Score**, **Issues Count**, **IP Address**, **MAC Address**, **Status**, **Band**, **SSID**, **Vendor**, **AP Name**, **Operating System**, **Average RSSI (dBm)**, **Average SNR (dB)**, and **Average Data Rate**.

The search results appear in a tabular format.

Step 10 To view a particular client on the map, check the check box next to the client in the table, and click **Show Selected on Maps**.

Note When you hover your mouse over the search result in the table, a solid line and a dotted line appears,

- Solid line indicates the location of the client on the map.
- Dotted line indicates the association of the access point and the client on the map.

Create a Floor Map Using an Ekahau Project File

Before you begin

The Ekahau Pro tool allows you to create the complete network plan for your enterprise, including floor layout, AP locations, and obstacles. After creating the floor layout, you can export the simulated network plan and the real-world site survey data into a format that Cisco DNA Center can use. You can import the Ekahau project file into Cisco DNA Center for further planning.

The Ekahau Pro tool allows you to automatically create the site hierarchy, save it as a project file, and import it into Cisco DNA Center.



Note Ekahau projects are supported only for predictive mode, not for design mode.

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

- Create buildings and floors.

It is not mandatory to create buildings in the Ekahau Pro tool.

- Import the floor plan.
- Add the planned APs or hypothetical APs.
- Add building coordinates.
- Define the site name.

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 obstacles.
- Export the project as a PDF.

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 the Ekahau Project to Cisco DNA Center

Step 1 Design your network hierarchy by adding sites, buildings, and floors.

For more information, see [Create a Site in a Network Hierarchy, on page 3](#), [Add Buildings, on page 7](#), and [Add a Floor to a Building, on page 8](#).

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

Step 2 In the left pane, navigate to the site where you want to import the Ekahau project.

Step 3 Click the gear icon next to the site, and click **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.

Once the import is successful, 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 real AP with the same name.

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

To view reason for 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 with the planned AP, then the planned AP is replaced with the discovered real AP.
- If a planned AP remains unmapped, then you can manually replace the planned AP with real AP, providing reasons for 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** Select 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**.
A world map appears in the right pane.
- Step 2** In the left pane, select the desired site, building, or floor.
- Step 3** To export an Ekahau project of a site or building, from the **Export** drop-down list, choose **Export Maps**, or from the left pane, click the gear icon next to the desired site or building and choose **Export Maps**.
To export an Ekahau project of a floor map, from the left pane, click the gear icon next to the desired floor and choose **Export Maps**.
The **Information** dialog box appears.
- Step 4** In the **Information** dialog box, select the **Ekahau Project** export format.
- Step 5** Click **Yes**.
An ESX file is created and saved to your local machine.
- Step 6** Import the ESX file into the Ekahau Pro tool, augment the floor, and save the file.
- Step 7** Import the Ekahau project into the Cisco DNA Center under the site. For more information, see [Import the Ekahau Project to Cisco DNA Center](#).
-

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 on the floor.

- Plan all APs in sequence.
- Export the floor map as a PDF.

Interactive Floor Planning

- 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 menu, select the floor.
You can draw the planned APs and obstacles on the selected floor.
- Step 4** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 5** In the **Floor Elements** panel, next to **Planned Access Points**, click **Add**.
The **Add Planned AP** window appears.
- Step 6** In the **AP Name** text box, enter a name for the planned AP.
- Step 7** (Optional) In the **MAC Address** text box, enter the MAC address of the planned AP.
- Step 8** From the **AP Model** drop-down list, choose an AP model.
- Step 9** In the **x** and **y** text boxes, enter the horizontal and vertical span of the map, in feet.
- Step 10** In the **AP Height** text box, enter the height of the AP.
- Step 11** Click the radio band tabs to configure the antenna type, azimuth, and elevation orientation.
- Step 12** From the **Antenna** drop-down list, choose the appropriate antenna type for this AP.
The antenna image reflects the antenna selected.
- Step 13** Depending on the antenna type, enter the **Azimuth** and **Elevation** orientation, in degrees.
- Step 14** Click **Save**.
The newly added planned AP appears on the floor map.
- Step 15** If you have not specified the horizontal and vertical span (that is, the x and y coordinates), the planned AP appears on the top-right corner of the floor map.
- Step 16** Position the planned AP correctly on the map by dragging and dropping to the appropriate location on the map.
- Step 17** Click **Save**.
- Step 18** The next AP that you can plan appears on the top-right corner of the floor map.
- Step 19** Repeat Step 6 through Step 14 to plan the next AP.
- Step 20** To draw obstacles, in the **Overlays** panel, next to **Obstacles**, click **Add**.
For more information, see [Create Obstacles, on page 17](#).
- Step 21** To export the floor plan as a PDF, click the  icon at the top-right corner of the **Network Hierarchy** window, and choose **Export**.
- Step 22** In the **Export** window, check the **PDF** check box to export as a PDF.
- Step 23** Click **Export**.

The PDF is created and downloaded to your local machine. The PDF contains the floor map along with the planned AP details that you configured. The planned APs are listed based on the AP model.

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 menu, select the floor.
You can draw the planned APs and obstacles on the selected floor.
- Step 4** Click the **Unlock Floor** icon (🔓), which is located above the floor plan in the middle pane.
The list of AP models that are available on a particular floor appears on the left side of the floor map.
- Step 5** To add a new AP model to the floor, click **Add model**.
The **Select AP models to add** dialog box appears.
- Step 6** From the **Select AP models to add** drop-down list, choose the AP models, and then click **Add AP models**.
The new AP models are added to the floor.
- Step 7** To remove an AP model, click the **X** above the AP model name.
You can only remove an AP model if no APs of that model type are added to the floor map.
- Step 8** To add the planned APs to the floor map, click the AP model to select it, move your cursor to the appropriate location on the floor map, and then click again.
A planned AP of the selected model is added to the floor map and the **Edit Planned AP** pane appears on the right, with an AP name added to it by default.
- Step 9** From the **Edit Planned AP** pane, click the gear icon, which is located next to the **AP Name** field.
The **Name pattern** dialog box appears.
- Step 10** 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 11** From the **Antenna** drop-down list in the **Edit Planned AP** pane, choose the appropriate antenna type for each of the radio slots of the AP.
The antenna image reflects the antenna selected.

- Step 12** Depending on the antenna type, enter the **Azimuth** and **Elevation** orientation, in degrees.
- Step 13** 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.
- A new AP appears on the map with all of the properties inherited and the AP name appended, for example BLD1-AP0002-TX.
- Step 14** To add more APs with the same properties and appended AP Name, click the floor map.
- Step 15** To stop adding APs to the floor map, press **Esc** or right-click the floor map.
- Step 16** To reposition the APs, drag and drop them to the appropriate location in the floor map.
- Step 17** Click **Save** to save your changes or click **X** to discard them.
- Step 18** To delete a planned AP, right-click the AP name on the floor map, and click **Delete**.
- Step 19** To edit a planned AP, right-click the AP name on the floor map, and click **Edit**.
- The **Edit Planned AP** window appears. Make your changes in the **Edit Planned AP** window, and then click **Save**.
- Step 20** To view details, right-click the AP name on the floor map, and click **View Details**.
-

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** and then click the **Wireless** tab.
- Step 2** From the **SSID** table, hover over **+Add**  and choose **Enterprise**.
- The **Wireless SSID** workflow appears.
- Step 3** Complete the **Basic Settings** step:
- In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network or the SSID that you are creating.

Note The SSID name can contain up to 32 alphanumeric characters with leading spaces. All special characters except for </.* and trailing spaces are allowed.

The following combination of substring is not allowed: .*

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

- **Dual band operation (2.4 GHz and 5 GHz):** The WLAN is created for both 2.4 GHz and 5 GHz. The band select is disabled by default.
- **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 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 4 Complete the **Security Settings** step:

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

- **Enterprise:** You can configure both **WPA2** and **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).

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:** You can configure **WPA2** and **WPA3** security authentication types by checking the respective check boxes. 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 37](#).

- **Open Secured:** From the **Assign Open SSID** drop-down list, select an open SSID to redirect the clients to open secured SSID. The open secured policy provides least security.
- **Open:** Provides no security. It allows any device to connect to the wireless network without any authentication.

b) For **Authentication, Authorization, and Accounting Configuration**, configure the AAA-related settings:

- For **Configure AAA**, click  to add and configure the AAA servers for enterprise wireless network SSID. For more information, see [Configure AAA Server for an Enterprise Wireless Network](#).
- **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:** Check this check box to enable unique pre-shared keys that can be created for individuals or groups of users in the SSID.
- **Deny LLA Clients:** Check this check box to deny clients with random MAC addresses.

c) Click **Next**.

Step 5

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 access points and clients. MFP provides both infrastructure and client support.

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

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 their 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. The session timeout range is from 300 to 86400 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. The range is from 0 to 2147483647 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, the **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 6 Complete the **Associate SSID to Profile** step:


a) 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 non fabric.

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. Non fabric is a traditional wireless network that does not require SD-Access.


For a non fabric 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 access point 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.

- Click **Associate Profile** to choose the profile.
- Click **Next**.

Step 7 Review the **Summary** step and if necessary, click **Edit** for a step to go back to the step to make changes.

Step 8 If you are satisfied with the SSID settings, click **Save**.

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 menu, select 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

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 > Wireless**.

Step 2 Under **Enterprise Wireless** area, in the **Action** column click **Configure AAA** of SSID for which you want to configure the AAA server.

The **Configure AAA Server** for SSID window appears.

Step 3 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 AAA IP address.

Note The **Configure AAA** feature is not supported for Mobility Express (ME) and Evolved Converged Access (ECA) devices.

Step 4 Click+ to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of guest wireless network.

Step 5 From the **Additional Server** drop-down list, choose the server IP address.

Step 6 (Optional) To delete a server or an additional server, click the delete icon next to each server.


Step 7 Click **Configure**.


The 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, the 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, the 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 > Wireless**.

Step 2 Under  **Create**, click **Guest** to create a new SSID.

The **Guest Wireless Network** window appears.

Step 3 In the **Wireless Network Name (SSID)** field, enter a unique name for the guest SSID that you are creating.

The SSID name can contain up to 32 alphanumeric characters with leading spaces. All special characters except for < /.* and trailing spaces are allowed.

The following combination of substring is not allowed: .*

Step 4 Under **Type of Enterprise Network**, click **Voice and Data** or **Data Only**. The selection type defines the quality of service that is provisioned on the wireless network.

If you select **Voice and Data**, the quality of service is optimized for voice and data traffic.

If you select **Data Only** option, the quality of service is optimized for wireless data traffic only.

Step 5 Configure wireless band preferences by selecting one of the **Wireless Options**:

- **Dual band operation (2.4 GHz and 5 GHz):** The WLAN is created for both 2.4 GHz and 5 GHz. The band select is disabled by default.
- **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.

Step 6 Under **SSID STATE**, configure the following:

- Click the **Admin Status** button off, to disable the admin status.
- Click the **BROADCAST SSID** button off, if you do not want the SSID to be visible to all wireless clients within the range. Turning off the **Broadcast SSID** hides the SSID from clients attempting to connect to this SSID, reducing unnecessary load on the wireless infrastructure.

Step 7 Under **Level Of Security**, configure the layer 2 and layer 3 security policies.

Step 8 Under **L2 Security**, set the encryption and authentication type for this network.

Step 9 Click the **Enterprise**, **Personal**, **Open Secured**, or **Open** radio button to configure the respective security authentication.

- **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.

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.

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.

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

Step 10 Under **L3 Security**, set the encryption and authentication type for this guest network: **Web Policy** or **Open**.

Step 11 The **Open** policy type provides no security. It allows any device to connect to the wireless network without any authentication.

Step 12 If you choose **Web Policy**, you need to configure one of the authentication servers: **ISE Authentication**, **Web Authentication**, or **Web Passthrough**.

The **Web Policy** encryption and authentication type provides a higher level of Layer 3 security.

- For an External Web Authentication (EWA), click the **Web Policy** radio button as the level of security under **L3 Security** and **Web Authentication External** as the authentication server from the **Authentication** drop-down list.
- For a Central Web Authentication (CWA), click the **Web Policy** as the level of security under **L3 Security** and **ISE Authentication** as the authentication server from the **Authentication** drop-down list.

Step 13 Under **Authentication Server**, you can configure the authentication server for the SSID.

Step 14 If you choose **ISE Authentication**, choose the type of portal you want to create from the **WHAT KIND OF PORTAL ARE YOU CREATING TODAY ?** drop-down list:

- **Self Registered**: The guests are redirected to the Self-Registered Guest portal to register by providing information to automatically create an account.
- **HotSpot**: The guests can access the network without providing any credentials.

Choose where you want to redirect the guests after successful authentication from the **WHERE WILL YOUR GUESTS REDIRECT AFTER SUCCESSFUL AUTHENTICATION ?** drop-down list:

- **Success Page**: The guests are redirected to an **Authentication Success** window.
- **Original URL**: The guests are redirected to the URL they had originally requested.
- **Custom URL**: The guests are redirected to the custom URL that is specified here. Enter a redirect URL in the **Redirect URL** field.

Now that you have created an SSID, you must associate it with a wireless profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

Step 15 If you choose **Web Authentication** or **Web Passthrough**, configure **Internal** or **External** authentication type.

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.

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.

- If you choose **Web Authentication Internal** or **Web Passthrough Internal** from the **Authentication Server** drop-down list, then the page is reconstructed by the Cisco Wireless Controller.
- If you choose **Web Authentication External** or **Web Passthrough External** from the **Authentication Server** drop-down list, then the client is redirected to the specified URL. You need to enter a redirect URL in the **Web Auth Url** field.

Step 16 Under **TIMEOUT SETTINGS FOR SLEEPING CLIENTS**, configure authentication for sleeping clients: **Always authenticate** or **Authenticate after**.

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 page. You can configure the duration for which the sleeping clients are to be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 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 lesser than the time configured on the sleeping timer of the WLAN, then the lifetime of the client is used as the sleeping time.

- Click the **Always authenticate** radio button to enable authentication for sleeping clients.
- Click the **Authenticate after** radio button and enter the duration for which the 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.

Step 17 Click **Show Advanced Settings** to configure the following.

Step 18 Set **Fast Transition (802.11r)** to **Enable**, **Adaptive**, or **Disable** mode.

By default, **Fast Transition (802.11r)** is in **Adaptive** mode.

The 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.

Step 19 Check the **Over the DS** check box to enable fast transition over a distributed system. This option is available only if the **Fast Transition (802.11r)** is in **Adaptive** or **Enable** mode.

By default, the **Over the DS** check box is enabled.

Step 20 Under **11k**, check the **Neighbor List** check box to allow the 11k capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

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 their Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for next roam from the response frame.

Step 21 Check the **Client Exclusion** check box, and enter a value to set the client exclusion timer in the **in (secs)** field.

When a user fails to authenticate, the wireless controller excludes the client from connecting and 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. The range is 0 to 2147483647 seconds.

Step 22 Check the **Session Timeout** check box, and enter a value in seconds.

The session timeout is the maximum time for a client session to remain active before reauthorization. By default, the **Session Timeout** is enabled with a timeout of 1800 seconds. The range is 300 to 86400 seconds.

Step 23 Under **MFP Client Protection**, click one of the radio buttons: **Optional**, **Required**, and **Disabled**.

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 access points and clients. MFP provides both infrastructure and client support.

By default, the **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 the client supports CCXv5 MFP and is also configured for WPA2).

Step 24 Under **11k**, check the **Neighbor List** check box to allow the 11k capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

To facilitate roaming, a 11k capable client that is associated with an AP sends 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 their Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for the next roam from the response frame.

- Step 25** Under **11v BSS Transition Support**, configure the following.
- Step 26** Check the **BSS Max Idle Service** 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.
- 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.
- Step 27** Check the **Client User Idle Timeout** check box and enter a value to configure the user idle timeout for a WLAN in the **Client User Idle Timeout** field.
- If the data sent by the client is more than the threshold quota specified within the user idle timeout, then the client is considered to be active and the wireless controller refreshes for another timeout period.
- By default, the **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.
- Step 28** Check the **Directed Multicast Service** check box to enable the directed multicast service.
- By default, the **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 save the battery power.
- Step 29** Click **Configure AAA** to add and configure the AAA servers for guest wireless network SSID. For more information, see [Configure AAA Server for a Guest Wireless Network](#).
- Step 30** Click **Next**.
- The **Wireless Profiles** window is displayed.
- Step 31** If you do not have an existing wireless profile, in the **Wireless Profiles** window, click **Add** to create a new wireless profile.
- Step 32** Enter a profile name in the **Wireless Profile Name** field.
- Step 33** Specify whether the SSID is fabric or not by clicking the **Yes** or **No** radio button next to **Fabric**.
- 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 SDA. Nonfabric is a traditional wireless network that does not require SD-Access.
- Step 34** If you want the guest SSID to be a guest anchor, click the **Yes** or **No** radio button next to **Do you need a Guest Anchor for this guest SSID**.
- If you want your guest SSID to be a guest anchor, click **Yes**.
- Step 35** From the **Select Interface** drop-down list, choose the interface or click + to create a new wireless interface.
- This is the VLAN ID that is associated with the wireless interface.
- Step 36** If you click **No**, enable the FlexConnect mode by checking the **Flex Connect Local Switching** check box. The selection of FlexConnect mode switches the traffic locally. Based on your configuration, the profile is applied to a site and a flex group is created internally.
- 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.
- Step 37** In the **Local to VLAN** field, enter a value for the VLAN ID.
- Step 38** To assign this profile to a site, click **Sites**.

- Step 39** In the **Sites** window, check the check box next to the site to associate this profile and click **OK**.
You can either select a parent site or the individual sites. If you select a parent site, all children inherit their settings from the parent site. You can uncheck the check box to deselect a site.
- Step 40** Click + Add Model Config to attach a model config design to the wireless profile.
The **Add Model Config** window appears.
- Step 41** 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 42** Under **APPLICABILITY**, from the **Tags** drop-down list, choose the applicable tags.
- Step 43** Click **Add**.
- Step 44** Click **Save**.
The created profile appears in the **Wireless Profiles** window.
- Step 45** To associate the SSID to a wireless profile, in the **Wireless Profiles** window, check the **Profile Name** check box to associate the SSID; then, click **Next**.
The **Portal Customization** window appears, where you can assign the SSID to a guest portal.
- Step 46** In the **Portal Customization** window, click **Add** to create the guest portal.
The **Portal Builder** window appears.
- Step 47** Expand **Page Content** in the left menu to include various variables.
- Step 48** Drag and drop variables into the portal template window and edit them.
- The variables for the **Login** page are:
 - **Access Code**
 - **Header Text**
 - **AUP**
 - **Text Fields**
 - The variables for the **Registration** page are:
 - **First Name**
 - **Last Name**
 - **Phone Number**
 - **Company**
 - **SMS Provider**
 - **Person being visited**
 - **Reason for a visit**
 - **Header text**
 - **User Name**

- **Email Address**
- **AUP**
- The variables for the **Registration Success** page are:
 - **Account Created**
 - **Header texts**
- The variable for the **Success** page is: **Text fields**.

Step 49 To customize the default color scheme in the portal, expand **Color** in the left menu and change the color.

Step 50 To customize the font, expand **Font** in the left menu and change the font.

Step 51 Click **Save**.

The created portal appears in the **Portal Customization** window.

Step 52 Under **Portals**, click the radio button next to the **Portal Name** to assign the SSID to that guest portal.

Step 53 Click **Finish**.

Configure AAA Server for a Guest Wireless Network

Before you begin

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 > Wireless**.

Step 2 Under **Guest Wireless** area, in the **Action** column click **Configure AAA** of SSID for which you want to configure the AAA server.

The **Configure AAA Server** for SSID window appears.

Step 3 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) and Evolved Converged Access (ECA) devices.

Step 4 Click+ to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of guest wireless network.

Step 5 From the **Additional Server** drop-down list, choose the server IP address.

Step 6 (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 7 Click **Configure**.

The 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, the 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, the 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 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 > Wireless**.

Step 2 Under **Wireless Interfaces**, click **+Add**.

The **New Interfaces** window appears.

Step 3 In the **Interfaces Name** text box, enter the dynamic interface name.

Step 4 (Optional) In the **VLAN ID** text box, enter the VLAN ID for the interface. The valid range is from 0 to 4094.

Step 5 Click **Ok**.

The new interface appears under **Wireless Interfaces**.

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 > Wireless**.
- Step 2** In **VLAN Group**, you can view the **VLAN Group Name** and **VLAN ID** columns.
- Step 3** Click **Add**.
The **Add VLAN Group** dialog box opens.
- 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 a screen, click **Next** to advance to the next screen.
- Step 15** Click **Deploy**.
The **Provision Device** dialog box is displayed.
- Step 16** Choose **Now** and click **Apply**.
The message **Task Scheduled view status in Tasks** appears at the bottom-right corner.
-

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 > Wireless**.
- Step 2** Under **Wireless Radio Frequency Profile**, click **+Add RF**.
The **Wireless Radio Frequency** window appears.
- Step 3** In the **Profile Name** text box, enter the RF profile name.

Step 4 Use the **On/Off** button to select the radio band: **2.4 GHz** or **5 GHz**. 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 5 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 pre-canned RF profiles. If you select any of the pre-canned RF profiles, the respective RF profiles which are there in the device is used and the new RF profile is not be 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 need to configure these channels globally on Cisco Wireless Controller.

- 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**, you can set the power level and power threshold for an AP.
 - **Power Level**—To determine whether the power of an AP needs to be reduced or not. 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 -10 to 30 dBm and the default is -10 dBm.
 - **Power Threshold**—It is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP or not. 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 -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 APs 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 6 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 pre-canned RF profiles. If you select any of the pre-canned RF profiles, the respective RF profiles which are already there in the device is used and the new RF profile is not be created on the 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, or Best.**
- Set the **DCA Channel** to manage channel assignments:

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

- **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 the check box of the channels to select them individually.
- **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 the check box of the channels to select them individually.
- **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 the check box of the channels to select them individually.
- 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**, you can set the power level and power threshold for an AP.
 - **Power Level**—To determine whether the power of an AP needs to be reduced or not. 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 -10 to 30 dBm and the default is -10 dBm.
 - **Power Threshold**—It is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP or not. 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 -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 APs 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 Click **Save**.

Step 8 To mark a profile as a default RF profile, check the **Profile Name** check box and click **Mark Default**.

Step 9 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 > Wireless**.
- Step 2** Click **Add Create** and choose **Enterprise**.
- Step 3** Toggle the **Sensor** field and click **Next**.
- Note** The parameters for the SSID are automatically populated and cannot be edited.
- Step 4** Click **Next**.
- Step 5** In the **Wireless Profiles** screen, check a profile from the **Profiles** table. The **Edit Wireless Profile** dialog box opens.
- Step 6** In Fabric, select **Yes** and click **Save**. The **Success Profile sensorProfile selected** message appears.
- Step 7** Click **Finish**.
- Step 8** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 9** Check a device and from the **Actions** drop-down menu, choose **Provision > Provision Device**.
- Step 10** Review the details under **Assign Site, Configuration, Model Configuration, Advanced Configuration, and Summary**. Click **Next** after each screen.
- Step 11** Click **Deploy**. The **Provision Device** dialog box is displayed.
- Step 12** Choose **Now** and click **Apply**. 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**. The **Sensor List** window appears.

Step 2 Click on **Settings > Backhaul Settings** tab. The **Backhaul Settings** window appears.

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 user name and password in the fields provided.

- **PEAP-MSCHAPv2:** Enter the user name 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 user name 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 user name 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 pre-shared 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 pre-shared 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 > External Services > CMX Servers**.

The **CMX Servers** window appears.

Step 2 Click **Add**.

The **Add CMX Server** window appears.

Step 3 In the **IP Address** field, enter the valid IP address of the CMX web GUI.

Step 4 In the **User Name** and **Password** fields, enter the CMX web GUI username and password credentials.

Step 5 In the **SSH User Name** and **SSH Password** fields, enter the CMX admin username and password credentials.

Note Make sure that CMX is reachable.

Step 6 Click **Add**.

The CMX server is added successfully.

Step 7 To assign a CMX server to a site, building, or a floor, click the **Menu** icon and choose **Design > Network Settings > Wireless**.

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

Step 9 Under **CMX Servers**, from the **CMX Servers** drop-down list, select the CMX server.

Step 10 Click **Save**.

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.

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 11 If the CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** page, click the gear icon next to the building or floor on which you made the changes in the left tree pane, and then choose **Sync with CMX** to push the changes manually.

Step 12 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 > External Services > CMX Servers**.
- b) Select the CMX server that you want to edit, make any changes, and click **Update**.
- c) Select the CMX server that you want to delete and click **Delete**.
- d) 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

Deploy the **DNA Spaces Enabler Package** software on Cisco DNA Center:

- a) Contact your Cisco account representative to obtain the **DNA Spaces Enabler Package** software.
- b) Log in to Cisco DNA Center.
- c) From the Cisco DNA Center GUI, click the ? icon to verify that Cisco DNA Center is running the current release.
- d) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Software Updates**.

The **Software Updates** page opens and the **DNA Spaces Enabler Package** is displayed in the list of **Application Updates**.

- e) Click **Install All**.

The **Select Any Package To Continue** dialog box is displayed.

- f) Select the **DNA Spaces Enabler Package** and click **Continue**.

The **System Readiness Check** dialog box is displayed.

- g) Click **Continue**.

The **Success** dialog box states that the package will soon be installed.

Step 3 Register Cisco DNA Center with Cisco DNA Spaces:

- 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 **Integrations > DNA Center**.

The **DNAC Integration** window is displayed.

- d) In the **DNAC Integration** window, click **Create Token**.

The **Create new token** dialog box is displayed.

- e) In the **Instance Name** field, enter a unique name for the instance, and then click **Create Token**.

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**.

The **DNA Spaces/CMX Servers** window is displayed.

- j) From the **DNA Spaces** area, choose **Activate**.

The **Integrate DNA Spaces** dialog box is displayed.

- k) In the **Tenant Token** text box, press **Ctrl V** to paste the token that you copied from Cisco DNA Spaces, then click **Connect**.

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 4 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 > Wireless**.

- b) In the left tree view menu, select either **Global** or the area, building, or floor to which you want to assign Cisco DNA Spaces.

- c) Under **DNA Spaces/CMX Servers**, from the **Location Services** drop-down list, select a site (for example, DNA Spaces - dna-center-dev-US).
- d) Click **Save**.

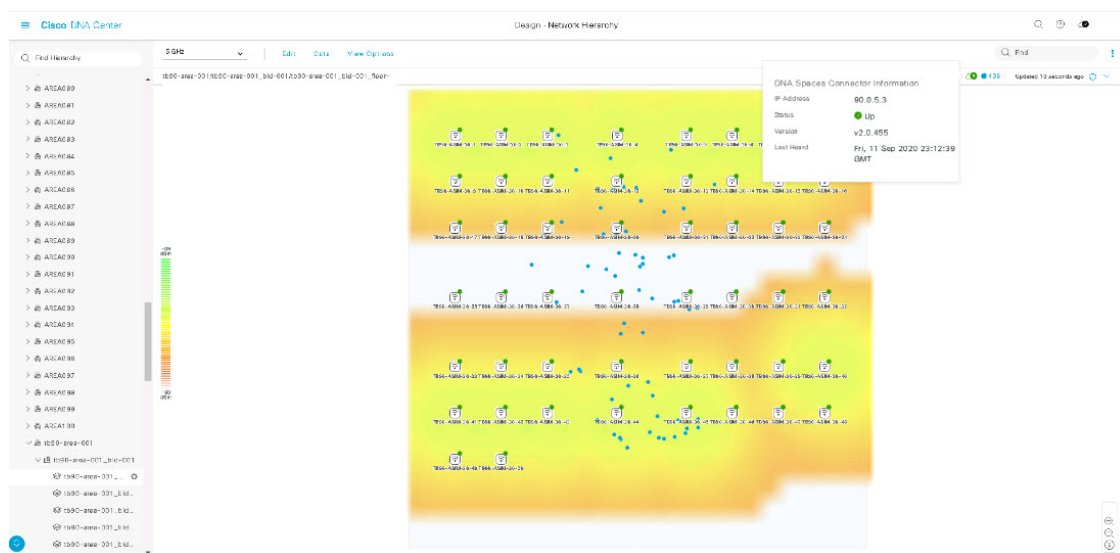
Step 5 Monitor sites in Cisco DNA Center using Cisco DNA Spaces:

- 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 2: Cisco DNA Spaces Status Icon



Configure Native VLAN for a Flex Group

Native VLAN carries the management traffic between APs and Cisco Wireless Controllers. With this feature, you can configure VLAN for a site through the Cisco DNA Center user interface. You can configure native VLAN at the global level and override at the site, building, or floor level.

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 **Global** if you are configuring native VLAN at the global level.


Step 3 Under **Native VLAN**, enter a value for the VLAN ID in the VLAN text box. The valid range is from 1 to 4094.

Step 4 Click **Save**.

Step 5 Configure the SSID and create a wireless network profile. Make sure that the **FlexConnect Local Switching** check box on the **Design > Network Settings > Wireless** page is enabled. For more information, see the [Create SSIDs for an Enterprise Wireless Network, on page 33](#) and [Create SSIDs for a Guest Wireless Network, on page 38](#).

- Step 6** For the saved VLAN ID to get configured on the wireless controller, you must provision the wireless controller on the **Provision** page. For more information, see [Provision a Cisco AireOS Controller](#).
- Step 7** After provisioning the wireless controller, you must provision the AP that is associated with the controller. For more information, see [Provision a Cisco AP—Day 1 AP Provisioning](#).
- Step 8** To override the native VLAN at the site, building, or floor level, in the left tree view menu, select the site, building, or floor.
- Step 9** Under **Native VLAN**, enter a value for the VLAN ID.
- Step 10** Reprovision the wireless controllers and the associated access point.
-

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 81](#).
- 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 3](#).

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 81](#).
- 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 3](#).

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 3](#).

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 3](#).

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** Check the **Flex Connect Local Switching** check box to enable local switching for the WLAN.
- 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 10** 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 11** Click **+ Add Model Config** to add model config designs to a network profile.
- The **Add Model Config** window appears.
- Step 12** 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 13** Expand **Wireless** and select the model config design that you are attaching to this wireless profile.
- Step 14** From the **Tags** drop-down list under **APPLICABILITY**, select the applicable tags.
- Step 15** Click **Add**.
- The attached model config appears under the **Attach Model Config** area in the **Add a Network Profile** window.
- Step 16** To associate a template with the network profile, click **Add** under the **Attach Template(s)** area.
- Step 17** 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 18** 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 19 Click **Add**.

The created profile appears in the **Wireless Profiles** window.

Step 20 Click **Save** to add a network profile.

The newly added network profile appears on the **Design > Network Profiles** page.

Step 21 To assign this profile to a site, click **Assign Sites**.

Step 22 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 23 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:
- 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**.

About 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 defined 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 81](#).
- Device credentials, such as CLI, SNMP, and HTTP(S)—For more information, see [Configure Global CLI Credentials, on page 68](#), [Configure Global SNMPv2c Credentials, on page 69](#), [Configure Global SNMPv3 Credentials, on page 70](#), and [Configure Global HTTPS Credentials, on page 72](#).
- IP address pools—For more information, see [Configure IP Address Pools, on page 76](#).
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—For more information, see [Configure Global Wireless Settings, on page 33](#).
- 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.
AuthNoPriv	Either: <ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA 	No	Provides authentication based on the Hashed Message Authentication Code-Secure Hash Algorithm (HMAC-SHA).
AuthPriv	Either: <ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA 	Either: <ul style="list-style-type: none"> • CBC-DES • CBC-AES-128 	Provides authentication based on HMAC-MD5 or HMAC-SHA. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or 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.
Password	<p>Password that is used to log in to the CLI of the devices in your network.</p> <p>For security reasons, re-enter the password as confirmation.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Enable Password	<p>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</p> <p>For security reasons, re-enter the enable password.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

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	<ul style="list-style-type: none"> • 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. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • 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. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

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.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5: Authentication based on HMAC-MD5.

Field	Description
Auth Password	<p>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.</p> <p>Note</p> <ul style="list-style-type: none"> • 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	<p>Privacy type. (Enabled if you select AuthPriv as the authentication mode.) Choose one of the following privacy types:</p> <ul style="list-style-type: none"> • AES128: CBC mode AES for encryption. • None: No privacy.
Privacy Password	<p>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.</p> <p>Note</p> <ul style="list-style-type: none"> • 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	<p>You can configure up to 10 HTTPS read credentials:</p> <ul style="list-style-type: none"> • 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). <p>The password must contain from 7 to 128 characters, including at least one:</p> <ul style="list-style-type: none"> • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>

Field	Description
Write	<p>You can configure up to 10 HTTPS write credentials:</p> <ul style="list-style-type: none"> • 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). <p>The password must contain from 7 to 128 characters, including at least one:</p> <ul style="list-style-type: none"> • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>

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

When you edit global device credentials, the changes impact all devices that are associated to the sites under the global site. After you edit and save a global device credential, 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, select the device credential you want to change, and under the **Actions** column on the right, click **Edit**.

Step 3 In the **Edit CLI Credentials** dialog box, click **Save**.

Step 4 In the **Apply CLI Credentials** dialog box, click **Cancel**.

Step 5 At the bottom of the **Device Credentials** window, click **Save**.

The following message is displayed:

```
Created Common Settings successfully.
```

Step 6 Return to the **Device Credentials** window and click **Edit** for the desired device credential.

Step 7 In the **Edit CLI 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 8 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 9 To view the status of the credential change, in the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > 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.

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:
- Drag and drop the file to the drag and drop area.
 - 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:
- 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.)
 - Edit the CIRD prefix values as necessary.
 - 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:
- From the **Actions** drop-down list, choose **Release All**.
 - Click **Yes** in the **Warning** message.
 - At the prompt, click **Release**.
- Step 4** To release only the desired IP pools, do the following:
- Choose the desired IP pools and from the **Actions** drop-down list, click **Release Selected**.
 - 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**.
