Manage Maps

Manage Maps

Uploading Maps to Cisco Spaces: Detect and Locate

One of the first setup tasks is uploading maps that are exported from Cisco Prime Infrastructure to Cisco Spaces: Detect and Locate. Typically, map data contains floor images, floor coordinates, access points (AP), calibration data, and details about APs on a floor.

Before you begin

If Cisco Spaces: Detect and Locate is launched through Cisco Spaces, maps are automatically synchronized into through Cisco CMX tethering.

Step 1 Log in to Cisco Spaces: Detect and Locate.

Step 2 From the left navigation pane, click **Maps** and then choose the **Upload** button.

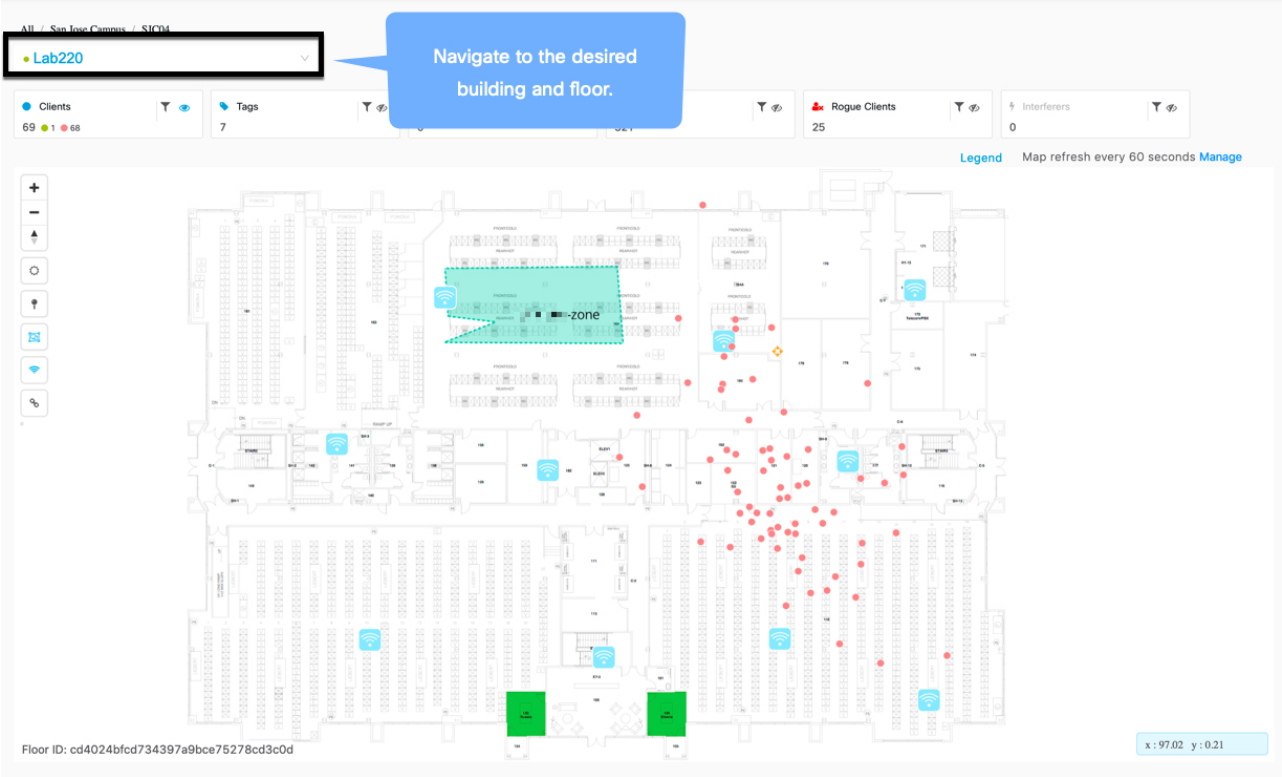
Step 3 Browse to the location where the maps are stored (on your computer). Select the maps that were previously exported from Cisco Prime Infrastructure.

Step 4 Verify if the maps are uploaded successfully.

Viewing the Map on Cisco Spaces: Detect and Locate

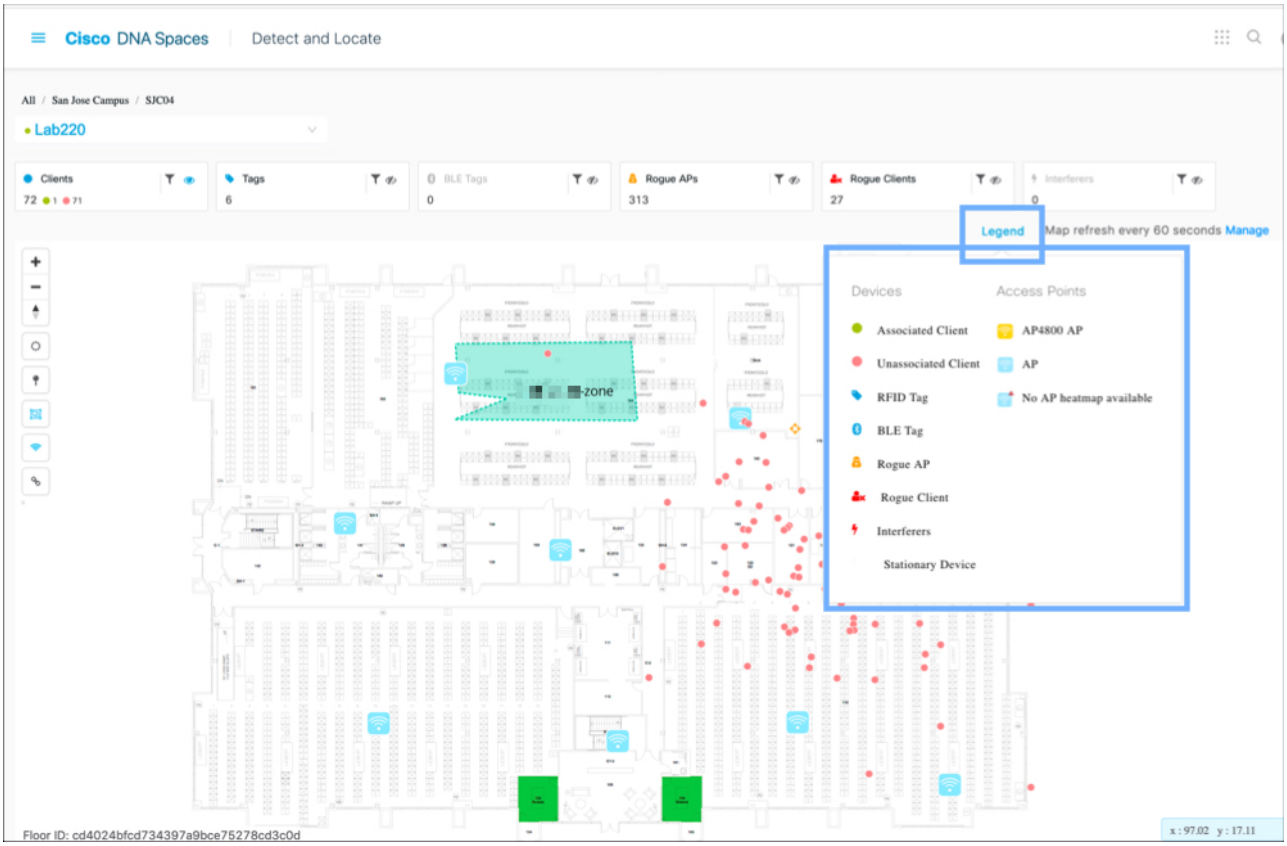
Step 1 From the Cisco Spaces: Detect and Locate dashboard, use the drop-down list to navigate to the desired campus, building, and floor.

Figure 1: Cisco Spaces: Detect and Locate Dashboard



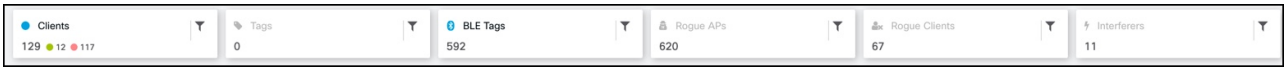
Step 2 Click **Legend** to understand the various markings on the map.

Figure 2: Legend



Step 3 From the toolbar on the top, choose any combination of the icons to customize your view of the devices.

Figure 3: Dashboard: Total Count Toolbar



- Clients: All client devices (connected and detected).
  - A red dot indicates probing clients. Click to see additional details about a client.
  - A dot associated with a number indicates a cluster of probing clients. Click to view details of all the clients in that cluster. You can also zoom in to view the clients individually.
  - A green dot indicates connected clients. Click to see additional details of a client.
- Rogue Access Points: APs that are not part of or managed by the Cisco CMX infrastructure. Click to see additional details.
- Rogue Clients: Clients that are connected to rogue access points.
- Interferers: Devices that can create a radio frequency interference. .

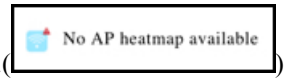
- Tags: Vendor-specific information that is related to Wi-Fi tags are displayed in raw format.
- BLE Tags: Bluetooth Low Energy tags attached to track devices.

Step 4 (Optional) Click the  icon to filter the displayed items. These filters are persistent and across sessions.

Step 5 Choose any combination of the following icons to enable or disable other elements on your dashboard, like zones, access points, and tags and heat maps.

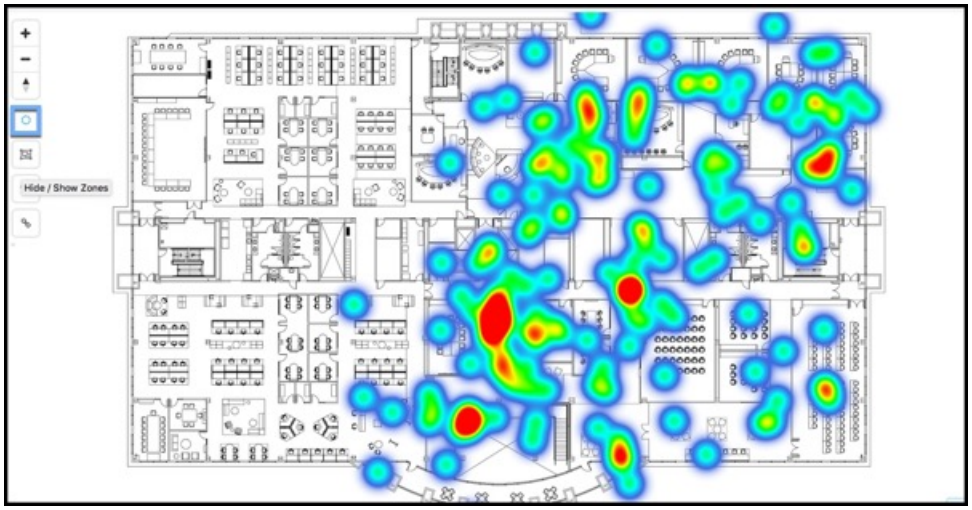
Figure 4: Dashboard: Left Toolbar

- Zones  : Show or hide the zones on a specific floor.
- Access Point  : Show or hide all the APs that have been deployed on a specific floor. If the map has been uploaded to Detect and Locate, your map indicates which APs have device location (

) and which APs have issues with device location and hence may need troubleshooting.(

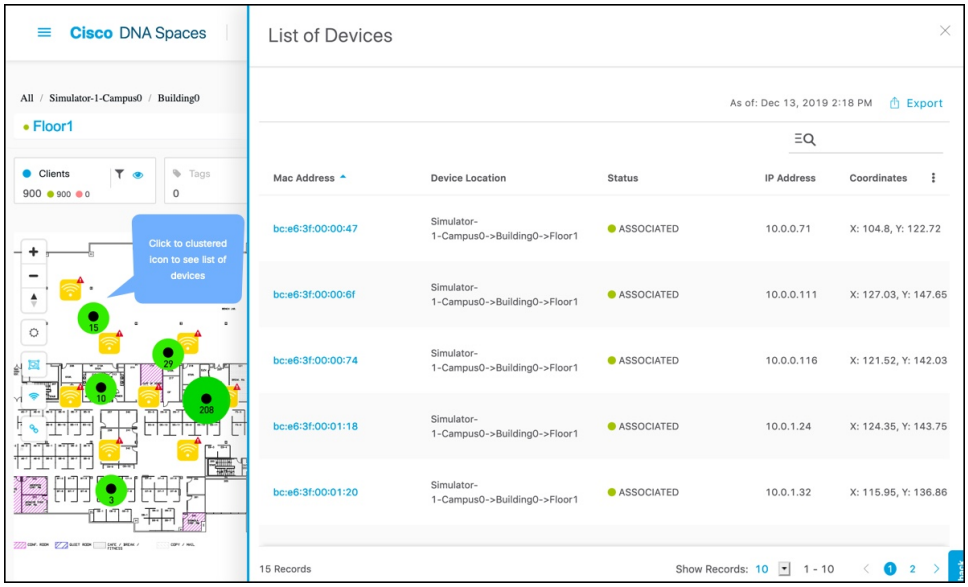
)
- Heatmap: Display the movement of various clients as a heatmap.

Figure 5: Heatmap



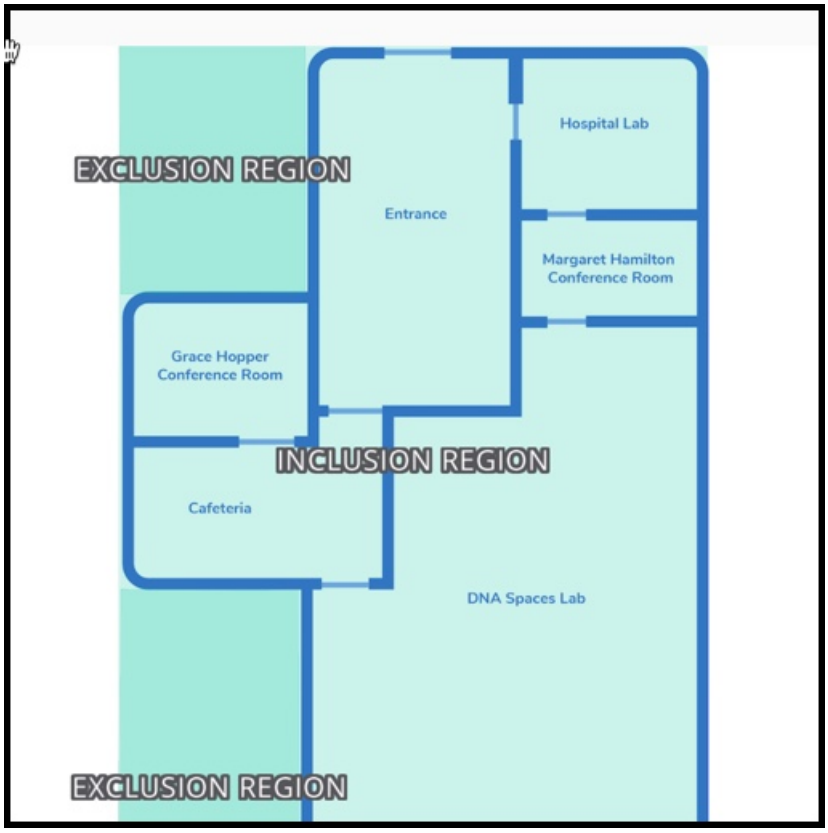
- Clustering: Enable clustering to group devices that are closely located and possibly overlapping. Click on the clustered icon to view list of devices in a separate window.

Figure 6: Clustering



- **Show/Hide Inclusion and Exclusion Regions:** Enables the display of inclusion and exclusion regions.

Figure 7: Show/Hide Inclusion and Exclusion Regions



Note

- Only one inclusion zone per floor is possible.
- You can add multiple exlusion zones per floor for areas where device tracking is unnecesary.

Create Zones

From the left navigation pane, click **Maps**, and browse to the location where you need to create a zone. Click the **Create a Zone** icon from the toolbar to the left and click on the map to create the zone boundaries. You can double-click to complete the creation of the zone. Add a name for the zone after placing it on the map. You can zoom into the zone and view it.

Figure 8: Create Zones