Cisco Spaces: Detect and Locate Configuration Guide

First Published: 2019-01-29

Last Modified: 2024-08-12

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Audience

This document is meant for Cisco Spaces network and IT administrators who deploy Cisco Spaces to monitor, manage, and optimize usage of assets in an organization.

Conventions

This document uses the following conventions.

Table 1: Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string. Otherwise, the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means the following information will help you solve a problem.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation

Cisco Spaces: Connector3 Configuration Guide

Cisco Spaces: Connector3 Command Reference Guide

Release Notes for Cisco Spaces: Connector

Cisco Spaces: IoT Service Configuration Guide (Wireless)

Cisco Spaces: IoT Service Configuration Guide (Wired)

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

PART I

Product Overview

CHAPTER 1

Product Overview

Note **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

Introduction to Cisco Spaces: Detect and Locate

Cisco Spaces: Detect and Locate enables you to view the current and historic location of Wi-Fi devices in your deployment.

Using Cisco Spaces: Detect and Locate, you can view the fixed physical layout of the buildings in your network and the Wi-Fi access points (APs) deployed in the building. You can see other fixed components such as GPS markers and Exclusion or Inclusion Zone for location calculation. Cisco Spaces: Detect and Locate also allows you to see the dynamic nature of the Wi-Fi devices in your network. You can view the calculated location of the following devices:

- Associated clients: Represented by a green dot ●. Includes information about the device from the Cisco AireOS Wireless Controller such as IP address and Manufacturer (when available). The history of when these devices were seen is also maintained.
- Unassociated clients: The location of these types of devices and their number is calculated on a best-effort basis and displayed.
- Tags: Active Radio-Frequency Identification (RFID) Wi-Fi tags. This information is displayed to help troubleshoot applications that use RFID tag data.
- BLE Tags: Bluetooth low energy data. This information is displayed to help troubleshoot applications that use the BLE tag data.
- Rogue Access Points: These are APs that the wireless controller detected and labeled as Rogue. The AP MAC address is displayed along with the estimated location.

- Rogue Clients: These are Wi-Fi clients that the wireless controller has detected and labeled as Rogue. The client MAC address is displayed along with the estimated location.
- Interferers: Any device that is not an AP or a wireless client, but still generate a radio frequency (RF) signal. For more information, see Detecting Interferers

Warning Web GL browser functionality is necessary to render maps on Cisco Spaces: Detect and Locate, and is enabled by default. Do not manually disable the Web GL functionality on your browser as this will prevent maps from rendering accurately.

Note These devices can change their MAC address and do not have a valid location history as long as they are not associated with the network.

Figure 1: Detect and Locate dashboard

Cisco Spaces tracks only active devices, defined as those sending a Wi-Fi probe packet at intervals of five minutes or less. The frequency of probe sending is determined by the device, making it unpredictable.

You cannot directly compare client counts between Cisco Spaces and the wireless controller due to differences in their designs. Both the wireless controller and Cisco Catalyst Center regard associated devices as active. Associated devices are simply connected to the network. Since Cisco Catalyst Center relies on Cisco Spaces for device locations, it shows such devices as un-positioned.

You cannot directly compare client counts (both associated and probing) between Cisco Spaces and the Wireless Controller due to differences in their designs. Both the Wireless Controller and Catalyst Center consider associated devices as active. Associated devices are devices that are merely associated to the network. Since Catalyst Center relies on Cisco Spaces for device locations, it shows such devices as un-positioned.

Linking of a Cisco CMX device to Cisco Spaces is a design that should be used to help a customer transition to Cisco Spaces(Tethering). This allows a customer an initial view of how devices are displayed on Cisco Spaces. However, device counts on Cisco CMX andCisco Spaces should not be compared. For tethered devices, perform accuracy troubleshooting on Cisco CMX.

The Wireless Controller does not require active devices to probe continuously. In contrast, Cisco Spaces requires a probe frequency of five minutes or less. Therefore, devices shown as active on the Wireless Controller might not appear on Cisco Spaces. These are termed non-locatable devices.

Devices may be listed as missing on Cisco Spaces for the following reasons:

- The device is reported by an AP that is not placed on the map. If many APs connected to the Wireless Controller are not on the map, the devices they report will be missing
- Associated clients probe less frequently to conserve battery, affecting the accuracy of location. They do not probe when in ultra-power reserve mode (sleeping mode and screen blanked out). Cisco Spaces cannot locate devices in this inactive state. Once the user activates the device (unlocks screen, starts streaming), it resumes sending probes to the network.
- Cisco Spaces expects Wi-Fi devices to send regular Wi-Fi probe packet updates to ensure that the device status is active. However, some devices are considered active by the Wireless Controller although they are not sending Wi-Fi probes, and such devices are considered as non-locatable devices

- Cisco Spaces requires regular Wi-Fi probe updates to maintain active device status. Some devices may be considered active by the wireless controller even without sending Wi-Fi probes, making them non-locatable on Cisco Spaces.

For more information about the open source used in Cisco Spaces: Detect and Locate, see:

Open Source Documentation.

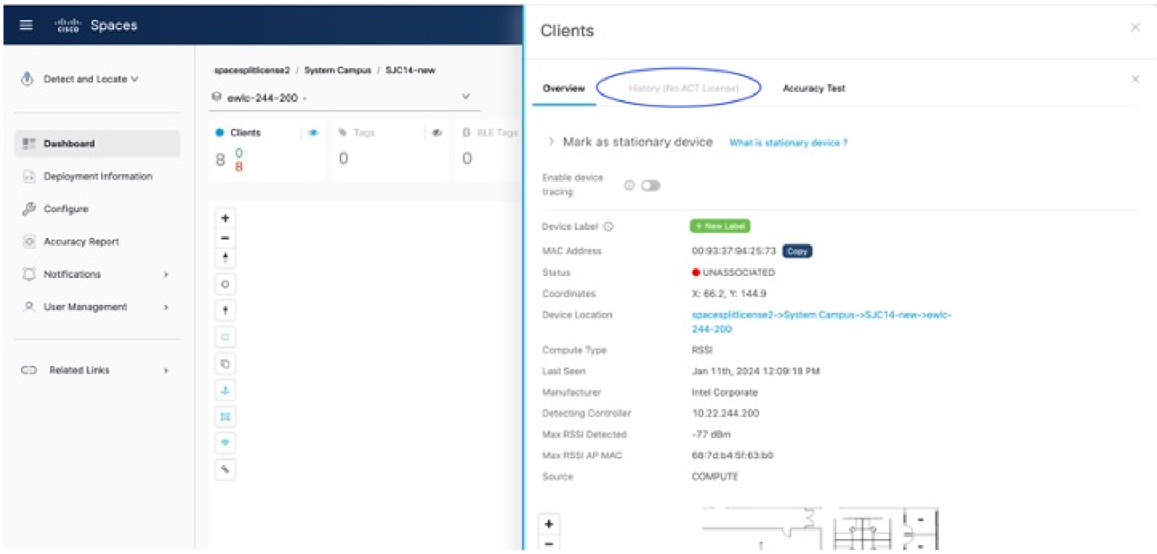
Licensing

Cisco Spaces: Detect and Locate is included in the Cisco Spaces ACT license

There are six types of licenses for Cisco Spaces users (see table below), and the type of license held by a Cisco Spaces user affects the following areas on Cisco Spaces: Detect and Locate:

- Device history: Device history is supported only by UNLIMTED and ACT license. You can observe device history on the detailed information page that opens when clicking a device (See History Tab, on page 42). If you do not have the required license, the **History** tab is disabled.

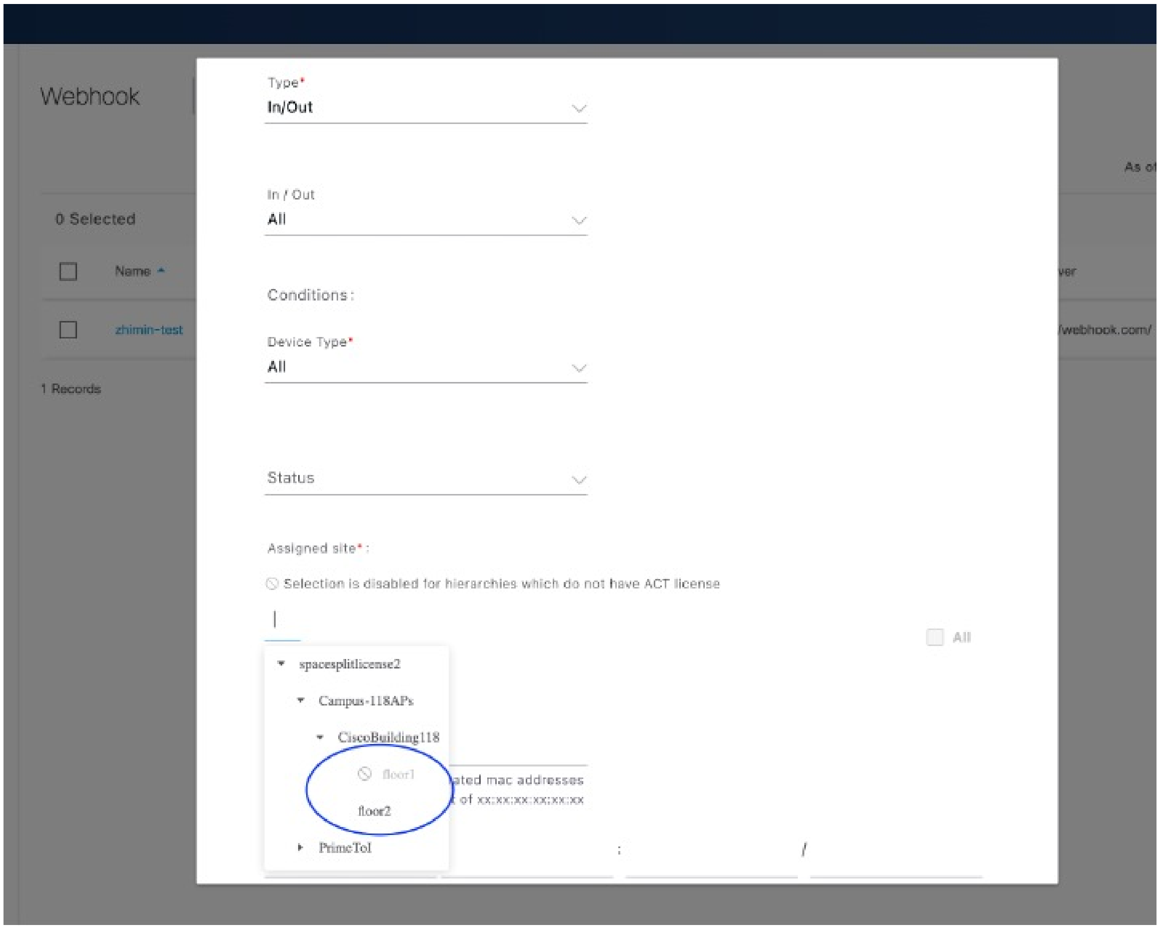
  Figure 2: Disabled Device History



Device Label	
MAC Address	00:93:37:94:25:73
Status	UNASSOCIATED
Coordinates	X: 66.2, Y: 144.9
Device Location	spacesplitlicense2->System Campus->SJC14-new->ewlc-244-200
Compute Type	RSSI
Last Seen	Jan 11th, 2024 12:09:18 PM
Manufacturer	Intel Corporate
Detecting Controller	10.22.244.200
Max RSSI Detected	-77 dBm
Max RSSI AP MAC	68:7d:b4:5f:63:b0
Source	COMPUTE

- Webhook creation: When attempting to add a new webhook in the Cisco Spaces dashboard left navigation pane (**Notifications** > **Webhooks**), the **Assigned Sites** section is disabled for heirarches that are not under the **UNLIMITED** or **ACT** license.

Figure 3: Webhook Disabled in the Assigned Site Selection



Type*
In/Out

In / Out
All

Conditions :

Device Type*
All

Status

Assigned site* :

⃠ Selection is disabled for hierarchies which do not have ACT license

□ All

- spacesplitlicense2
  - Campus-118APs
    - CiscoBuilding118
      - ⃠ floor1
      - floor2
  - PrimeTol

Table 2: License Type and Features They Affect

License Type	Device History Available	Webhook Creation
UNLIMITED	YES	YES
ACT	YES	YES
SMART_OPERATIONS	YES	YES
SMART_VENUES	NO	NO
EXTEND	NO	NO
SEE	NO	NO

PART II

Getting Started

CHAPTER 2

Setup

Onboard To Cisco Spaces

This procedure has to be done only once for your account. Do not repeat it for every Cisco Spaces app. Ignore if you have completed the procedure already.

Step 1 Request an account on Cisco Spaces by sending an email to spaces@cisco.com requesting for a demo or live account creation on the Cisco Spaces dashboard. For more information, see Getting Started with Spaces Dashboard.

Step 2 Accept the invitation from Cisco Spaces and setup your password.

Step 3 Onboard your wireless network on Cisco Spaces. See Setup Guide.

Step 4 Setup your location heirarchy. See Best Practices.

Setup

test

CHAPTER 3

Data Source

Configuring Location Data Source

Configuring Location Data Source

You can configure any of the following as a source for location data:

- Cisco Spaces Connector Configuration. Refer to Cisco DNA Spaces Connector Configuration Guide
- Cisco AireOS Wireless Controller configuration: You can configure the Detect and Locate using wireless controller as data source. For more information, see **Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco DNA Spaces**
- Cisco CMX tethering: With the Cisco CMX as a data source, location computation for wireless devices is calculated using Cisco CMX. Cisco Spaces: Detect and Locate displays wireless clients and tags.

PART III

Deployment Information

Deployment Information

From the **Cisco Spaces: Detect and Locate > Deployment Information** window, you can get an overview of the deployment across several floors and controllers. You can now view the following information:

- Active Access Points (APs)
- Inactive APs
- APs connected to wireless controller
- APs you have placed on the uploaded map.

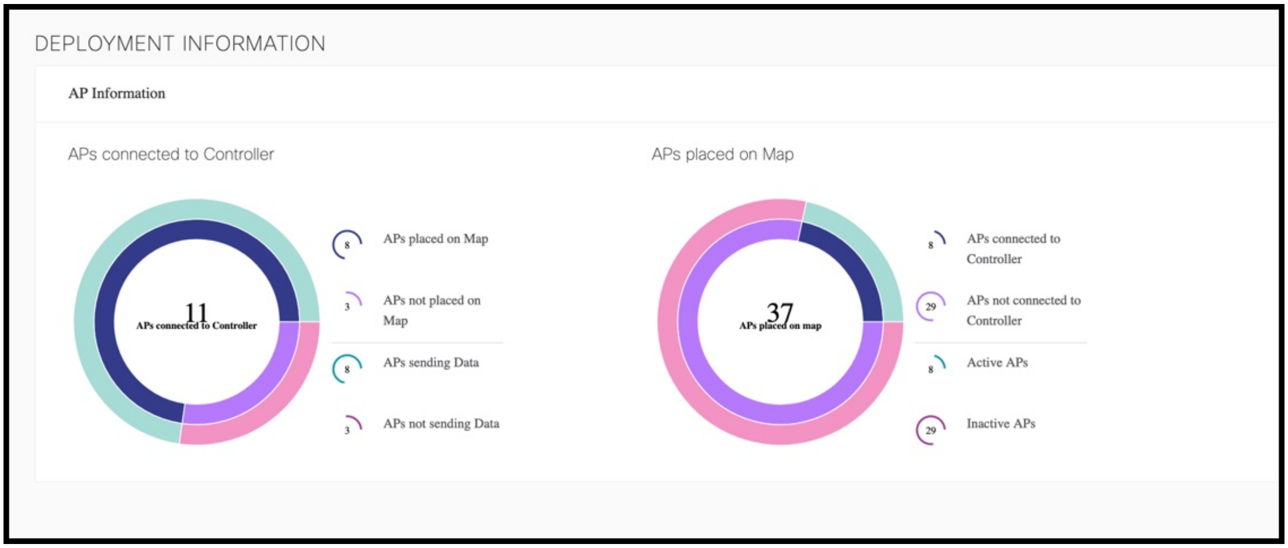
There are two graphs displayed on the **Deployment Information** page. One graph contains information collected from the wireless controller and the other contains the same information collected from the Cisco Spaces maps. You can now compare the information in the two graphs and check if the information is the same.

From the following image, you can observe the **APs connected to Controller** graph which provides information about the wireless controller. This graph indicates that while 11 APs are connected to the wireless controller, only eight are actually sending data to the wireless controller. Three APs are not sending any data to the wireless controller. The graph also shows that three APs are not placed on the Cisco Spaces maps. Finally, the graph indicates that eight APs are placed on the Cisco Spaces map.

From the following image, you can also observe the **APs placed on Map** graph. This graph displays information about the Cisco Spaces maps. The graph shows that there are 37 APs on the Cisco Spaces maps. This number includes access points that are active, inactive, and stale. Out of this, eight APs are connected to the wireless controller and 29 are not connected to any wireless controller, although they are present on the Cisco Spaces maps.

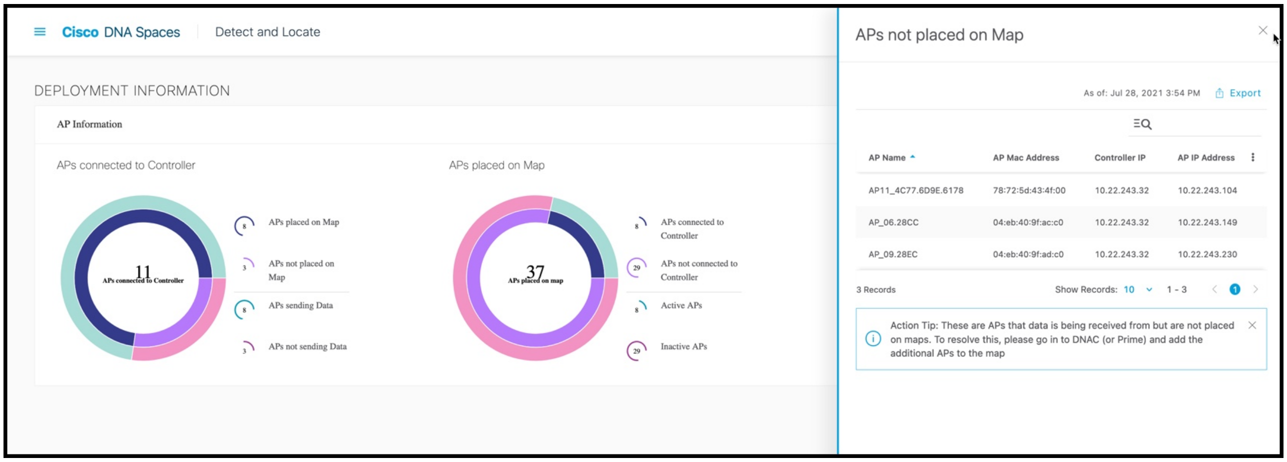
You can also identify which APs are inactive and why they are inactive. Inactive APs are placed on the Cisco Spaces map, but do not report the data they receive. Data is not reported because the APs are either not connected to the wireless controller or they are connected but not sending the measured data. You can find the specifics of this information by cross-checking with the graphs. In the following image, observe the **APs placed on Map** section, and observe that 29 APs are inactive (**Inactive APs**) and 29 APs are not connected to the wireless controller (**APs not connected to the wireless controller**).

Figure 4: Inactive APs, APs Not Connected to Wireless Controller



Click each metric to see a detailed list of APs.

Figure 5: Detailed List of APs



APs not placed on Map

As of: Jul 28, 2021 3:54 PM

AP Name	AP Mac Address	Controller IP	AP IP Address
AP11_4C77.6D9E.6178	78:72:5d:43:4f:00	10.22.243.32	10.22.243.104
AP_06.28CC	04:eb:40:9f:ac:c0	10.22.243.32	10.22.243.149
AP_09.28EC	04:eb:40:9f:ad:c0	10.22.243.32	10.22.243.230

3 Records

Action Tip: These are APs that data is being received from but are not placed on maps. To resolve this, please go in to DNAC (or Prime) and add the additional APs to the map

PART IV

Setup

CHAPTER 4

Explore Heirarchy

View Map Heirarchy on Detect and Locate

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.

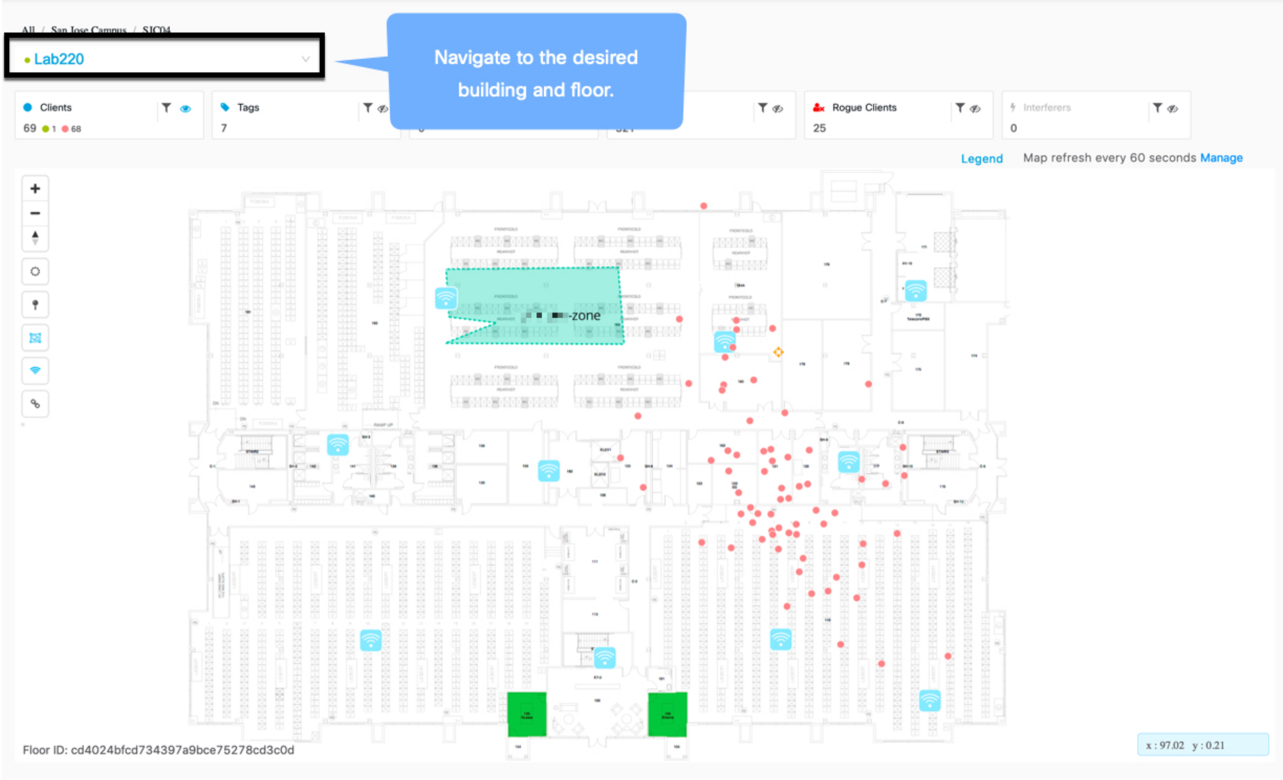
Step 3 Browse to the location where the maps are stored (on your computer). Select the maps that were previously exported from Cisco Prime Infrastructure.

Step 4 Verify if the maps are uploaded successfully.

Viewing the Map on Cisco Spaces: Detect and Locate

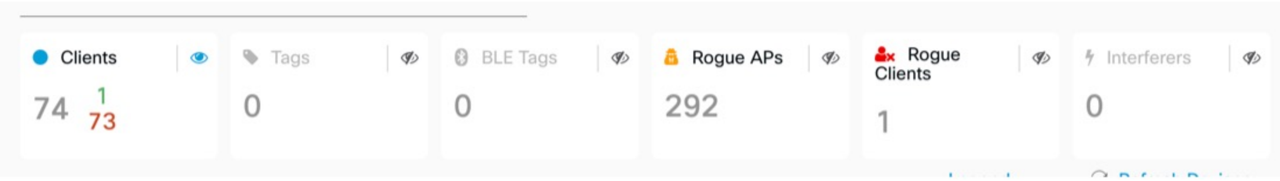
Step 1 From the Cisco Spaces: Detect and Locate dashboard, use the drop-down list to navigate to the desired campus, building, and floor.

Figure 6: Cisco Spaces: Detect and Locate Dashboard


All / San Jose Campus / SJC04
Lab220
Navigate to the desired building and floor.
Clients
69 ● 1 ● 68
Tags
7
Rogue Clients
25
Interferers
0
Legend
Map refresh every 60 seconds Manage
-zone
Floor ID: cd4024bfcd734397a9bce75278cd3c0d
x : 97.02 y : 0.21

Step 2 From the toolbar on the top, choose any combination of the icons to customize your view of the devices.

Figure 7: Dashboard: Total Count Toolbar



Clients	Tags	BLE Tags	Rogue APs	Rogue Clients	Interferers
74 1 73	0	0	292	1	0

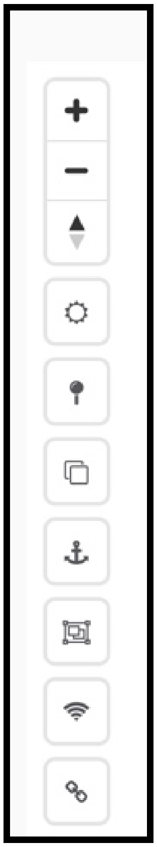
- Clients: All client devices (connected and detected).
  - A red dot 🔴 indicates probing clients. Click to see additional details about a client.
  - A dot associated with a number 4 indicates a cluster of probing clients. Click to view details of all the clients in that cluster. You can also zoom in 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 3 (Optional) Click the icon to filter the displayed items. These filters are persistent and across sessions.

Step 4 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.

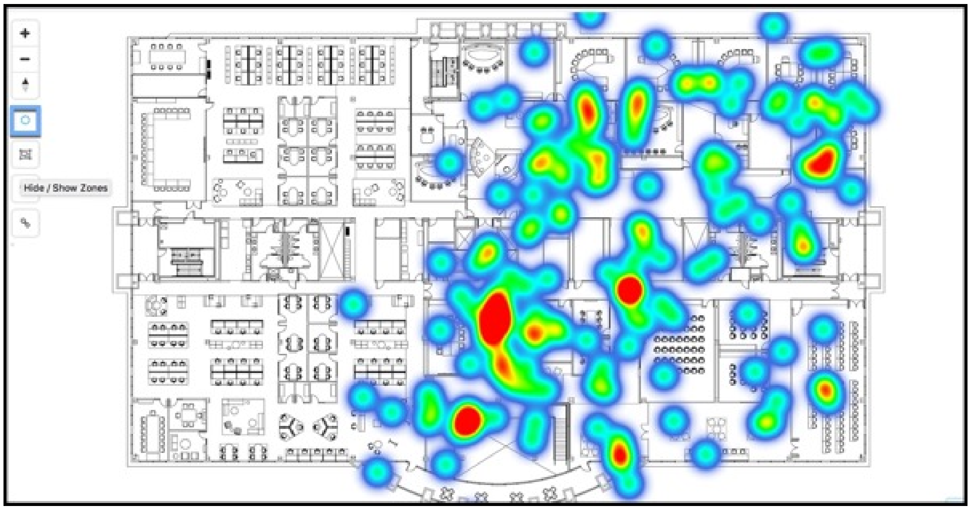
Figure 8: Dashboard: Left Toolbar



- 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 (AP) and which APs have issues with device location and hence may need troubleshooting.(No AP heatmap available)

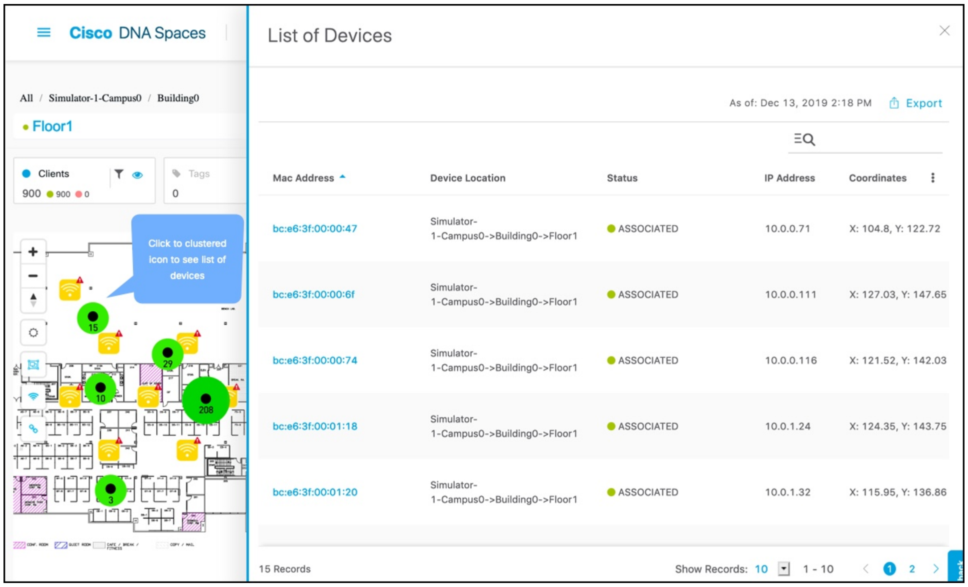
- Heatmap: Display the movement of various clients as a heatmap.

Figure 9: 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 10: Clustering


Cisco DNA Spaces
All / Simulator-1-Campus0 / Building0
Floor1
Clients
900 900 0
Tags
0
Click to clustered icon to see list of devices
15
29
10
208
3

List of Devices

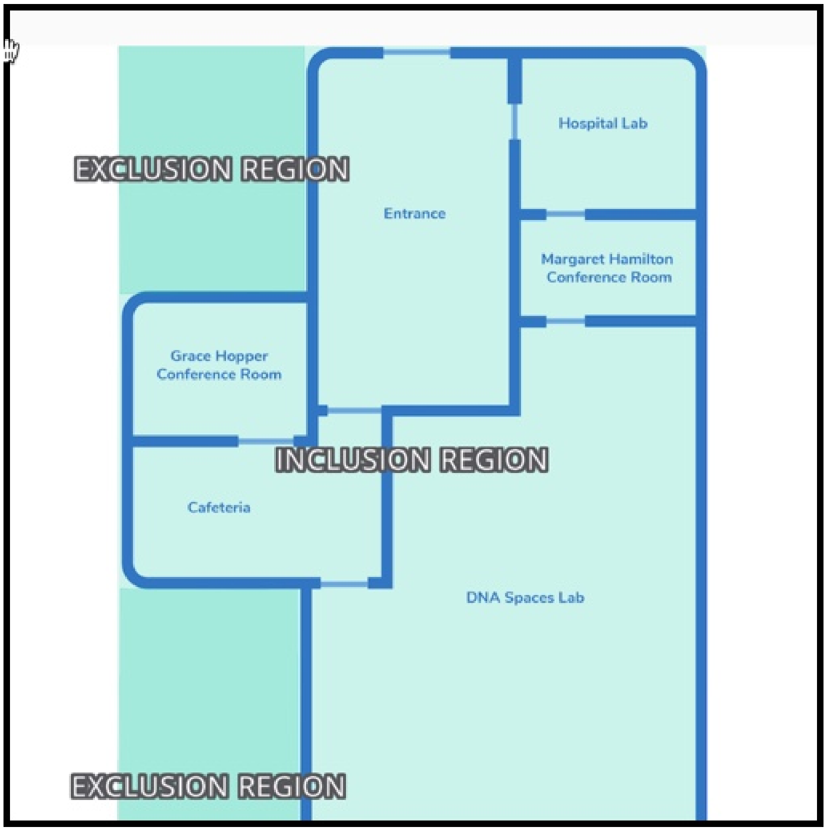
As of: Dec 13, 2019 2:18 PM Export

Mac Address	Device Location	Status	IP Address	Coordinates
bc:e6:3f:00:00:47	Simulator-1-Campus0->Building0->Floor1	● ASSOCIATED	10.0.0.71	X: 104.8, Y: 122.72
bc:e6:3f:00:00:6f	Simulator-1-Campus0->Building0->Floor1	● ASSOCIATED	10.0.0.111	X: 127.03, Y: 147.65
bc:e6:3f:00:00:74	Simulator-1-Campus0->Building0->Floor1	● ASSOCIATED	10.0.0.116	X: 121.52, Y: 142.03
bc:e6:3f:00:01:18	Simulator-1-Campus0->Building0->Floor1	● ASSOCIATED	10.0.1.24	X: 124.35, Y: 143.75
bc:e6:3f:00:01:20	Simulator-1-Campus0->Building0->Floor1	● ASSOCIATED	10.0.1.32	X: 115.95, Y: 136.86

15 Records Show Records: 10 1 - 10 1 2

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

Figure 11: Show/Hide Inclusion and Exclusion Regions



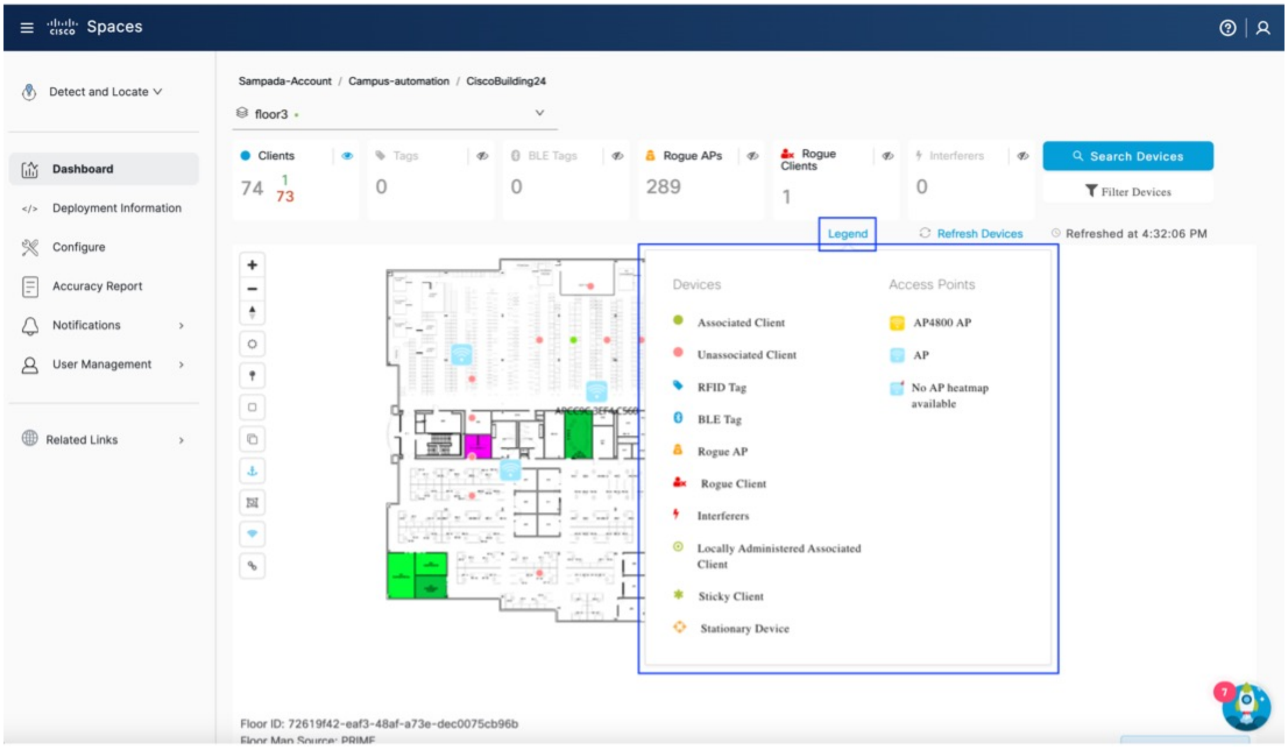
Note

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

Understand the Map Legend

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

Figure 12: Understand the Map Legend

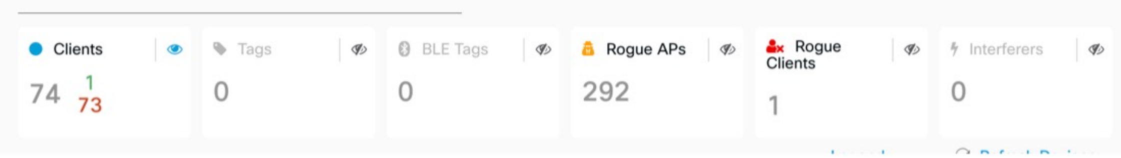


- A green dot ● indicates connected clients. Click to see additional details of a client.
- A red dot ● indicates probing clients. Click to see additional details about a client.
- A dot associated with a number ● indicates a cluster of probing clients. Click to view details of all the clients in that cluster. You can also zoom in to view the clients individually.
- Locally Administered Associated Client
- Sticky Client
- Stationary Device

Customize the Devices Viewed

The toolbar on the top lists the various types of devices. A device is represented by a name, icon, and a corresponding number that indicates the number of such devices on your network. Use the 👁 icon beside each device to show or hide a particular type of device, so that you customize your view of the devices.

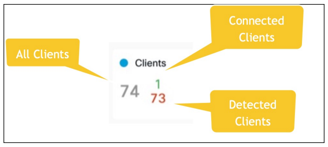
Figure 13: Device Toolbar: Show or Hide Various Devices



The devices represented on this toolbar are described below:

- Clients: All client devices. You can see the breakdown of this number into connected and detected devices.

  Figure 14: Connected and Detected Devices

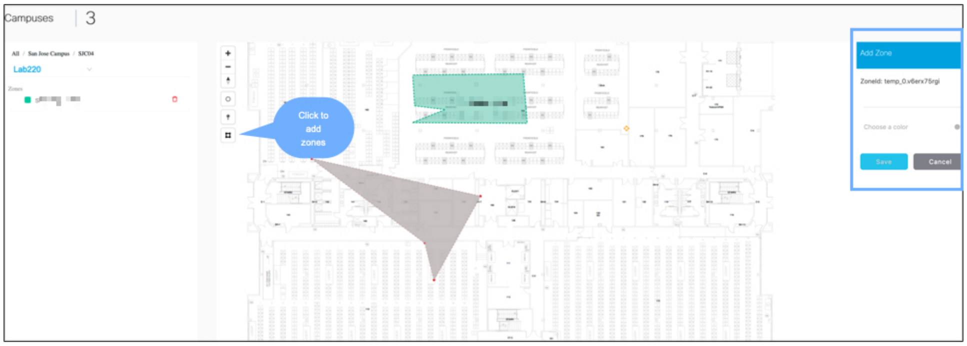
  

- Tags: Vendor-specific information that is related to Wi-Fi tags are displayed in raw format.
- BLE Tags: Bluetooth Low Energy tags attached to track devices.
- Rogue APs: APs that are not part of or managed by the Cisco CMX infrastructure. Click to see additional details.
- Rogue Clients: Clients that are connected to rogue access points.
- Interferers: Devices that can create a radio frequency interference. .

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 15: Create Zones



CHAPTER 5

Customize Your Dashboard Using Filters

Customize Your Dashboard with Filters

Detect and Locate aggregates and displays various devices in your network, such as clients, tags, BLE tags, and interferes. If the number of such devices is large, you maybe unable to focus on devices that are of specific interest to you.

Filters are a feature of the Detect and Locate workspace. Filters allow you to control the visibility of devices on the Detect and Locate dashboard. This allows you to focus your attention on devices that are of interest to you. You can see that the device count displayed on the toolbar on the top of the dashboard also changes according to the criteria you have specified.

You can configure filters, and set them up at various levels of your location hierarchy. Your filters can be applicable throughout your network (referred to as the global level) or at a specific floor or building (referred to as a hierarchical level)

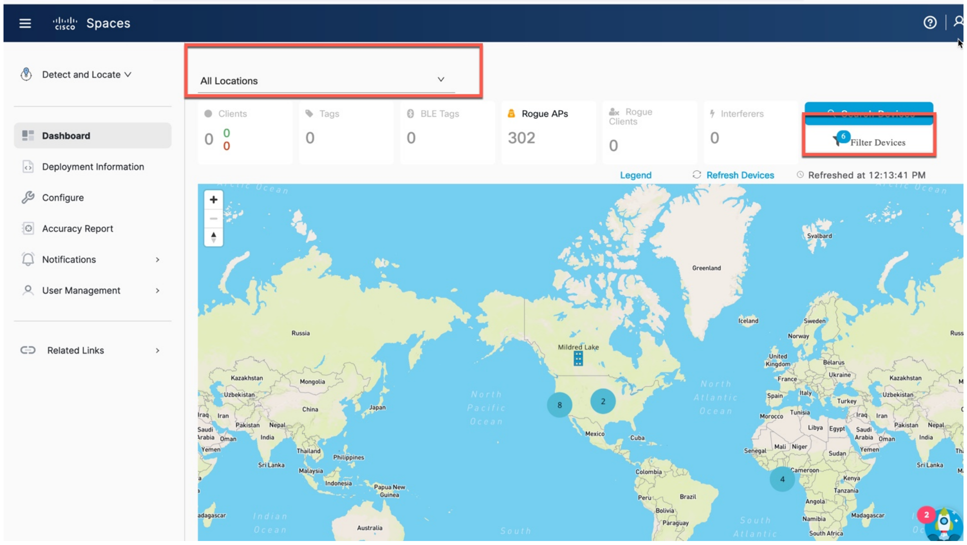
Filter configurations are unique to each user. This means that your filter remains in place even after you log out and log back in. Detect and Locate does not remove your filters unless you delete them manually.

Set Up the Filter

This procedure shows you how to customize the devices that appear on your dashboard using filters.

Step 1 From the Detect and Locate dashboard, navigate to the desired location.

Figure 16: Navigate to the Desired Location



Step 2 Locate the **Filter Devices** button on the dashboard.

Step 3 Specify the conditions of this filter, and then click **Filter**.

Figure 17: Specify the Filter Conditions

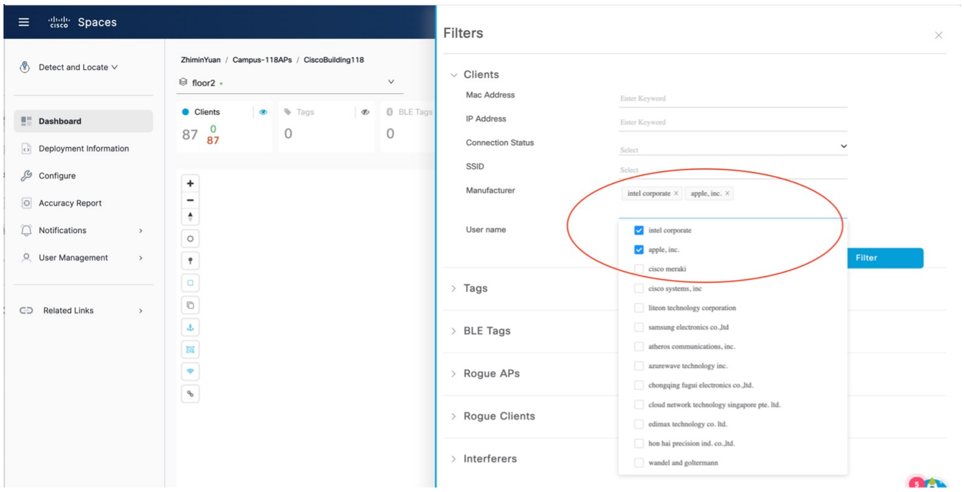
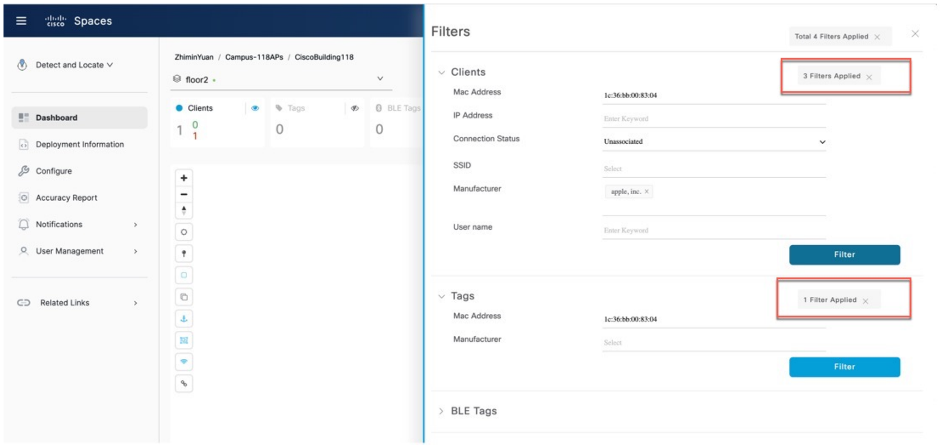


Figure 18: View All Configured Filters



Filters

Total 4 Filters Applied ×

Clients — 3 Filters Applied ×

Mac Address	1c:36:bb:00:83:04
IP Address	Enter Keyword
Connection Status	Unassociated
SSID	Select
Manufacturer	apple, inc. ×
User name	Enter Keyword

Tags — 1 Filter Applied ×

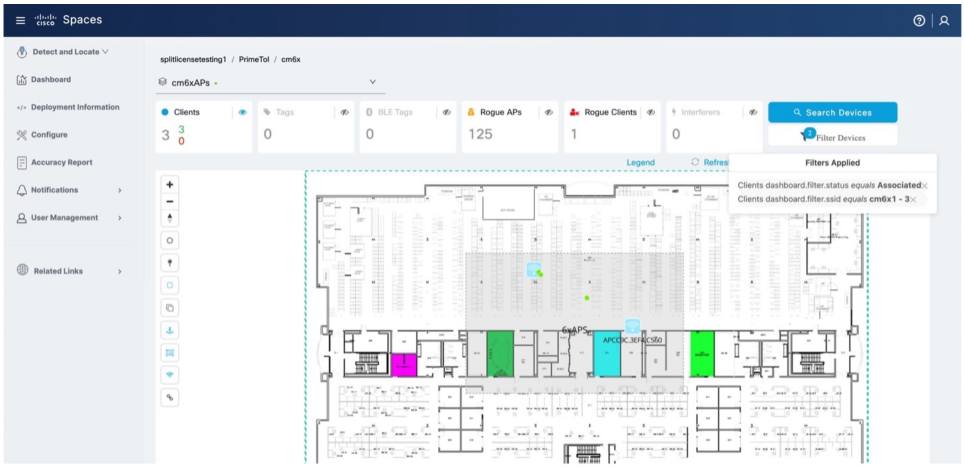
Mac Address	1c:36:bb:00:83:04
Manufacturer	Select

In the same **Filters** window, you can now see the configured filters on the top right of each category. A total of all the filters also appears on the top right.

You can remove a filter by clicking the "X" next to the filter text.

The filter counts are also visible on the dashboard. You can see them on the **Filter Devices** button.

Figure 19: Filter Count on the Filter Devices Button



Filters Applied

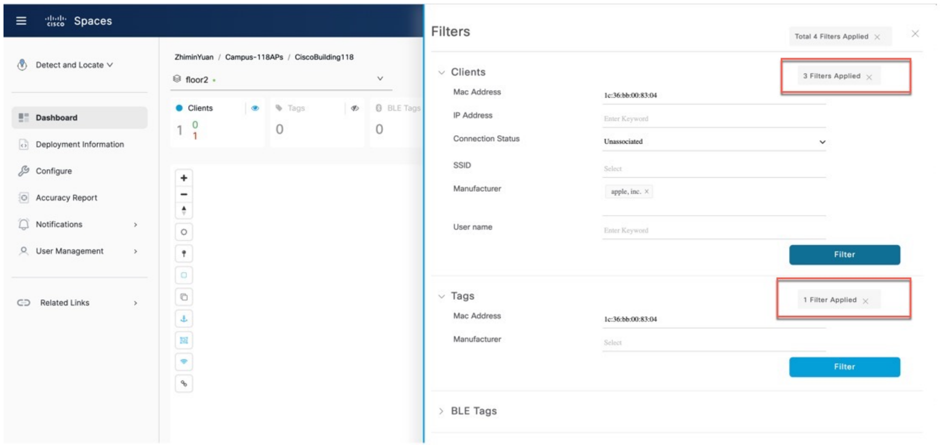
Clients dashboard.filter.status *equals* **Associated** ×

Clients dashboard.filter.ssid *equals* **cm6x1 - 3** ×

Using Multiple Device Filters for Multiple Conditions

Each condition requires a filter. To incorporate multiple conditions, you must create several filters. These filters operate collectively, necessitating that all established conditions be met for the search to become more precise.

Figure 20: Configuring Multiple Conditions with Multiple Filters



Filters

Total 4 Filters Applied ×

Clients — 3 Filters Applied ×

Mac Address: 1c:36:bb:00:83:04
IP Address: Enter Keyword
Connection Status: Unassociated
SSID: Select
Manufacturer: apple, inc. ×
User name: Enter Keyword

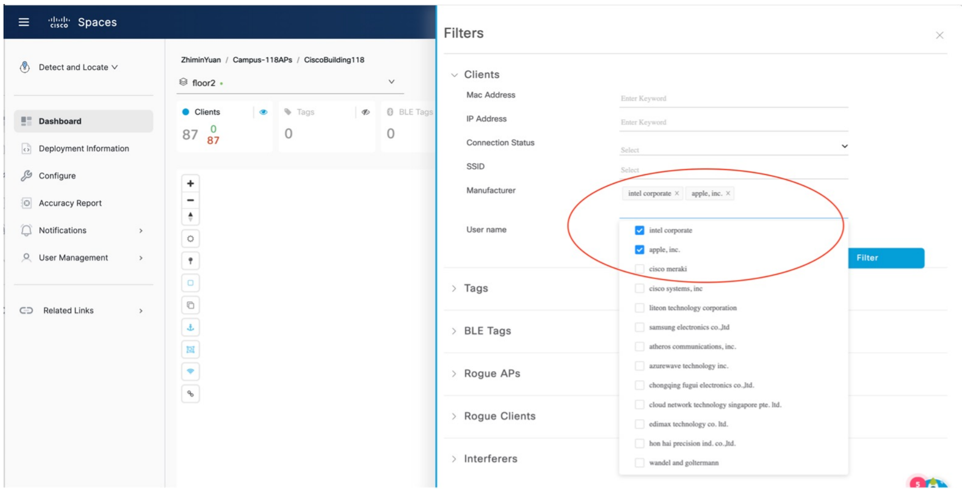
Tags — 1 Filter Applied ×

Mac Address: 1c:36:bb:00:83:04
Manufacturer: Select

Filter Condition Dropdown Menu

The **Filters** window offers drop-down menus for specific conditions. You can see the options available at the chosen hierarchy level. Certain conditions, such as **Service Set Identifier (SSID)** and **Connection Status** permit only one selection. Others, like **Manufacturer**, allow for multiple selections. This means that once you choose an option such as **Manufacturer** as one of your multiple choices, the search results will display the device's manufacturer details.

Figure 21: Filter Conditions Dropdown Menu



Filters

Clients

Mac Address: Enter Keyword
IP Address: Enter Keyword
Connection Status: Select
SSID: Select
Manufacturer: intel corporate × apple, inc. ×
User name

- ☑ intel corporate
- ☑ apple, inc.
- □ cisco meraki
- □ cisco systems, inc
- □ liteon technology corporation
- □ samsung electronics co.,ltd
- □ atheros communications, inc.
- □ azurewave technology inc.
- □ chongqing fugui electronics co.,ltd.
- □ cloud network technology singapore pte. ltd.
- □ edimax technology co. ltd.
- □ hon hai precision ind. co.,ltd.
- □ wandel and goltermann

Understanding Filtering by SSID

Networks with multiple SSIDs are often differentiated by suffixes such as _1, _2. You can filter SSIDs by specifying these suffixes. This can help in troubleshooting network issues.

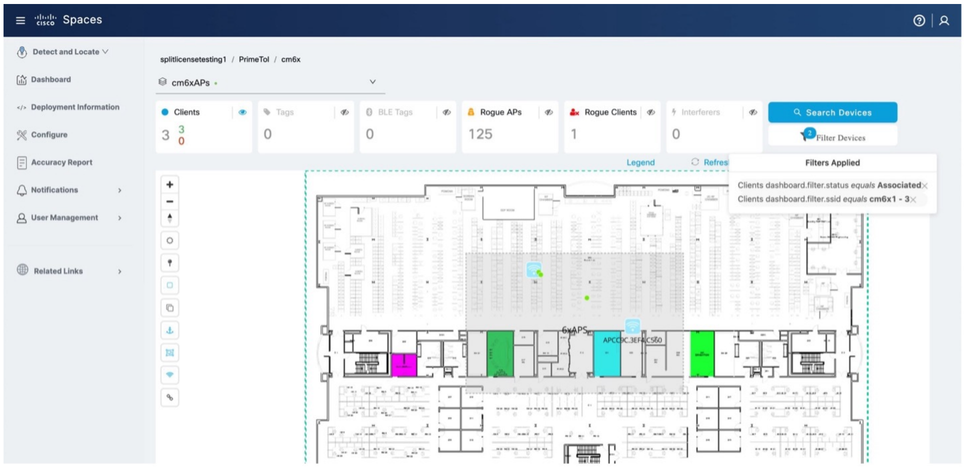
Filter Effect on the Dashboard

When you apply a filter, the following gets modified:

- the number displayed on the Device toolbar, and
- the device icons on the map within the dashboard. Only device icons that meet the filter criteria are visible.

When you hover over the **Filter Devices** button, a popup appears displaying the active filter.

Figure 22: Effect of Filter on the Dashboard



Filters Applied

Clients dashboard.filter.status *equals* **Associated**

Clients dashboard.filter.ssid *equals* **cm6x1 - 3**

CHAPTER 6

Sticky Clients

Sticky Clients

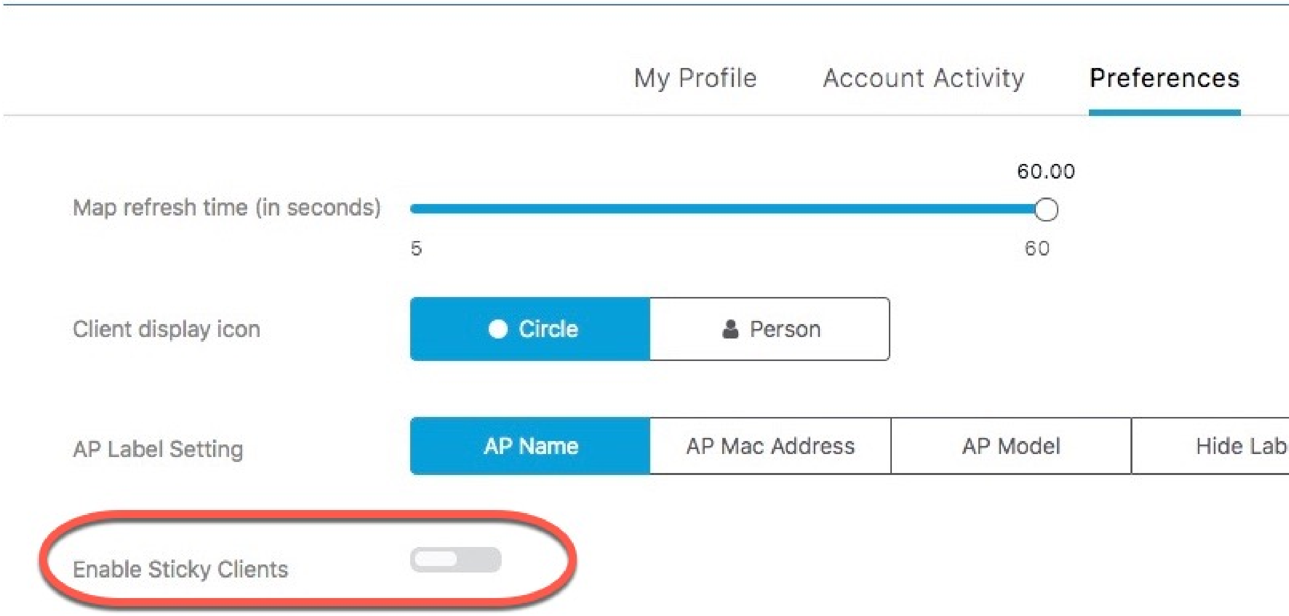
Usually, an associated client is in closest proximity of the access point it is connected to, in comparision to other APs in the vicinity. However, there could be instances where the device connects to an access point, and moves into the range of another access point and does not change its association to the other closer AP. Such a client is referred to as a sticky client.

For example, a user enters the first floor and connects to the access point on the same floor. The user moves to the third floor, where he continues to stay. While you may expect the connected AP to change to the third floor for that device, if it doesn't, then this referred to as a sticky client as the roaming pattern is not reflected because of their stickiness to APs that are at a greater distance.

This information about sticky clients is obtained from the controller and is not computed by Cisco Spaces. When Cisco Spaces tags a client as sticky, there is no difference in the way the device is processed. Cisco Spaces continues to receive messages from the controller and reflects the state of the device accordingly. On the Cisco Spaces: Detect and Locate UI, the associated clients displayed in green star icon are sticky clients.

This feature is disabled by default. To enable this feature, on the Cisco Spaces: Detect and Locate UI, click on the profile icon in the top-right corner, and click **Preferences**. Then click **Enable Sticky Clients**.

Figure 23: Enable Sticky Clients



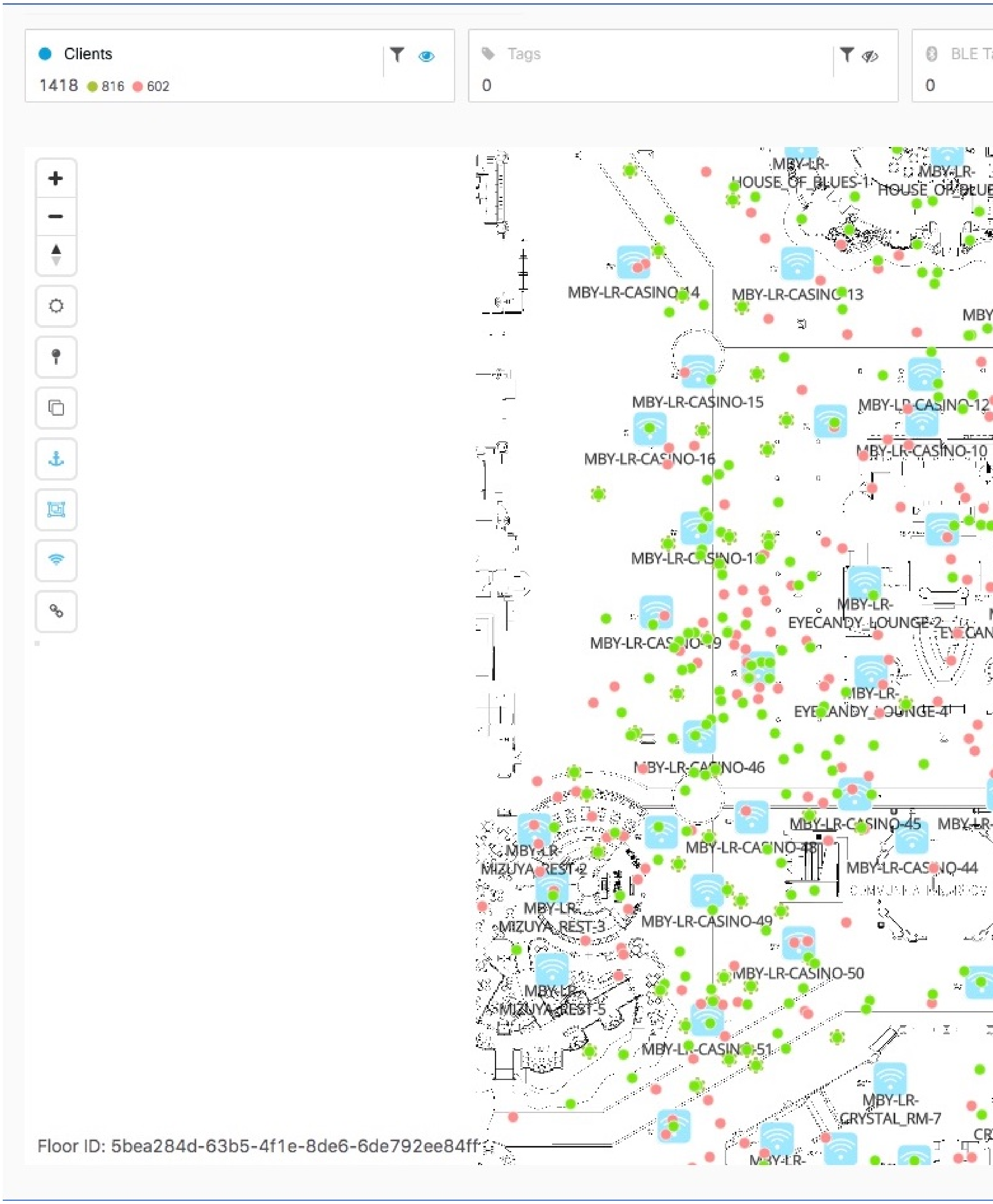
Map refresh time (in seconds) 60.00 (5 – 60)

Client display icon: [✓ Circle] Person

AP Label Setting: [✓ AP Name] AP Mac Address AP Model Hide Lab

Enable Sticky Clients ○

Figure 24: Sticky Clients Displayed As Green Star Icon



Clients
1418 ● 816 ● 602

Tags
0

BLE Ta
0

Floor ID: 5bea284d-63b5-4f1e-8de6-6de792ee84ff

CHAPTER 7

Global Search

Global Search in Detect and Locate

Cisco Spaces: Detect and Locate aggregates and displays various devices in your network. These devices are clients, tags, Bluetooth Low Energy (BLE) tags, and interferers.

You can search for these devices using global search on Cisco Spaces: Detect and Locate.

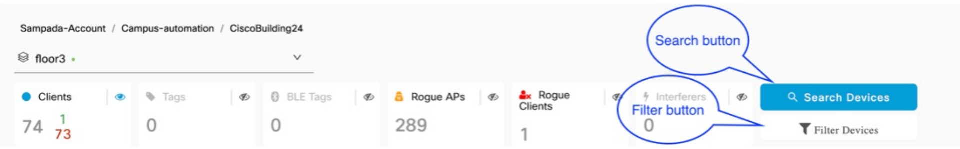
The article covers various aspects of the global search process, including

- initiating searches
- managing search results, and
- handling scenarios with no results.

Search Your Assets

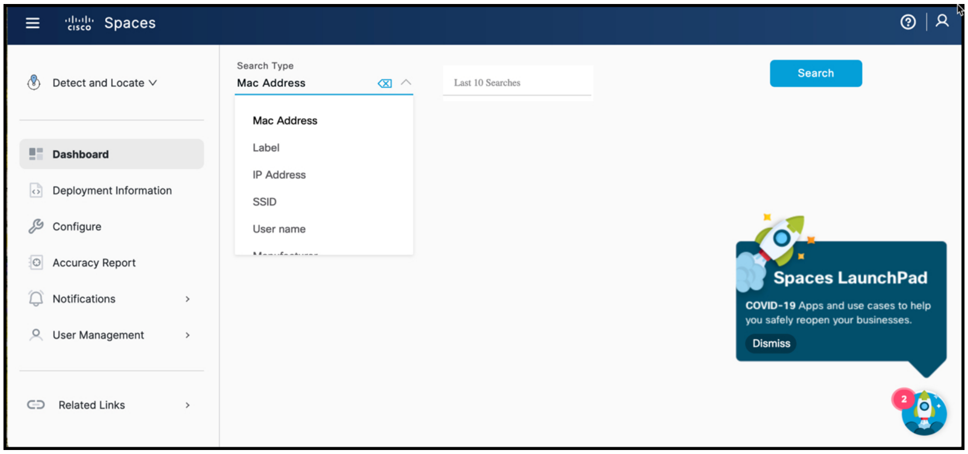
Search your assets by clicking the **Search Devices** button as shown in the image.

Figure 25: Search Devices Button



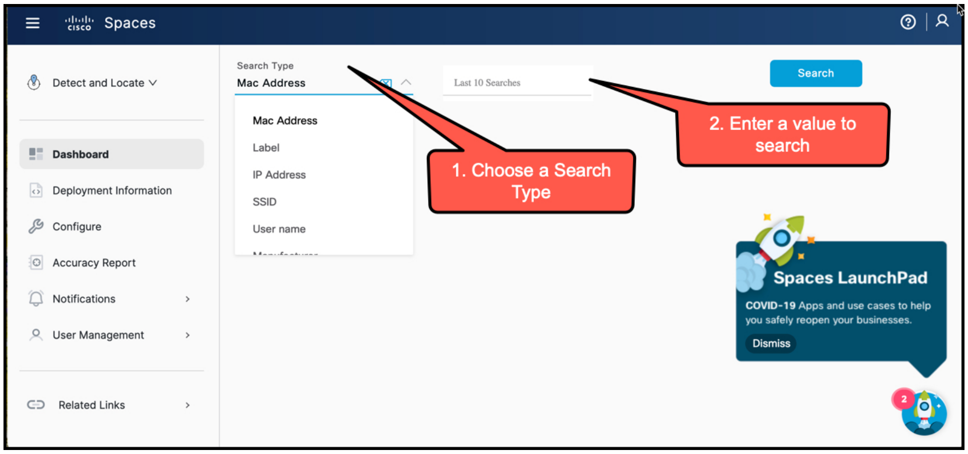
In the window that opens, you can search all assets tracked by your Cisco Spaces: Detect and Locate account.

Figure 26: Search Your Assets



Choose from the **Search Type** drop-down list and enter a value in the text field beside it.

Figure 27: Search Your Assets



1. Choose a Search Type

2. Enter a value to search

You can search based on

1. MAC Address
2. Label
3. IP Address
4. SSID
5. Username, or
6. Manufacturer.

Search Rules For Each Search Types

The global search applies different rules to each search type:

1. **Exact matching** is supported only for the **Label** search. For other search types, fuzzy matching is supported.
2. **Format verification** is supported for MAC address and IP address searches. If your input values contain illegal characters or an incorrect format, you can see alerts to warn you.

The table describes each search type and the applicable search rules.

Table 3: Global Search Rules

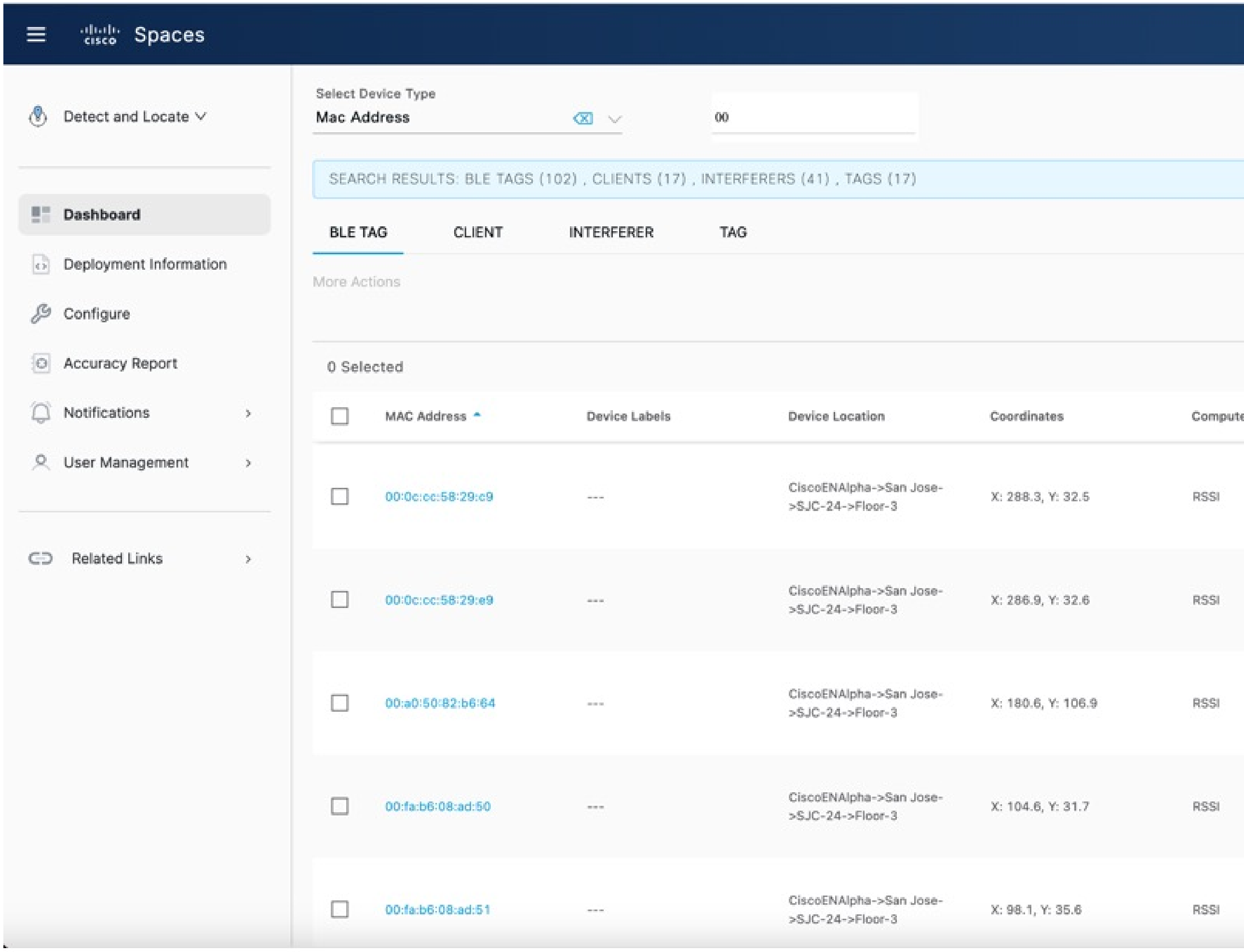
Search By	Matching Type Support	Format Verification
MAC Address	Fuzzy	YES
Label	Absolute	NO
IP Address	Fuzzy	YES for IPv4
SSID	Fuzzy	NO
Username	Fuzzy	NO
Manufacturer	Fuzzy	NO

Search Results

Search results are organized into different tabs by device type, such as BLE TAG, CLIENT, and INTERFERER. Only those device types that are included in the search results appear as tabs. If there is only one device in the search results, you can see detailed information of that device in your results.

To view detailed information of a device present in your search results, click on the device's MAC Address.

Figure 28: Search Results Organized by Device-Type Tabs



Select Device Type: Mac Address

00

SEARCH RESULTS: BLE TAGS (102) , CLIENTS (17) , INTERFERERS (41) , TAGS (17)

0 Selected

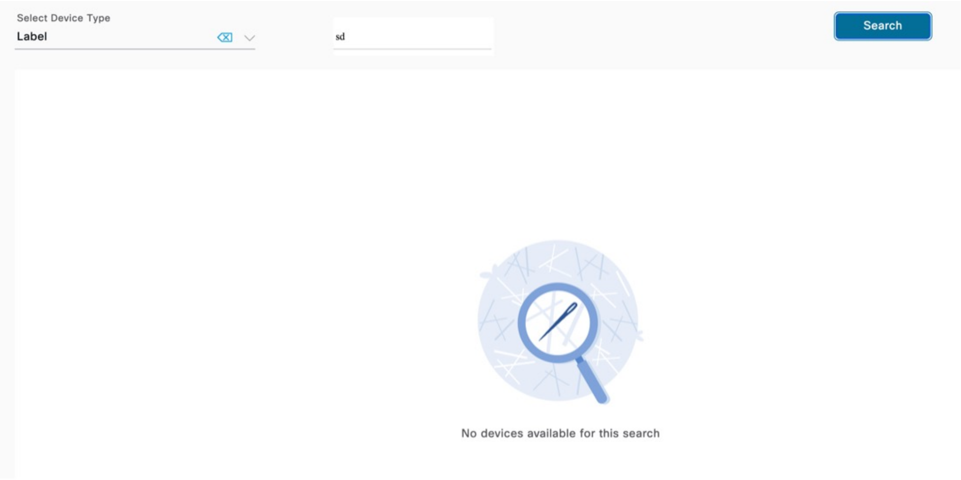
□	MAC Address	Device Labels	Device Location	Coordinates	Compute
□	00:0c:cc:58:29:c9	---	CiscoENAlpha->San Jose->SJC-24->Floor-3	X: 288.3, Y: 32.5	RSSI
□	00:0c:cc:58:29:e9	---	CiscoENAlpha->San Jose->SJC-24->Floor-3	X: 286.9, Y: 32.6	RSSI
□	00:a0:50:82:b6:64	---	CiscoENAlpha->San Jose->SJC-24->Floor-3	X: 180.6, Y: 106.9	RSSI
□	00:fa:b6:08:ad:50	---	CiscoENAlpha->San Jose->SJC-24->Floor-3	X: 104.6, Y: 31.7	RSSI
□	00:fa:b6:08:ad:51	---	CiscoENAlpha->San Jose->SJC-24->Floor-3	X: 98.1, Y: 35.6	RSSI

No Result Cases

If your search returns no results, you can see the *No device available for this search* message.

MAC address searches are an exception to this rule.

Figure 29: No Search Results Scenario



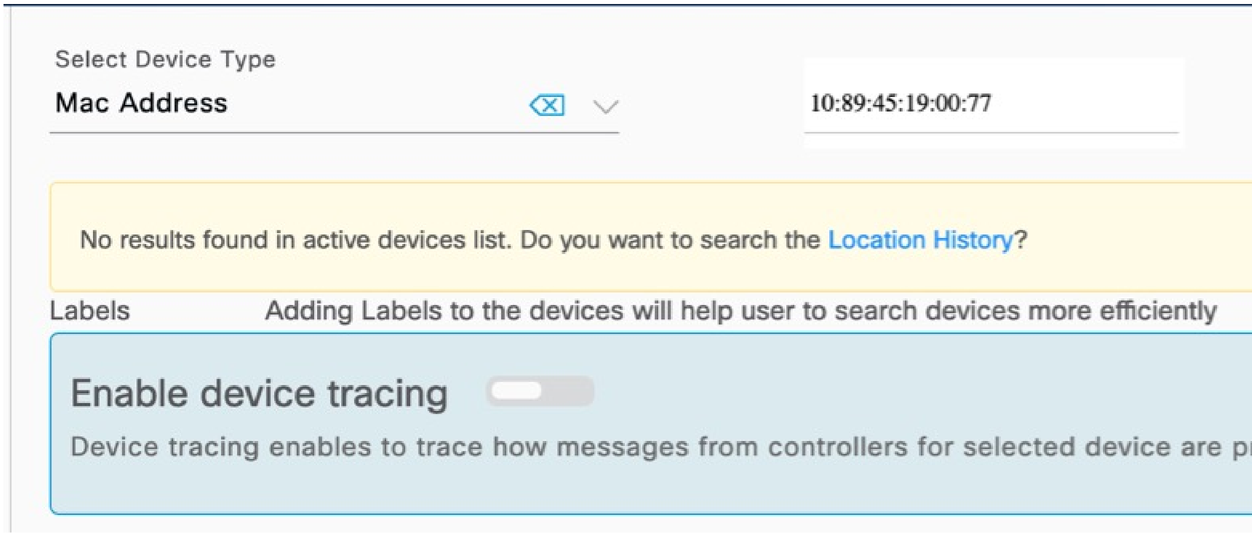
No devices available for this search

Other Options When MAC Address Not Found

If your MAC address search on the currently connected devices is unsuccessful, you can do one of the following:

- enable device tracing, or
- search the location history records.

Figure 30: Search Button



No results found in active devices list. Do you want to search the Location History?

Labels Adding Labels to the devices will help user to search devices more efficiently

Enable device tracing

Device tracing enables to trace how messages from controllers for selected device are p

Device Tracing

You can enable device tracing for a specified MAC Address, even if the device is not currently active. Once device tracing is enabled, all debugging logs for this device are recorded. You can access these logs on the Amazon Web Services (AWS) cloud logs.

Note For activated devices, you can enable device tracing on the device's detail page, as explained in the **Navigating the Device Overview Tab** section of the Access Device Details and Location History article.

Search From Location History

Search from location history link triggers a new search on the location history records of a device. For example, if a device was previously connected to Detect and Locate, but is now disconnected, there should be a record in the location history. The **Search from location history** link searches this historical data, and if successful, displays the information.

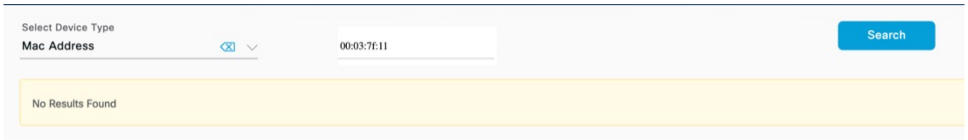
Note For tenants with **SEE**, **EXTEND**, or **SMART_VENUES** licenses, no history can be found on the **Location History** link.

Partial Values and Invalid Characters

Your search result displays the *No result found* message for

- partial values (such as an incomplete MAC address), or
- search strings with invalid characters.

Figure 31: Searching for Partial Value or Invalid Characters



Select Device Type
Mac Address

00:03:7f:11

No Results Found

Manage Columns in the Search Results

You can customize the display of your search results by choosing to hide or show specific columns. Click the three dots located at the top-right corner of the search results table.

Note This feature is available in all tables on Detect and Locate.

CHAPTER 8

Client History

Details and History of a Device

Cisco Spaces: Detect and Locate aggregates and displays various devices in your network. These devices include clients, tags, BLE tags, and interferers.

This article is structured to cover these main aspects:

- accessing and understanding the device details window
- exploring device history and location tracking, and
- delving into insights about your device.

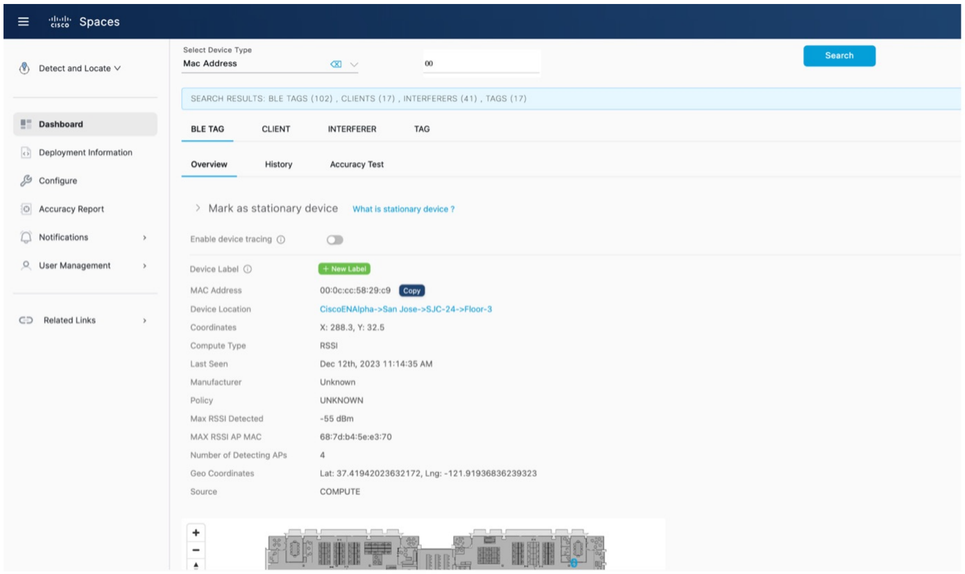
Through detailed device data and insights, you learn how to effectively manage your devices. You can interpret historical location data, and utilize insights for informed decision-making within your network.

Device Detail Window

Click the device to view details. The displayed window has these three tabs:

- Overview (See Overview Tab)
- History (See History Tab), and
- Accuracy Test (See the **Accuracy Test** article).

Figure 32: Details of a Device in Overview, History, and Accuracy Test Tabs



Select Device Type: Mac Address — 00

SEARCH RESULTS: BLE TAGS (102) , CLIENTS (17) , INTERFERERS (41) , TAGS (17)

Mark as stationary device

Enable device tracing

Device Label	+ New Label
MAC Address	00:0c:cc:58:29:c9
Device Location	CiscoENAlpha->San Jose->SJC-24->Floor-3
Coordinates	X: 288.3, Y: 32.5
Compute Type	RSSI
Last Seen	Dec 12th, 2023 11:14:35 AM
Manufacturer	Unknown
Policy	UNKNOWN
Max RSSI Detected	-55 dBm
MAX RSSI AP MAC	68:7d:b4:5e:e3:70
Number of Detecting APs	4
Geo Coordinates	Lat: 37.41942023632172, Lng: -121.91936836239323
Source	COMPUTE

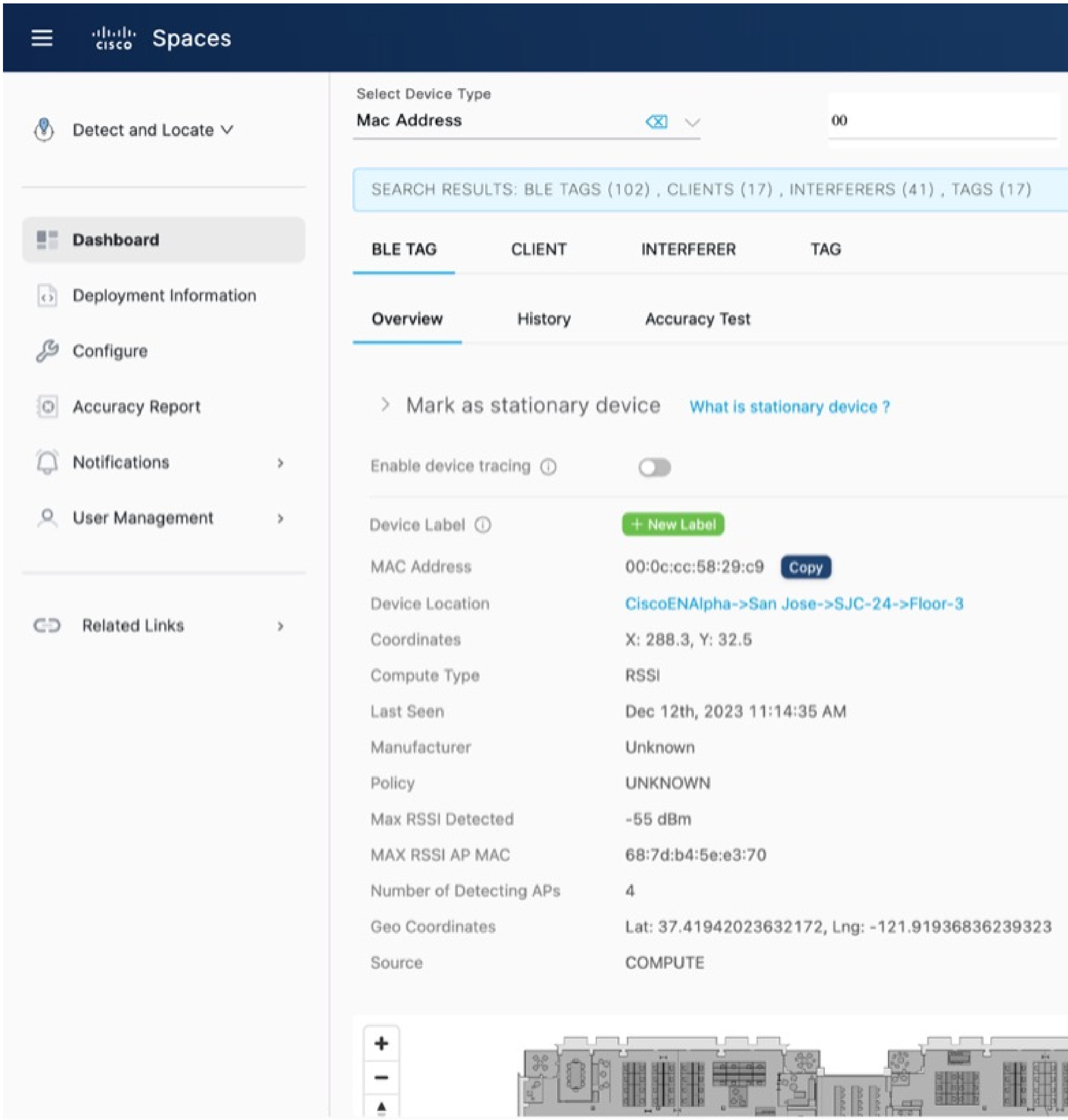
You can access this window with details of a device in any of the following ways:

- **Global search**: Search for a device from the dashboard and click the device from the search results. See the Global Search article.
- **Device toolbar**: From the toolbar on top of the dashboard, choose the device type of this device. This opens a table of devices, and you can choose a device to open the details.
- **Floor map**: Find the specific device on the map and click to view details.

Overview Tab

The **Overview** tab provides details of the device. You can access this tab from the device's detail window.

Figure 33: Overview Tab



Select Device Type: Mac Address

00

SEARCH RESULTS: BLE TAGS (102) , CLIENTS (17) , INTERFERERS (41) , TAGS (17)

Enable device tracing

Device Label	+ New Label
MAC Address	00:0c:cc:58:29:c9
Device Location	CiscoENAlpha->San Jose->SJC-24->Floor-3
Coordinates	X: 288.3, Y: 32.5
Compute Type	RSSI
Last Seen	Dec 12th, 2023 11:14:35 AM
Manufacturer	Unknown
Policy	UNKNOWN
Max RSSI Detected	-55 dBm
MAX RSSI AP MAC	68:7d:b4:5e:e3:70
Number of Detecting APs	4
Geo Coordinates	Lat: 37.41942023632172, Lng: -121.91936836239323
Source	COMPUTE

You can do the following on the **Overview** tab:

- **Mark as stationary device**: Expand this arrow to mark the device as stationary.
- **Enable device tracing**: Toggle this button to initiate MAC debugging for this device.
- **Device Label**: Add, edit, or delete the device label.
- **Device Location**: Click this link to navigate to the device's location on the map.

History Tab

Devices With Location History Records

Detect and Locate provides location history records for only four device types:

- Clients
- Tags
- BLE tags, and
- Rogue clients.

Four Device Location History Representations

This section demonstrates the various ways in which a device's location history is represented in Detect and Locate.

To view the location history of a device, click the device and in the device details window, select the **History** tab. Here you can see insights related to this device and the device's locations plotted over the preceding twenty-four hours (if the device was detected during this period). The location history of a client is represented in the following different forms:

- **Linear Time Frame:** is a graphical representation of a client's location history. The linear time frame consists of color-coded blocks on a bar that indicate the device's activity status over the last 24 hours.
- **Map or List:** are two methods of displaying changes in a device's location, either visually on a map or in a table form with coordinates and event times.
- **Calendar:** allows users to select a day from the past 30 days to view the device's location history. Only the data for that specific day are updated on the linear time frame and the map or list.
- **Client Insights:** are a summary of key data points of a device's location history, including first-seen time, last-seen time, total number of location changes, and total active time.

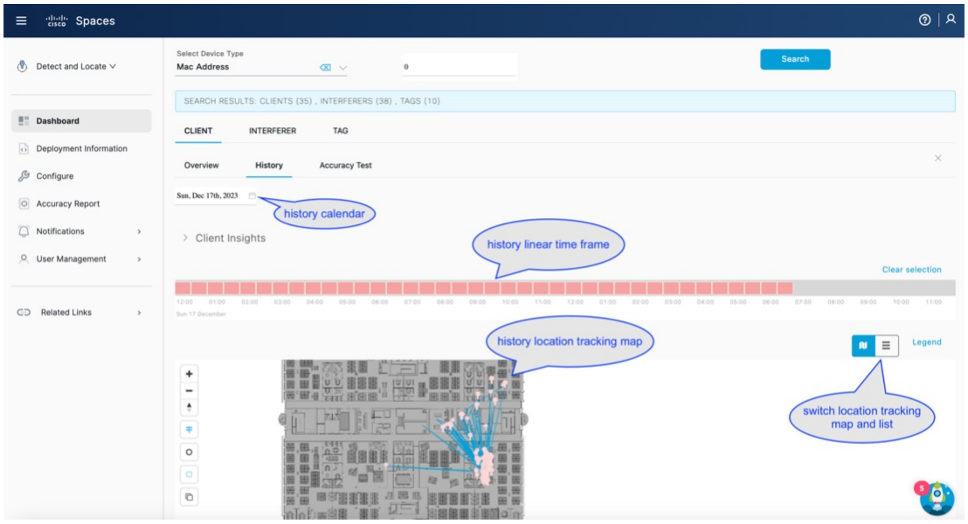
Each of these device history representations is described in detail in this article.

Linear Time Frame

The linear time frame is a graphical representation of a device's location history. You can observe the linear time frame from the **History** tab of a device's details window.

The linear time frame is a long bar indicating a device's activity status over the last 24 hours. This bar is subdivided into one-hour blocks that are color coded to indicate activity.

Figure 34: Linear Time Frame



Select Device Type: Mac Address

SEARCH RESULTS: CLIENTS (35) , INTERFERERS (38) , TAGS (10)

Sun, Dec 17th, 2023

The colour codes of these one-hour blocks are

- **Green**, indicating that the device was associated with the network
- **Red**, indicating that the device was only probing and not associated with the network, and
- **Grey**, indicating that the device was not detected.

You can zoom in and out of the linear time frame.

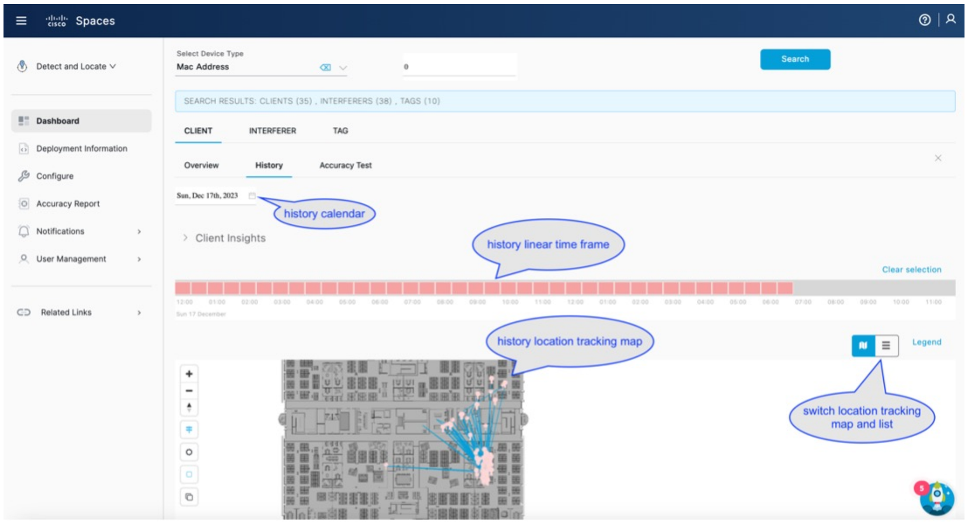
When you click on a particular block, you select the hour. You can observe that the map or list (below this linear time frame) is updated to represent the device's movements for the hour. You can learn more about this from Maps and Lists.

Maps and Lists

Maps and lists are graphical representations of a device's location history and are found in the **History** tab of a device's details. Clicking a block in the linear time frame of the **History** tab updates the map or list. You can click the map or list icons on the right to choose between the two:

- **Maps**: have pink dots to represent the device's location on the map, and blue lines to indicate the path traversed by the device.

Figure 35: Map Showing a Device's Location History



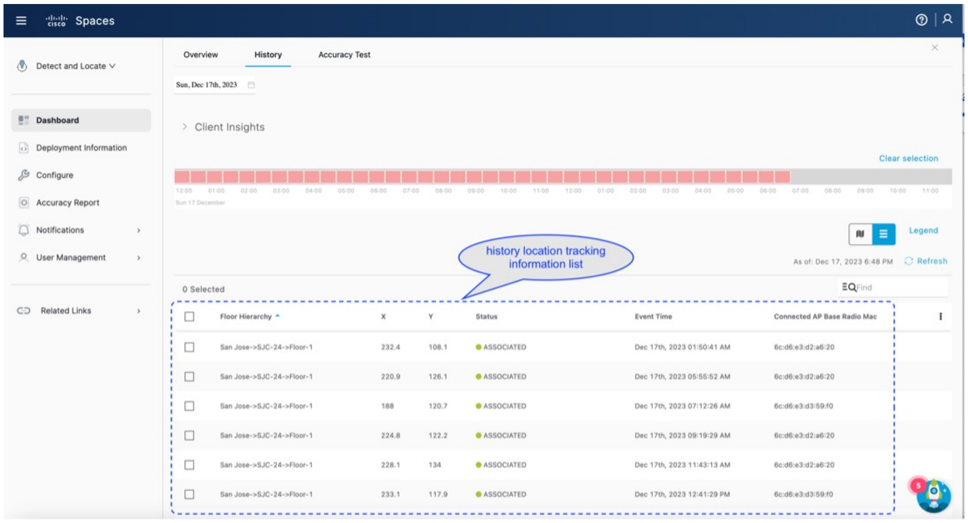
Select Device Type: Mac Address

SEARCH RESULTS: CLIENTS (35) , INTERFERERS (38) , TAGS (10)

Sun, Dec 17th, 2023

- **List**: is a table including the device's location details such as X-Y coordinates and the corresponding time of detection seen in the **Event Time** column.

Figure 36: List Showing a Device's Location History



Sun, Dec 17th, 2023

As of: Dec 17, 2023 6:48 PM

0 Selected

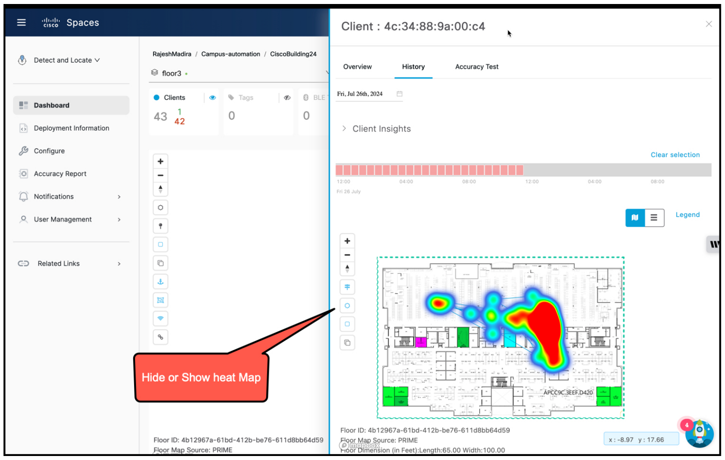
□	Floor Hierarchy	X	Y	Status	Event Time	Connected AP Base Radio Mac
□	San Jose->SJC-24->Floor-1	232.4	108.1	● ASSOCIATED	Dec 17th, 2023 01:50:41 AM	6c:d6:e3:d2:a6:20
□	San Jose->SJC-24->Floor-1	220.9	126.1	● ASSOCIATED	Dec 17th, 2023 05:55:52 AM	6c:d6:e3:d2:a6:20
□	San Jose->SJC-24->Floor-1	188	120.7	● ASSOCIATED	Dec 17th, 2023 07:12:26 AM	6c:d6:e3:d3:59:f0
□	San Jose->SJC-24->Floor-1	224.8	122.2	● ASSOCIATED	Dec 17th, 2023 09:19:29 AM	6c:d6:e3:d2:a6:20
□	San Jose->SJC-24->Floor-1	228.1	134	● ASSOCIATED	Dec 17th, 2023 11:43:13 AM	6c:d6:e3:d2:a6:20
□	San Jose->SJC-24->Floor-1	233.1	117.9	● ASSOCIATED	Dec 17th, 2023 12:41:29 PM	6c:d6:e3:d3:59:f0

Heat Map

A heat map is a visual representation that plots the location chirps of a device and highlights the areas where the device has traveled.

A heat map helps you identify suspicious activity or track missing equipment by providing you exact locations.

Figure 37: Heatmap of a Device



Client : 4c:34:88:9a:00:c4

Fri, Jul 26th, 2024

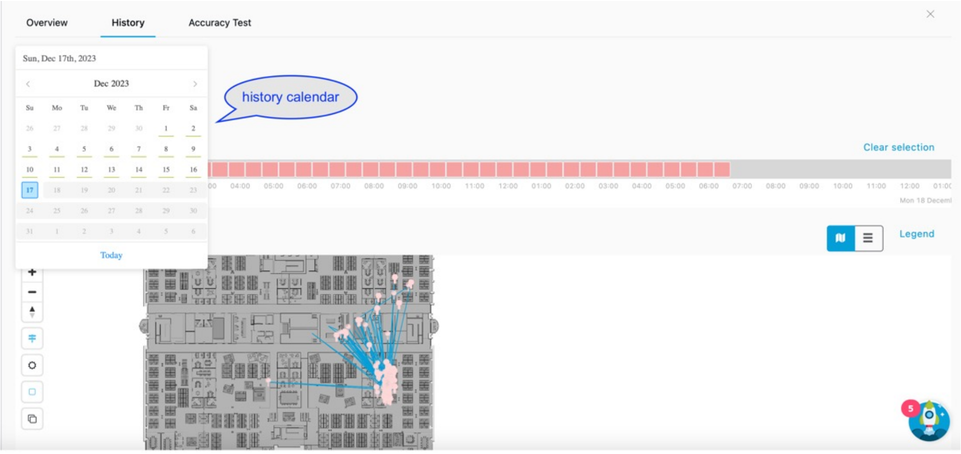
Floor ID: 4b12967a-61bd-412b-be76-611d8bb64d59
Floor Map Source: PRIME
Floor Dimension (in Feet):Length:65.00 Width:100.00

x : -8.97 y : 17.66

Calendar

A 30-day calendar helps you observe the location history of a device for the preceding 30 days.

Figure 38: Calendar Showing 30-Day Location History of a Device



Sun, Dec 17th, 2023

You can open this calendar by clicking the calendar icon at the top left of the **History** tab of a device's details window.

Choose a specific date on the calendar, and observe how the following are updated to represent the device's location data for that particular date:

- Linear time frame, and
- Maps or lists.

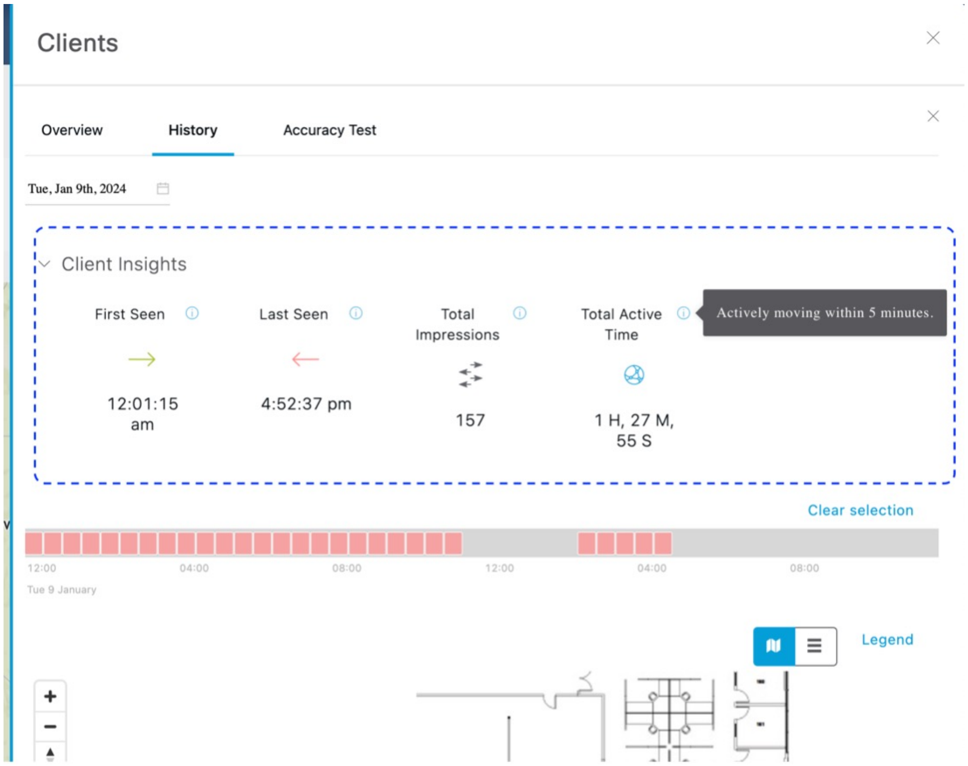
The calendar contains data for 30 days before the current date only. Visual indicators used to reflect the availability of historical records are

- **dates with a green line underneath** which have active history records, and
- **dates without a green line** which lack history records for that day.

Client Insights

Client insights are a summary of key data points of a device's location history:

Figure 39: Client Insights: Key Data Points of a Device's Location History



Tue, Jan 9th, 2024

Client Insights

First Seen: 12:01:15 am

Last Seen: 4:52:37 pm

Total Impressions: 157

Total Active Time: 1 H, 27 M, 55 S

Actively moving within 5 minutes.

- **First Seen:** is the time and date when the wireless controller first detected the device within a specific period.

Note

- **If the client stays connected for over a week**, the **First Seen** time is when the client was first detected that week. For example, assume the day is Friday, and the client was first detected last Monday at 8:00 am, after which the client stayed connected the entire week. The **First Seen** as checked on Friday, would show as Monday, 8:00 AM.
- **If the client connects and disconnects over the week**, the **First Seen** would be the first time the client connected on the last day of connection. For example, assume the day is Friday, and the client connected at 8:00 am on Monday, Wednesday, and Friday. The **First Seen** as checked on Friday would show as Friday, 8:00 AM.

- **Last Seen:** is the time and date of the device's most recent appearance in the records.
- **Total Impressions:** is the number of times the device's location has changed.
- **Total Active Time:** is the duration that the device has been moving actively within the last five minutes.

CHAPTER 9

Location Accuracy

Location Accuracy

You can perform a location accuracy test for a single device with multiple location points. You can use the Location Accuracy Test tool to validate the placement and number of access points (APs), for a good location accuracy experience. The Location Accuracy tool provides you with the ability to quantify the location accuracy for a specific location. During the Location Accuracy test, the administrator uses a wireless client device to measure the difference between the actual and the calculated location of a device.

Restrictions for Location Accuracy

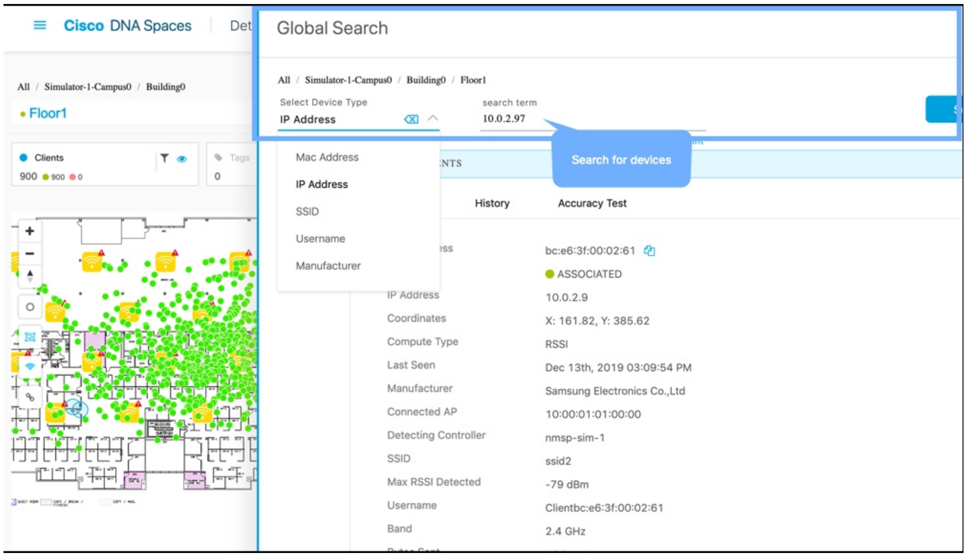
- The display refresh time is three seconds and cannot be reconfigured.
- You cannot run this location accuracy test on APs with external antennas. However, location detection is supported on these APs.
- You cannot reconfigure the display refresh time. The display refresh time is three seconds.
- The sample count displayed during a location accuracy test is a best-effort estimate of location values collected during back end processes. This sample count may differ from actual samples captured during an accuracy test.

Test Location Accuracy

This Cisco Spaces: Detect and Locate shows you how to run the location accuracy test.

Step 1 From the Detect and Locate dashboard, search for a device using a MAC address from the **Search MAC, IP, SSID, Manufacturer** text field.

Figure 40: Detect and Locate: Dashboard



Global Search

All / Simulator-1-Campus0 / Building0 / Floor1

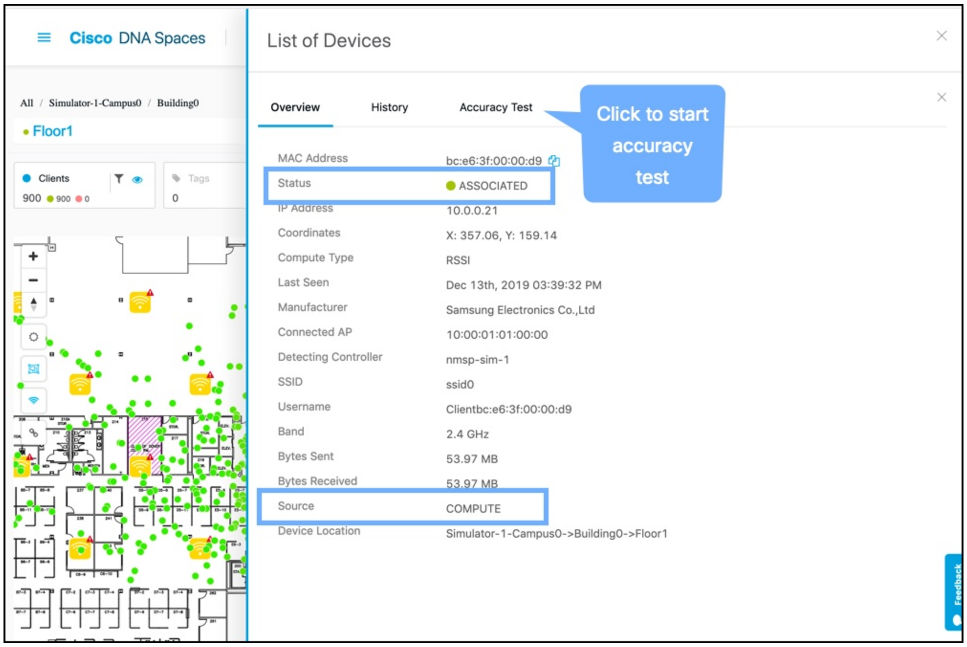
Select Device Type	search term
IP Address	10.0.2.97

ss	bc:e6:3f:00:02:61
	● ASSOCIATED
IP Address	10.0.2.9
Coordinates	X: 161.82, Y: 385.62
Compute Type	RSSI
Last Seen	Dec 13th, 2019 03:09:54 PM
Manufacturer	Samsung Electronics Co.,Ltd
Connected AP	10:00:01:01:00:00
Detecting Controller	nmsp-sim-1
SSID	ssid2
Max RSSI Detected	-79 dBm
Username	Clientbc:e6:3f:00:02:61
Band	2.4 GHz

Step 2 Ensure that the **Status** of the device is **ASSOCIATED** and the **Source** is **COMPUTE**.

Step 3 In the device details window, click **Accuracy Test** tab.

Figure 41: Detect and Locate; Initiate Accuracy Test

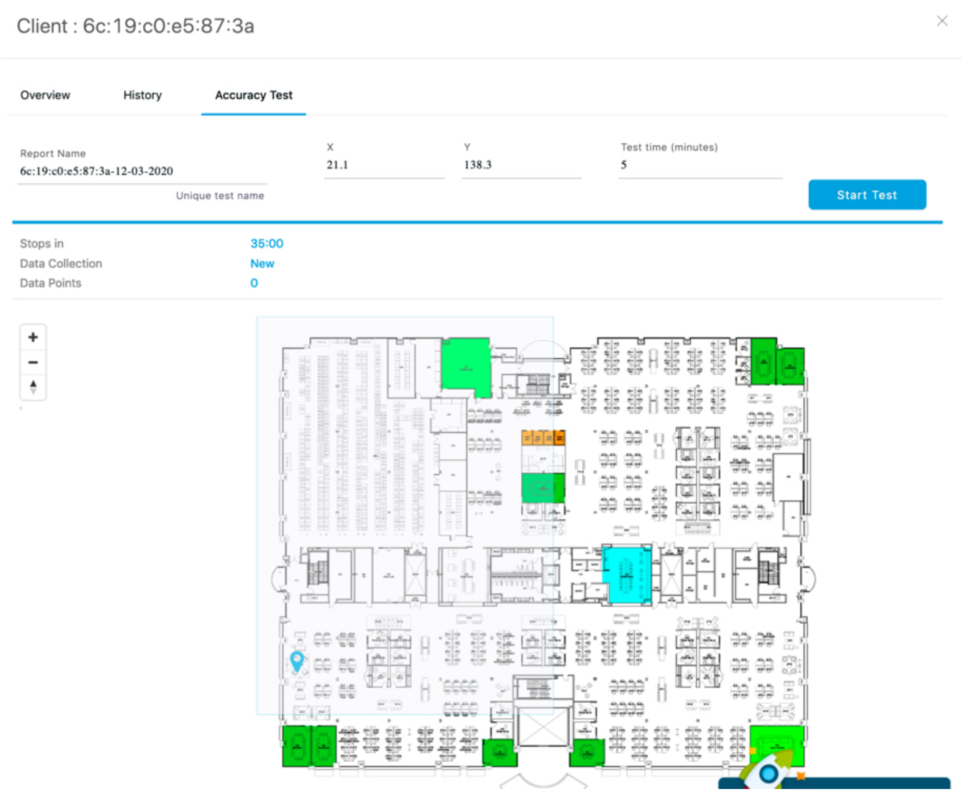


List of Devices

MAC Address	bc:e6:3f:00:00:d9
Status	● ASSOCIATED
IP Address	10.0.0.21
Coordinates	X: 357.06, Y: 159.14
Compute Type	RSSI
Last Seen	Dec 13th, 2019 03:39:32 PM
Manufacturer	Samsung Electronics Co.,Ltd
Connected AP	10:00:01:01:00:00
Detecting Controller	nmsp-sim-1
SSID	ssid0
Username	Clientbc:e6:3f:00:00:d9
Band	2.4 GHz
Bytes Sent	53.97 MB
Bytes Received	53.97 MB
Source	COMPUTE
Device Location	Simulator-1-Campus0->Building0->Floor1

Step 4 Enter a unique report name. Move the blue pointer to the client's real-time location or adjust the X and Y coordinates. To begin, click **Start Test**.

Figure 42: Detect and Locate Initiate Accuracy Test



Client : 6c:19:c0:e5:87:3a

Report Name: 6c:19:c0:e5:87:3a-12-03-2020

Unique test name

X: 21.1

Y: 138.3

Test time (minutes): 5

Stops in: 35:00

Data Collection: New

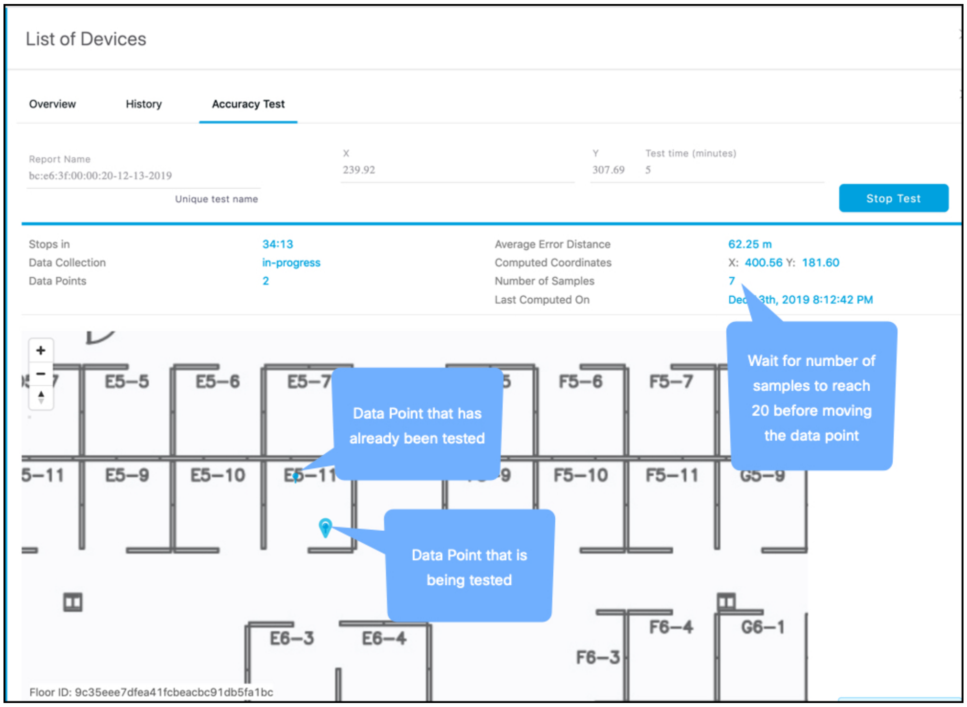
Data Points: 0

You can observe that the number of samples begins to increase.

Note The display refresh time is three seconds.

Step 5 Wait for the number of samples to reach 20 and click **Stop Test**. Move the blue pointer representing the data point to a new location and click **Start Test** again.

Figure 43: Sample Size Must Reach 20



List of Devices

Report Name
bc:e6:3f:00:00:20-12-13-2019
Unique test name

X
239.92

Y
307.69

Test time (minutes)
5

Stops in	34:13	Average Error Distance	62.25 m
Data Collection	in-progress	Computed Coordinates	X: 400.56 Y: 181.60
Data Points	2	Number of Samples	7
		Last Computed On	Dec 13th, 2019 8:12:42 PM

Wait for number of samples to reach 20 before moving the data point

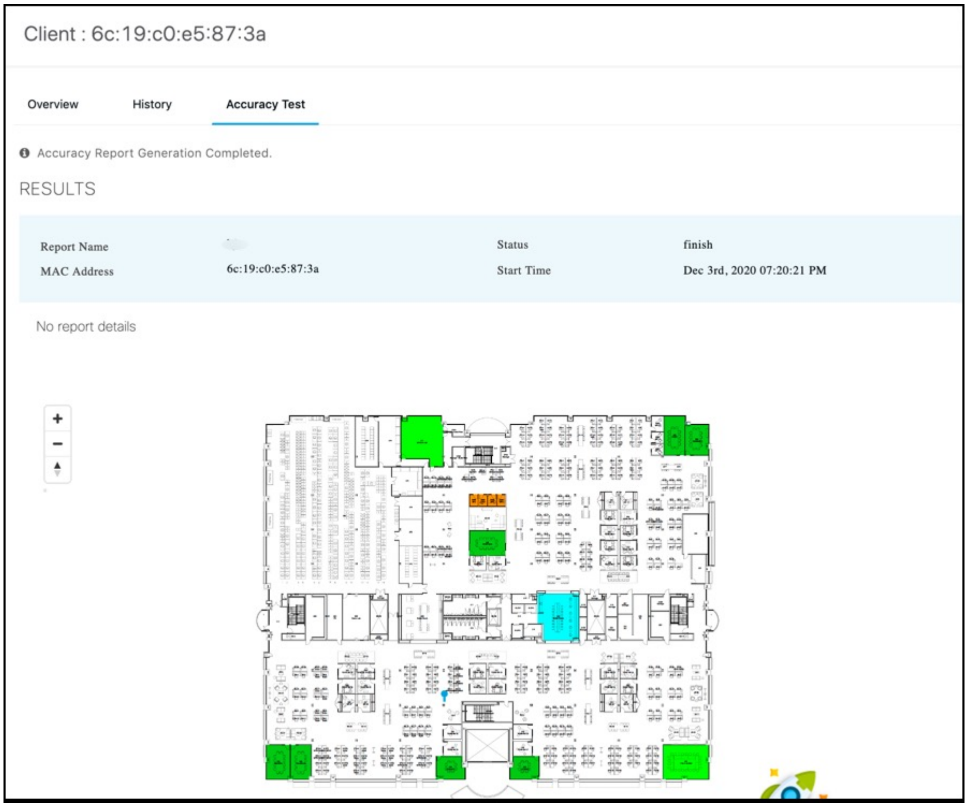
Data Point that has already been tested

Data Point that is being tested

Floor ID: 9c35eee7dfea41fcbeacbc91db5fa1bc

Step 6 Repeat for multiple locations for a more accurate understanding of location accuracy.

Figure 44: Repeat For Multiple Locations



Client : 6c:19:c0:e5:87:3a

Accuracy Report Generation Completed.

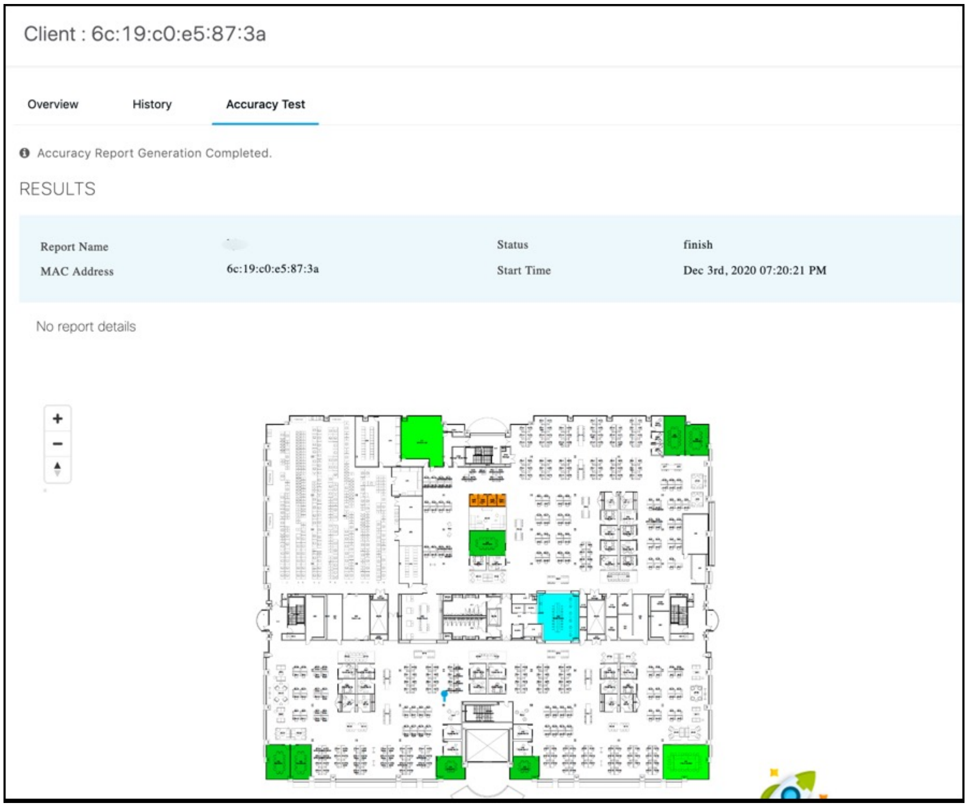
RESULTS

Report Name		Status	finish
MAC Address	6c:19:c0:e5:87:3a	Start Time	Dec 3rd, 2020 07:20:21 PM

No report details

Step 7 Repeat for multiple locations for a more accurate understanding of location accuracy.

Figure 45: Repeat For Multiple Locations



Client : 6c:19:c0:e5:87:3a

Accuracy Report Generation Completed.

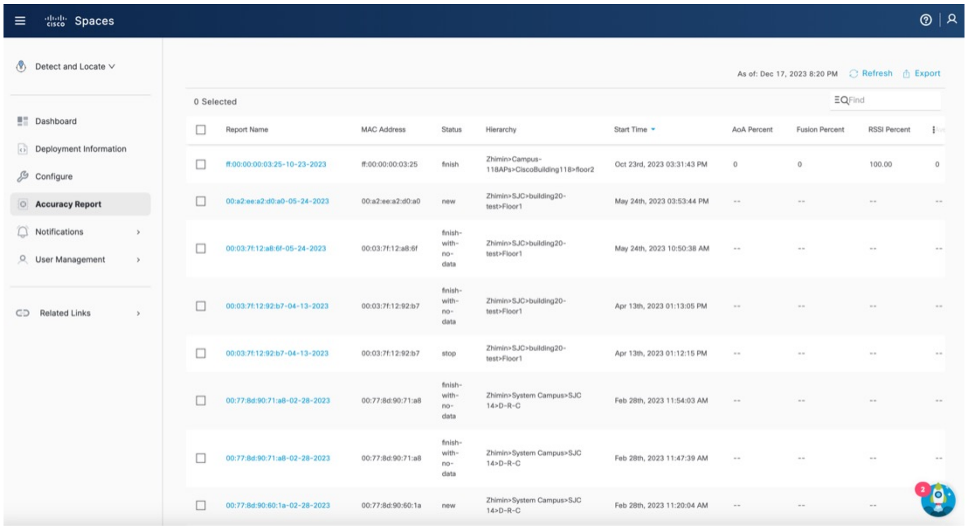
RESULTS

Report Name		Status	finish
MAC Address	6c:19:c0:e5:87:3a	Start Time	Dec 3rd, 2020 07:20:21 PM

No report details

The accuracy reports are generated after the accuracy testing is done. You can also check it from the Detect and Locate left navigation bar under **Accuracy Report**.

Figure 46: Repeat For Multiple Locations



As of: Dec 17, 2023 8:20 PM

0 Selected

□	Report Name	MAC Address	Status	Hierarchy	Start Time	AoA Percent	Fusion Percent	RSSI Percent	⋮
□	ff:00:00:00:03:25-10-23-2023	ff:00:00:00:03:25	finish	Zhimin>Campus-118APs>CiscoBuilding118>floor2	Oct 23rd, 2023 03:31:43 PM	0	0	100.00	0
□	00:a2:ee:a2:d0:a0-05-24-2023	00:a2:ee:a2:d0:a0	new	Zhimin>SJC>building20-test>Floor1	May 24th, 2023 03:53:44 PM	--	--	--	--
□	00:03:7f:12:a8:6f-05-24-2023	00:03:7f:12:a8:6f	finish-with-no-data	Zhimin>SJC>building20-test>Floor1	May 24th, 2023 10:50:38 AM	--	--	--	--
□	00:03:7f:12:92:b7-04-13-2023	00:03:7f:12:92:b7	finish-with-no-data	Zhimin>SJC>building20-test>Floor1	Apr 13th, 2023 01:13:05 PM	--	--	--	--
□	00:03:7f:12:92:b7-04-13-2023	00:03:7f:12:92:b7	stop	Zhimin>SJC>building20-test>Floor1	Apr 13th, 2023 01:12:15 PM	--	--	--	--
□	00:77:8d:90:71:a8-02-28-2023	00:77:8d:90:71:a8	finish-with-no-data	Zhimin>System Campus>SJC 14>D-R-C	Feb 28th, 2023 11:54:03 AM	--	--	--	--
□	00:77:8d:90:71:a8-02-28-2023	00:77:8d:90:71:a8	finish-with-no-data	Zhimin>System Campus>SJC 14>D-R-C	Feb 28th, 2023 11:47:39 AM	--	--	--	--
□	00:77:8d:90:60:1a-02-28-2023	00:77:8d:90:60:1a	new	Zhimin>System Campus>SJC 14>D-R-C	Feb 28th, 2023 11:20:04 AM	--	--	--	

CHAPTER 10

How to Track Devices

Device Tracking

Devices Tracked by Cisco Spaces: Detect and Locate

Cisco Spaces: Detect and Locate can track the following devices within your network:

- Wireless Clients
- Interferers
- Rogue APs
- Radio-Frequency Identification (RFID) tags, and
- Rogue Clients.

Enable or Disable Device Tracking in Cisco Spaces

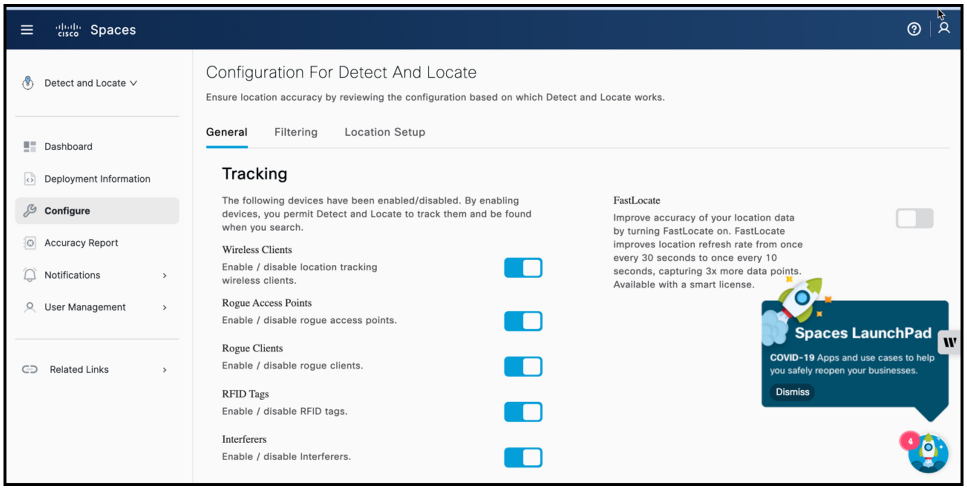
Follow these steps to enable or disable the tracking of specific device types:

Step 1 From the left navigation bar of the Detect and Locate dashboard, select **Configure**.

Step 2 Choose **General**.

a) Here, you can choose to enable or disable the tracking of device types as needed.

Figure 47: Enable or Disable Specific Device Types



Configuration For Detect And Locate

Ensure location accuracy by reviewing the configuration based on which Detect and Locate works.

Tracking

The following devices have been enabled/disabled. By enabling devices, you permit Detect and Locate to track them and be found when you search.

Wireless Clients
Enable / disable location tracking wireless clients.

Rogue Access Points
Enable / disable rogue access points.

Rogue Clients
Enable / disable rogue clients.

RFID Tags
Enable / disable RFID tags.

Interferers
Enable / disable Interferers.

FastLocate
Improve accuracy of your location data by turning FastLocate on. FastLocate improves location refresh rate from once every 30 seconds to once every 10 seconds, capturing 3x more data points. Available with a smart license.

COVID-19 Apps and use cases to help you safely reopen your businesses.

Device Visibility

Enable Device Visibility

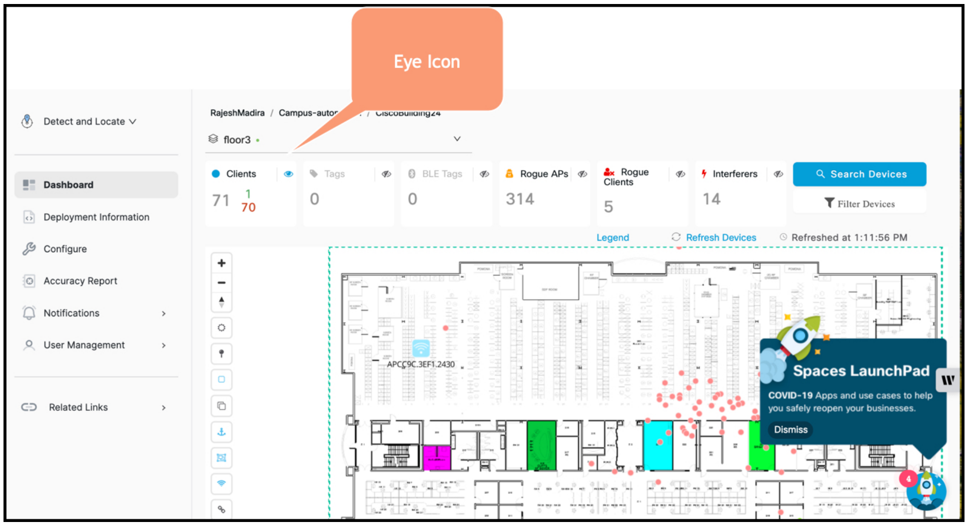
Follow these steps to show or hide devices of a particular type:

Step 1 Navigate to the Detect and Locate dashboard.

Step 2 Click on the **eye icon (Show/Hide button)** corresponding to the respective device type.

Step 3 Ensure that the eye icon is enabled so that you can view the device type on the dashboard.

Figure 48: Enable or Disable the Visibility of Specific Device Types


Eye Icon

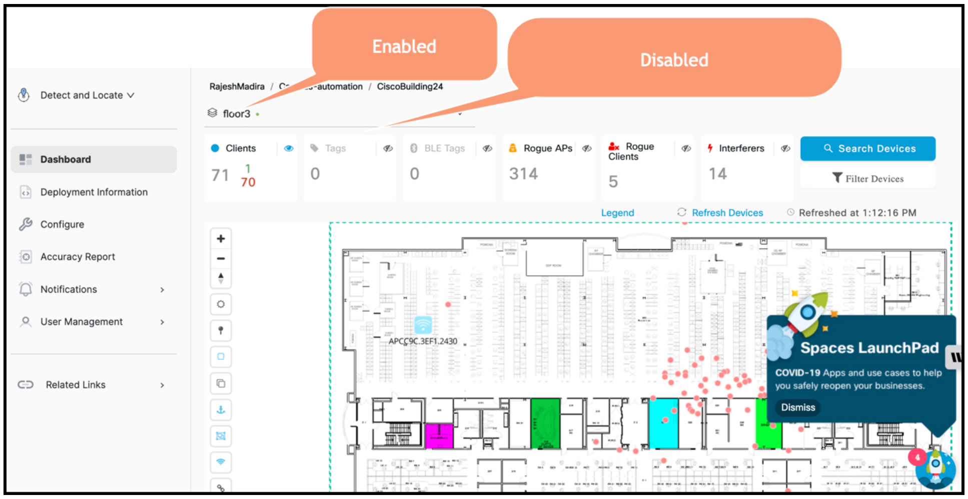
View Enabled Device Types

Follow these steps to view the enabled device types:

Step 1 Navigate to the Detect and Locate dashboard.

Step 2 Check the current status of each device type to see which ones are enabled.

Figure 49: Check the Visibility Status of Device Types


Enabled

Disabled

Keep Devices Visible with Regular Updates

Detect and Locate uses a device eviction time of 10 minutes. Ensure that the following updates are received at this interval from the wireless controller:

- Received Signal Strength Indicator (RSSI)
- Angle of Arrival (AOA)
- Information (Info), and
- Statistics (Stats).

Eviction Times

If a device does not send updates within the ten-minute eviction time, Cisco Spaces removes the device from the system.

CHAPTER 11

Manage Columns

Manage Columns

Click the **Manage Columns** ⚙ icon to reorder, hide, or show the columns.

CHAPTER 12

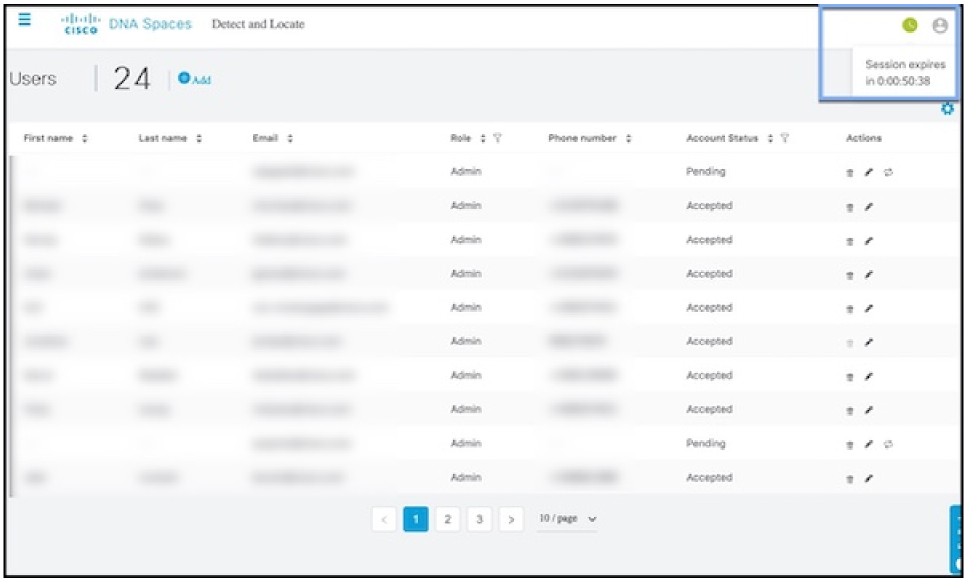
Manage Session Expiry

Session expiry

Manage Sessions Expiry

On the Detect and Locate dashboard, click the green icon at the top-right corner for details on session expiry.

Figure 50: Session Expiry



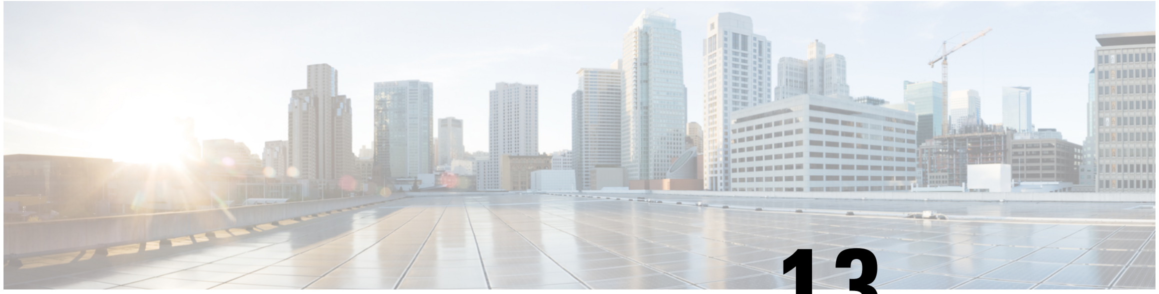
Session expires in 0:00:50:38

Users | 24 Add

First name	Last name	Email	Role	Phone number	Account Status	Actions
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Pending	
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Accepted	
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Accepted	
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Accepted	
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Accepted	
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Accepted	
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Accepted	
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Accepted	
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Pending	
[redacted]	[redacted]	[redacted]	Admin	[redacted]	Accepted	

PART V

Manage Notifications



CHAPTER 13

Using Northbound Notifications

Using Northbound Notifications

Cisco Spaces: Detect and Locate can be configured to send notifications to a notification endpoint of your choice. You can find the configured notification from the **NOTIFICATIONS** menu.

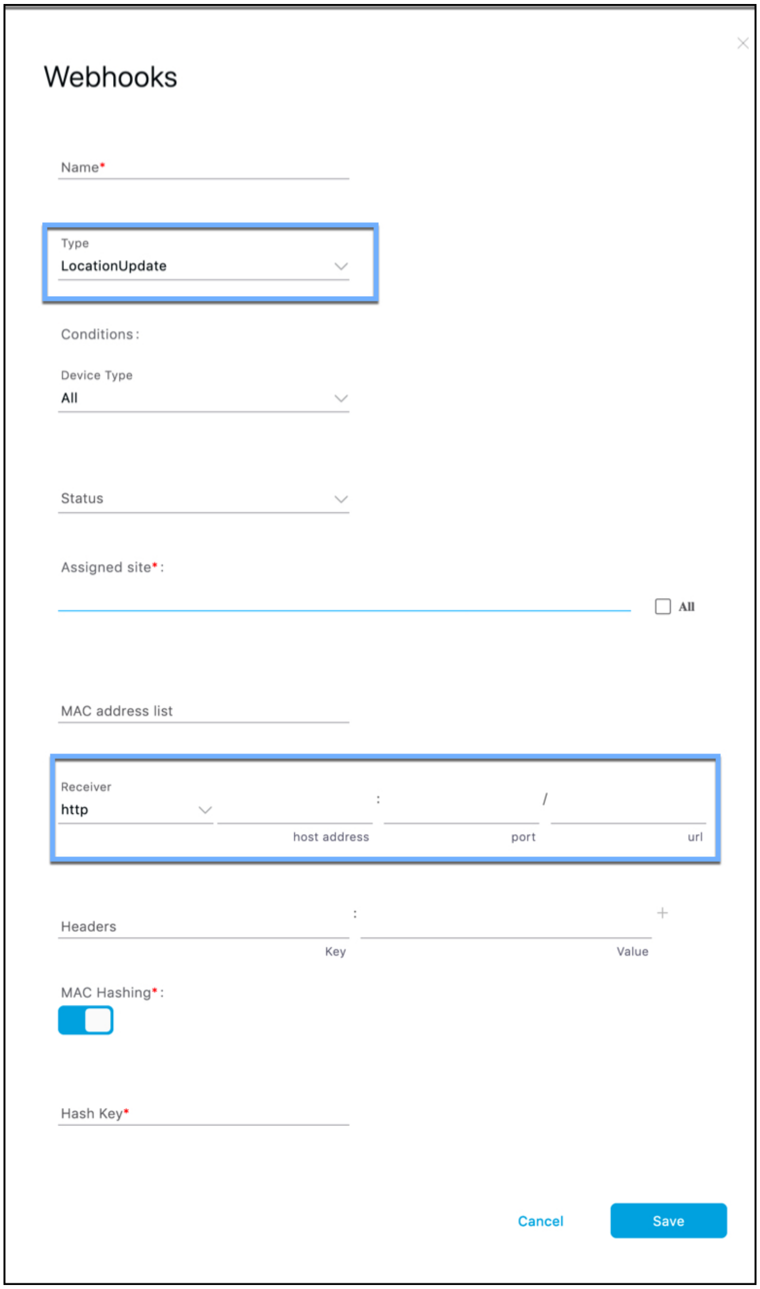
Currently, the following notification types are supported:

- **Association**: Generates a notification when a device is associated to a network or dissociated from a network.
- **Absence**: Generates a notification when a device is undetected for more than 15 minutes.
- **LocationUpdate**: Generating a notification when a device changes location, for example, between campuses, buildings, or floors.
- **In/Out**: Generates a notification when a device is detected as moving into or moving out of a specific area in the location hierarchy.

Location Update (Northbound Notification)

This type of notification is generated when a device changes location, for example, between campuses, buildings, or floors. Supported device types are Rogue Client, Client, RFID Tag, Rogue AP, Interferer.

Figure 51: Location Update



Webhooks

Name*

Type
LocationUpdate

Conditions:

Device Type
All

Status

Assigned site*:

□ All

MAC address list

Receiver
http : /
host address port url

Headers : +
Key Value

MAC Hashing*:

Hash Key*

The fields of the displayed Location Update page are described below:

- **Status**: You can configure to restrict the notification generation based on whether the device is associated with the network or not (probing). You can select **All** if the status of the device does not matter.
- **Assigned Site**: Check one or more areas (floor, campus, zone, building) by drilling down the map hierarchy. Check the **All** check box if the location of the device does not matter.
- **MAC Address list**: If you want to generate notifications for specific devices, enter the specific MAC addresses here.

- **Receiver**: Enter the destination to send the notification messages. Only HTTP and HTTPS are supported. Enter the hostname, port number, and URL.
- **Headers**: You can configure to send additional information along with the notifications in these headers, for example, company-specific information like company name. You can enter multiple headers.
- **MAC Hashing**: You can enable (or disable) the hashing of your MAC address to protect the MAC addresses sent in the notification. To do this, you must enter a hash key.

Notification Subscription Sample (JSON)

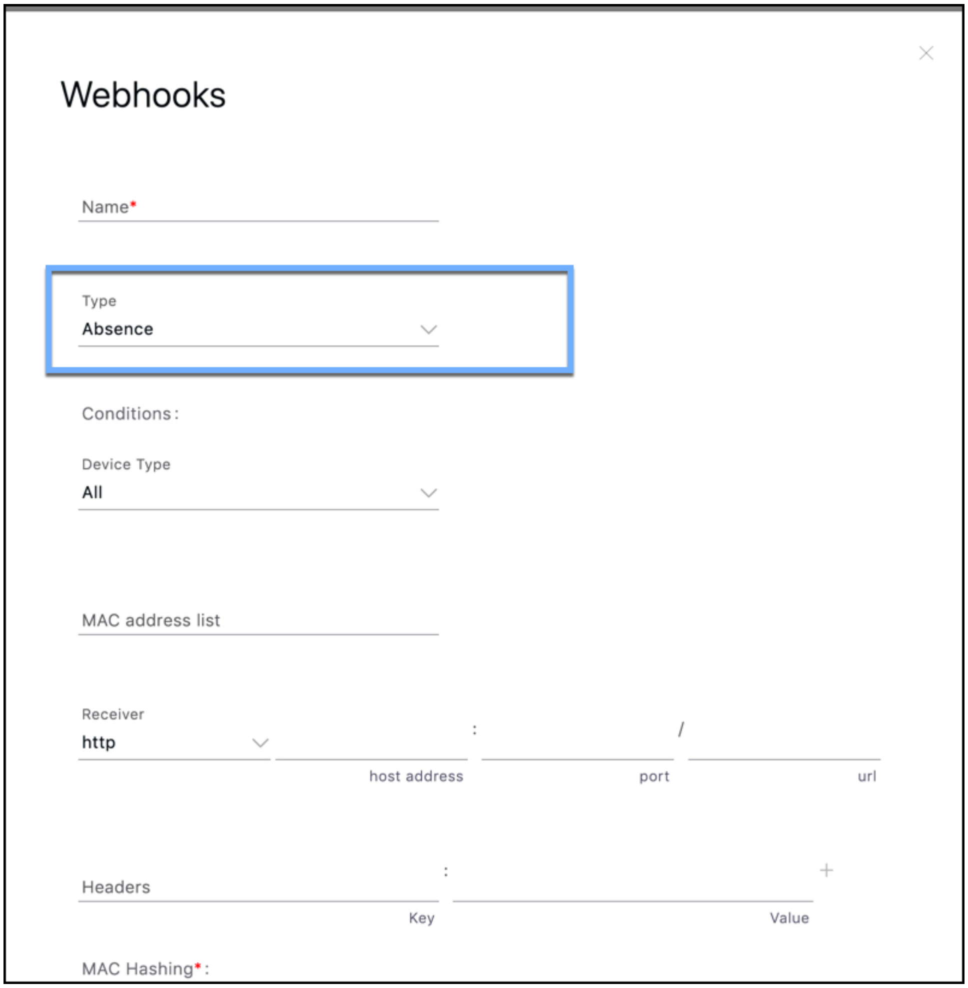
The following is a sample of the Location Update notification subscription:

```
{
    tenantId: '1001',
    id: "552a1a14-20cb-4581-855d-f3c9f120248e",
    name: "Test LocationUpdate Notification",
    type: "LocationUpdate",
    userid: "miczhao",
    enabled: true,
    internal: false,
    conditions: {
        deviceType: "Client",
        status: "Associated",
        hierarchy: {
            name: "System Campus -> SJC-24“,
            level: “CAMPUS”,
              campus: [“d12365e0ce514780aa2b5f01c7edaacd”],
              building: [“dbaf32ce320f4fe2a8935aebc387c8be”],
        }
        macAddressList: "11:22:33:44:55:66;11:22:33:44:55:67"
    },
    receiver: {
        url: "https://data.customer.com:443",
        messageFormat: "JSON",
        qos: "AT_MOST_ONCE",
        headers: {"Content-Type": "application/json", Accept: "application/json"}
    },
    enableMacScrambling: true,
    macScramblingSalt: "salt"
}
}
```

Absence (Northbound Notification)

This type of notification is generated when a device is undetected for more than 15 minutes. Supported device types are **Client** and **RFID Tag**.

Figure 52: Absence



Webhooks

Name*

Type
Absence

Conditions:

Device Type
All

MAC address list

Receiver
http : /
host address port url

Headers : +
Key Value

MAC Hashing*:

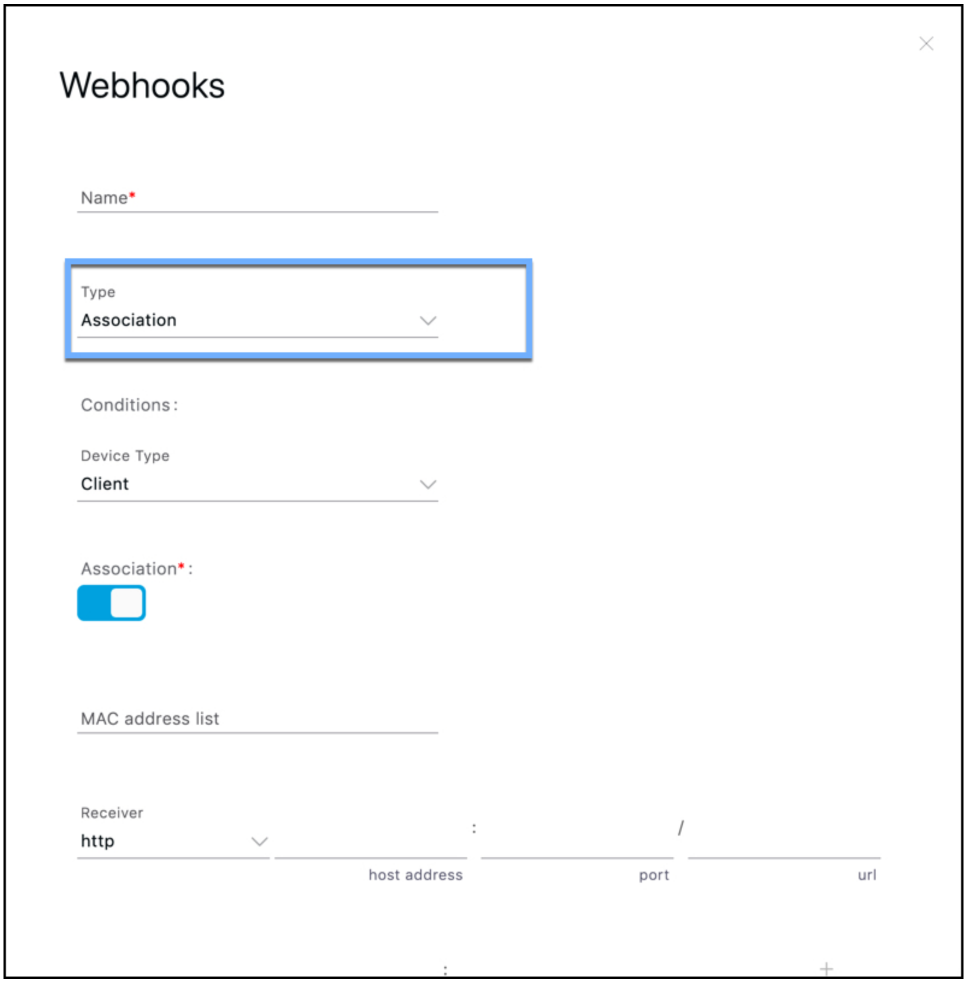
The fields of the **Absence** page are described below:

- **MAC Address list**: For device-specific notifications, enter the specific MAC addresses here.
- **Receiver**: Enter destination to send the notification messages to. Only HTTP and HTTPS are supported. Enter the host IP address, port number, and URL.
- **Headers**: Configure more headers, for example, company-specific information such as company name. Note that multiple headers can be added.
- **MAC Hashing**: Enable (or disable) the hashing of your MAC address, to protect the MAC addresses sent in the notification. Now, you have to enter a hash key.

Association (Northbound Notification)

This type of notification is generated when one or more devices are associated to a network or dissociated from a network.

Figure 53: Association



Webhooks

Name*

Type
Association

Conditions :

Device Type
Client

Association* :

MAC address list

Receiver
http : /
host address port url

- **Association**: Enable this button to generate a notification when a device is associated with a network. Disable the button to generate a notification when a device is disassociated from the network.
- **Status**: You can configure to restrict the notification generation based on whether device is associated with the network or not (probing). If the status of the device does not matter, choose **All**.
- **MAC Address list**: If you want to generate notifications for specific devices, enter the specific MAC addresses here.
- **Receiver**: Destination to send the notification messages. Only HTTP and HTTPS are supported. Enter the hostname, port number, and URL.
- **Headers**: You can configure to send additional information along with the notifications in these headers, for example, company-specific information like company name. You can add multiple headers can be added.
- **MAC Hashing**: You can enable (or disable) the hashing of your MAC address, to protect the MAC addresses sent in the notification. This requires you to enter a hash key.

Notification Subscription Sample (JSON)

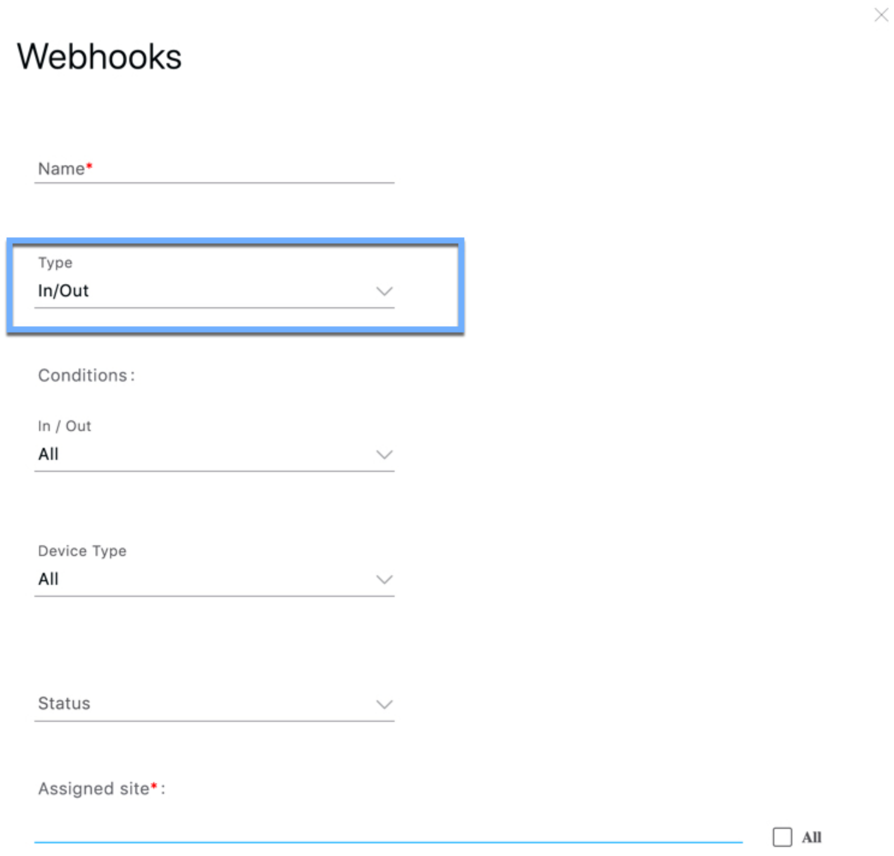
The following is a sample of the Association notification subscription:

```
{
    tenantId: '2001',
    id: "552a1a14-20cb-4581-855d-f3c9f120248e",
    name: "Test Association Notification",
    type: “Association”,
    userid: “testuser”,
    enabled: true,
    intenal: false,
    conditions: {
        association: true,
        deviceType: “Client”,
        hierarchy: {
              name: “System Campus -> Building-24 -> 3rd Floor”,
              level: “FLOOR”,
              campus: [“d12365e0ce514780aa2b5f01c7edaacd”],
              building: [“dbaf32ce320f4fe2a8935aebc387c8be”],
              floor: [“2747871a29af4ab1989a4fb52b143552”]
        }
    },
    receiver: {
        url: "https://data.customer.com:443",
        messageFormat: "JSON",
        qos: "AT_MOST_ONCE",
        headers: {"Content-Type": "application/json", Accept: "application/json"}
    },
    enableMacScrambling: true,
    macScramblingSalt: "hashit"
}
```

In/Out (Northbound Notification)

This type of notification is generated when a device is detected as moving into or moving out of a specific area in the location hierarchy.

Figure 54: Absence



Webhooks

Name*

Type
In/Out

Conditions:

In / Out
All

Device Type
All

Status

Assigned site*:

□ All

In/Out: Select the type of movement.

- Configure **In** if you want a notification generated when a device enters the configured **Assigned Site**.
- Configure **Out** if you want a notification generated when a device leaves the configured **Assigned Site**.
- Configure **No Change** if the entry and exit of the device into **Assigned Site** is not required, but a simple location change within the **Assigned site** is sufficient.
- Configure **All**, if both **In** and **Out** should generate notifications.

- **Status** : Configure to restrict the notification generation based on whether device is associated with the network or not (probing). You can select All if the status of the device does not matter.
- **Assigned Site**:Select one or more areas (floor, campus, zone, building) by drilling down the map hierarchy. Check the **All** checkbox if the location of the device does not matter. This field is required.
- **MAC Address list**: If you want to generate notifications for specific devices, enter the specific MAC addresses here.

- **Receiver**: Destination to send the notification messages. Only HTTP and HTTPS are supported. Enter the hostname, port number, and URL.
- **Headers**: Configure to send additional Information along with the notifications in these headers, for example, company-specific information like company name. Multiple headers can be added.
- **MAC Hashing**: You can enable (or disable) the hashing of your MAC address, to protect the MAC addresses sent in the notification. This requires you to enter a hash key.

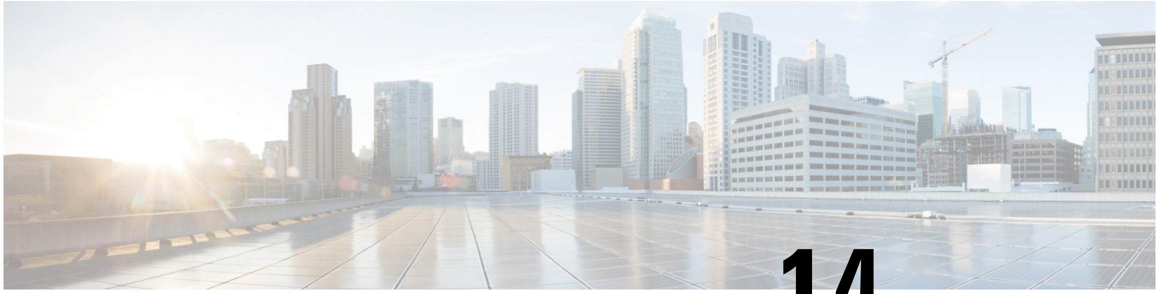
Notification Subscription Sample (JSON)

The following is a sample of the In/Out notification subscritpion:

```
{
    tenantId: '2001',
    id: "552a1a14-20cb-4581-855d-f3c9f120248e",
    name: "Test InOut Notification",
    type: “InOut”,
    userid: “testuser”,
    enabled: true,
    intenal: false,
    conditions: {
        inout: “All”,
        deviceType: “Client”,
        status: “Associated”,
        hierarchy: {
              name: “System Campus -> Building-24 -> 3rd Floor”,
              level: “FLOOR”,
              campus: [“d12365e0ce514780aa2b5f01c7edaacd”],
              building: [“dbaf32ce320f4fe2a8935aebc387c8be”],
              floor: [“2747871a29af4ab1989a4fb52b143552”]
        }
        macAddressList: "11:22:33:44:55:66;11:22:33:44:55:67"
    },
    receiver: {
        url: "https://data.customer.com:443",
        messageFormat: "JSON",
        qos: "AT_MOST_ONCE",
        headers: {"Content-Type": "application/json", Accept: "application/json"}
    },
    enableMacScrambling: true,
    macScramblingSalt: "hashit"
}
}
```

PART VI

Hyperlocation and FastLocate



CHAPTER 14

Configuring Hyperlocation

Enabling Cisco Hyperlocation

The Cisco Hyperlocation solution is a suite of technologies that enables advanced location capabilities through a mix of software and hardware innovations. The Cisco Hyperlocation solution substantially increases the location accuracy of the clients connected to Cisco Spaces. The solution uses the Angle-of-Arrival (AoA) of Wi-Fi signals to determine the location of connected mobile devices.

Cisco Hyperlocation is available on the following access points that have a hyperlocation module and a hyperlocation antenna:

- Cisco Aironet 3700 Series Access Points (Requires hyperlocation antenna)
- Cisco Aironet 4800 Series Access Points

You can deploy Cisco Hyperlocation using the following components:

- Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controllers
- Cisco Spaces
- Cisco Spaces: Connector

Note Cisco CMX is not requried for Cisco Hyperlocation.

Cisco Spaces uses advanced location algorithms to extract phase differences from the location information collected from the wireless clients. This allows Cisco Spaces to locate associated wireless clients up to a distance of one meter accuracy (with a 50% error distance) in an optimal deployment.

The improved location accuracy provides more granular analytics data compared to RSSI-based location.

Cisco Hyperlocation is available on the following controllers:

- Supported on Cisco AireOS Wireless Controller
- Supported on Cisco Catalyst 9800 Series Wireless Controllers

How to Configure Cisco Hyperlocation

This section describes how to enable Cisco Hyperlocation on your network. The section also shows you how to verify if Cisco Spaces is receiving Hyperlocation packets from client devices.

From every active and associated device, Cisco Spaces receives packets every 10 seconds. This is called packet rate frequency. For standard RSSI, packet frequency depends on device probing. But a typical frequency of the Wi-Fi probe packets is 30 seconds to one minute.

Before you begin

- Ensure that your wireless controller version is compatible with the Cisco Hyperlocation Access Points in your network.
- Ensure that Cisco Spaces supports the wireless controller version. For more information, see Compatibility Matrix.
- If a Cisco CMX and a Cisco Spaces account are both connected to the same wireless controller, ensure that you disable Cisco Hyperlocation on Cisco CMX.

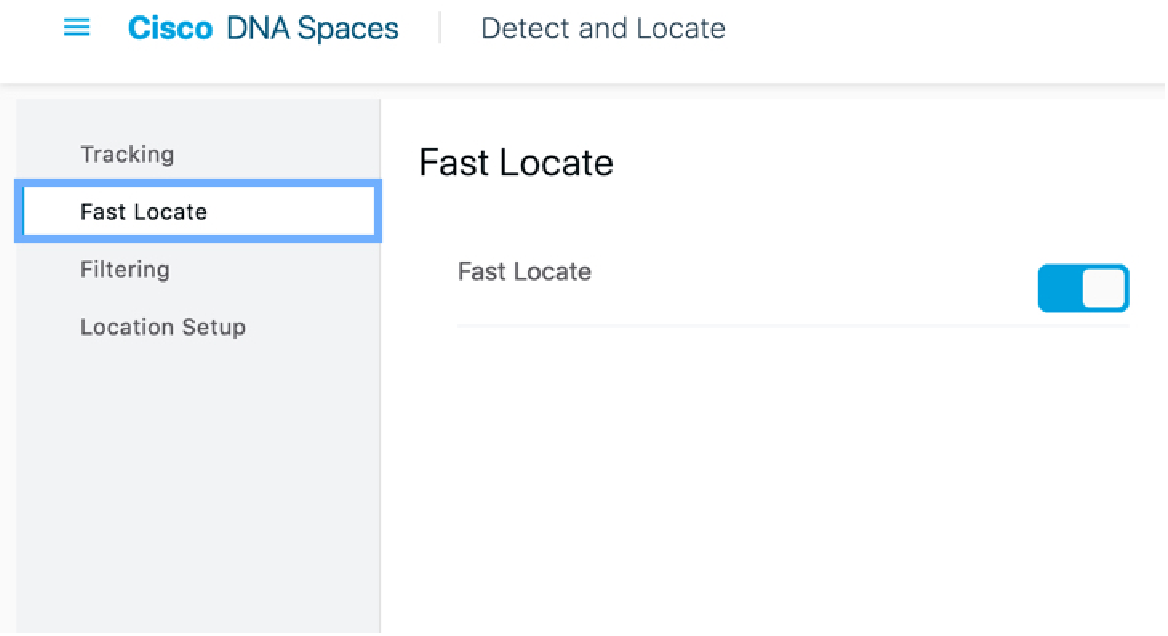
Step 1 Enable Hyperlocation on wireless controller.

For more details about how to enable hyperlocation on a wireless controller, see **Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide**

Step 2 Enable Hyperlocation on Cisco Spaces: Detect and Locate.

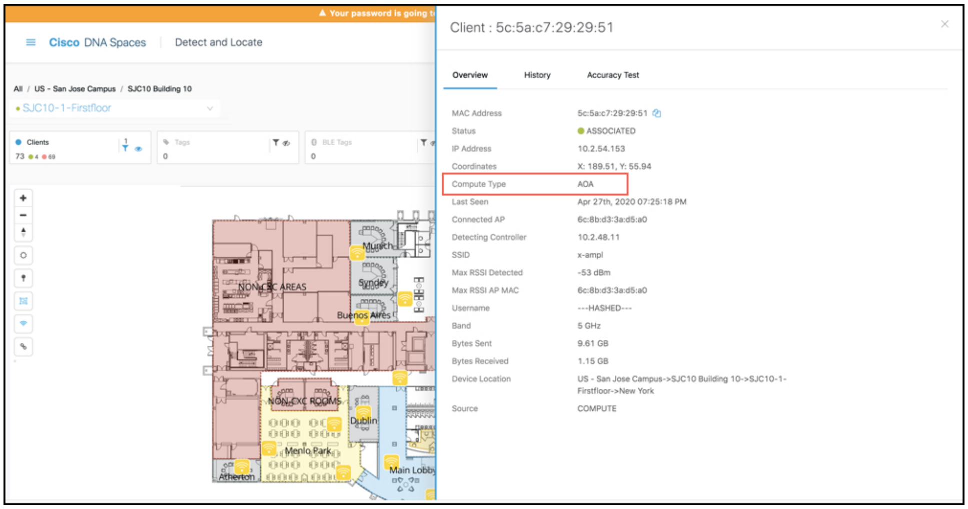
Navigate to Cisco Spaces: Detect and Locate dashboard. On the left-navigation pane, click **Configure** and enable the **Fast Locate** option.

Figure 55: Enabling Hyperlocation on Cisco Spaces: Detect and Locate



Step 3 Verify if Cisco Spaces: Detect and Locate is receiving Angle of Arrival (AoA) packets from client devices.

Navigate to the Cisco Spaces: Detect and Locate dashboard and checking if the **Compute Type** of a client device is AoA or Fusion.



Client : 5c:5a:c7:29:29:51

MAC Address	5c:5a:c7:29:29:51
Status	● ASSOCIATED
IP Address	10.2.54.153
Coordinates	X: 189.51, Y: 55.94
Compute Type	AOA
Last Seen	Apr 27th, 2020 07:25:18 PM
Connected AP	6c:8b:d3:3a:d5:a0
Detecting Controller	10.2.48.11
SSID	x-ampl
Max RSSI Detected	-53 dBm
Max RSSI AP MAC	6c:8b:d3:3a:d5:a0
Username	---HASHED---
Band	5 GHz
Bytes Sent	9.61 GB
Bytes Received	1.15 GB
Device Location	US - San Jose Campus->SJC10 Building 10->SJC10-1-Firstfloor->New York
Source	COMPUTE

- Angle of Arrival (AoA): AoA uses AoA-phase measurements to triangulate a device location. Several hyperlocation APs that are around the device report these AoA phase measurements. The AoA-compute type can achieve this more precise location of the device only if the device is within the convex hull of these hyperlocation APs.
- Fusion: Fusion combines the results of RSSI-location computation and AoA-location computation. These computations estimate the most-likely location of a device. The **Compute Type** field is Fusion when the location engine detects and concludes that a device is not within the convex-hull of Hyperlocation APs.

CHAPTER 15

Configure Cisco FastLocate

- Configuring Cisco FastLocate, on page 77

Configuring Cisco FastLocate

The Cisco FastLocate technology improves the location-refresh rate of connected wireless clients so that Cisco Spaces captures more location data points.

Whenever available, RSSI from data packets and probe frames is used for calculating the location of a device. A good location-accuracy test result for an RSSI deployment is 10 meters. Cisco FastLocate does not improve the accuracy of this result. But with an update frequency that is more than once in 30 seconds for active devices, the result improves to a value below 10 meters.

The Cisco FastLocate technology is available on both centrally switched WLANs and FlexConnect (locally switched WLANs).

The following wireless controllers support Cisco FastLocate:

- Supported on Cisco AireOS Wireless Controller, Release 8.1.122.0 and later.
- Supported on all releases of Cisco Catalyst 9800 Series Wireless Controllers

The following Wi-Fi 6 access points support Cisco FastLocate:

- Cisco Catalyst 9120 Series Access Points
- Cisco Catalyst 9130 Series Access Points

The following access points support Cisco FastLocate:

- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points

How to Configure Cisco FastLocate

This task shows you how to enable Cisco FastLocate on your network. The task also shows you how to verify if Cisco Spaces is receiving Cisco FastLocate packets from the client devices.

From every active and associated device, Cisco Spaces receives packets every 10 seconds. This is called packet rate frequency. For standard RSSI, packet frequency depends on device probing. But a typical frequency of the Wi-Fi probe packets is 30 seconds to one minute.

Before you begin

- Ensure that your Cisco FastLocate supported APs are compatible with the installed version of wireless controller. For more information on versions of wireless controller compatible with Cisco Spaces, see Compatibility Matrix.
- If a Cisco CMX and a Cisco Spaces account are both connected to the same wireless controller, ensure that you disable Hyperlocation on Cisco CMX so that the Cisco FastLocate stream is available for Cisco Spaces.

Step 1 Enable Hyperlocation on wireless controller.

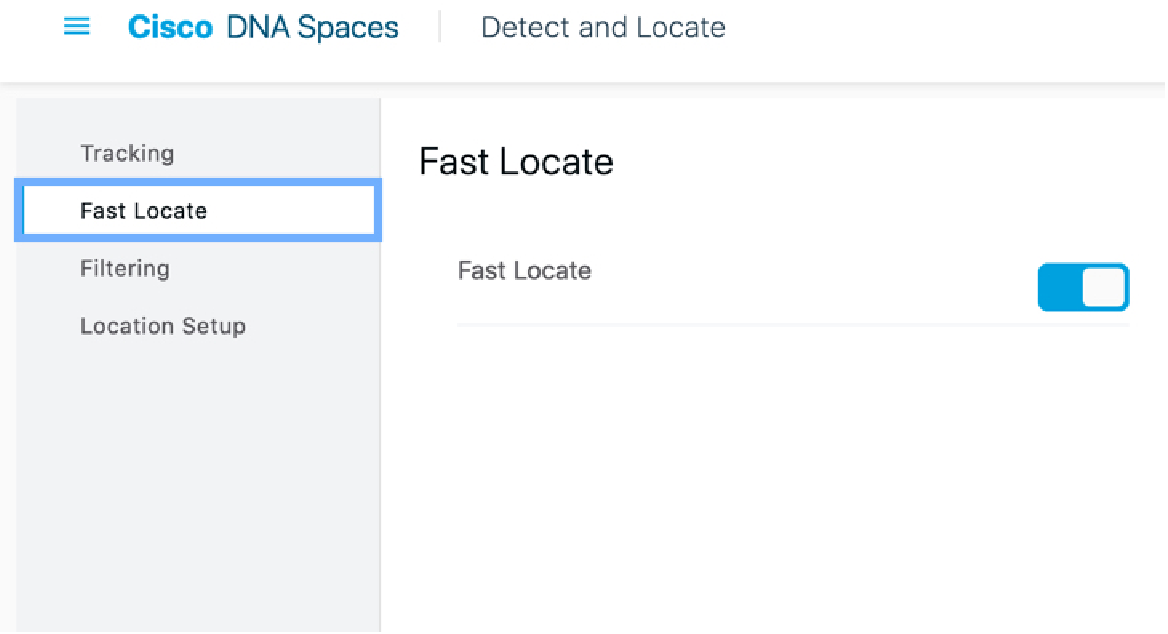
For instructions on how to enable hyperlocation on your specific wireless controller, see the respective configuration guide of your installed version.

For instructions on how to enable hyperlocation on Cisco Catalyst 9800 Series Wireless Controllers, see the **Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide**.

Step 2 Enable Cisco FastLocate on Cisco Spaces: Detect and Locate.

Navigate to Cisco Spaces: Detect and Locate dashboard, and on the left-navigation pane, click **Configure** and enable **Fast Locate**.

Figure 56: Enabling Cisco FastLocate on Cisco Spaces: Detect and Locate



Fast Locate

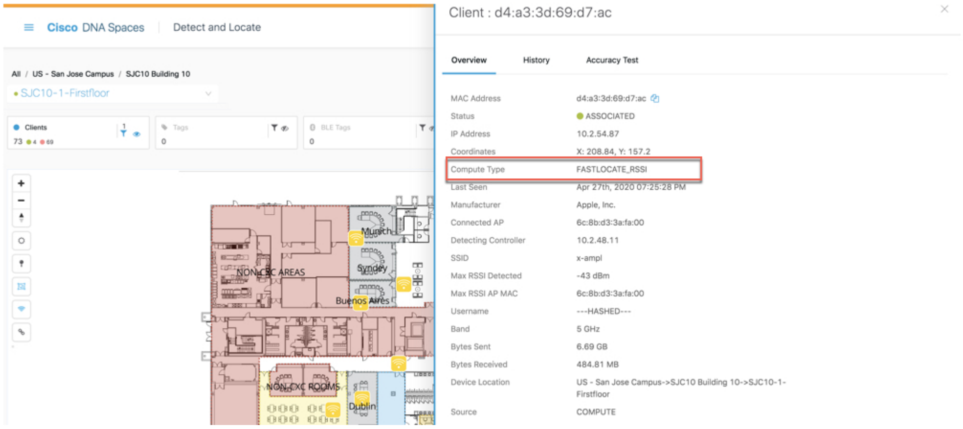
Fast Locate ●

Step 3 Verify if Cisco Spaces: Detect and Locate is receiving Cisco FastLocate RSSI packets from client devices.

Navigate to the Cisco Spaces: Detect and Locate dashboard and checking if the **Compute_Type** of a client device is Fastlocate_RSSI.

Note You may observe client devices continuing to display a **Compute_Type** of RSSI even after you have enabled Cisco FastLocate:

- If the client device is not active.
- Depending on the type of client device, for example, you may observe this behaviour on iPads and certain mobile phone.



Client : d4:a3:3d:69:d7:ac

MAC Address	d4:a3:3d:69:d7:ac
Status	● ASSOCIATED
IP Address	10.2.54.87
Coordinates	X: 208.84, Y: 157.2
Compute Type	FASTLOCATE_RSSI
Last Seen	Apr 27th, 2020 07:25:28 PM
Manufacturer	Apple, Inc.
Connected AP	6c:8b:d3:3a:fa:00
Detecting Controller	10.2.48.11
SSID	x-ampl
Max RSSI Detected	-43 dBm
Max RSSI AP MAC	6c:8b:d3:3a:fa:00
Username	---HASHED---
Band	5 GHz
Bytes Sent	6.69 GB
Bytes Received	484.81 MB
Device Location	US - San Jose Campus->SJC10 Building 10->SJC10-1-Firstfloor
Source	COMPUTE

PART VII

Manage Users

CHAPTER 16

Manage Users

Manage Users

Configure User Roles and Invite Users

Cisco Spaces: Detect and Locate users have role-based access control (RBAC), where users or groups of users are provided with various user roles. User roles have different restrictions based on the permissions that are associated with each role. The available permissions are **AdminAccess**, **ReadOnlyAccess, and SiteAdminAccess** and these define the locations and sites an associated user has access to. A user's Cisco Spaces: Detect and Locate dashboard displays only those locations that are defined for the particular user role.

Table 4: Permissions and Privileges

Permissions	Privilege
AdminAccess	Read and write access to entire system.
ReadOnlyAccess	Read only access.
SiteAdminAccess	Read and write access at site-level.

Before you begin

Upload maps.

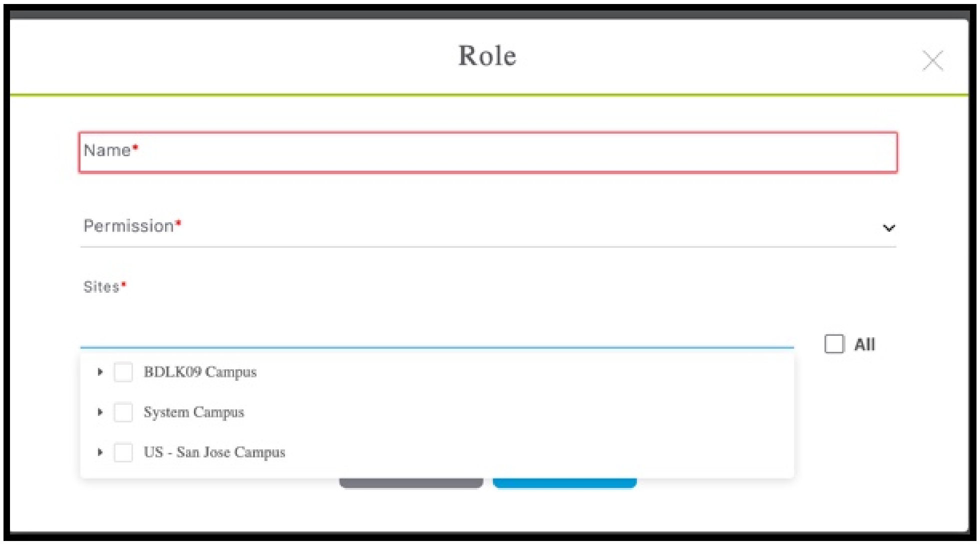
Step 1 In the left navigation pane, click **User Management** > **User Roles**. From the **Roles** window, Click the **Add** button.

Step 2 In the **Role** window, do the following:

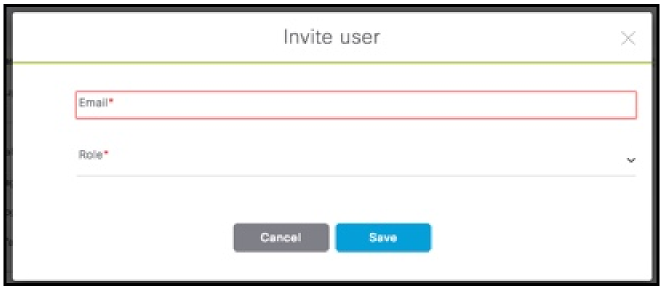
a) **Name**: Enter a name for the user role.

b) **Permission**: Choose a permission from the drop-down list.

c) Choose specific **Sites** from the drop-down list.



Step 3 Invite users by entering their email IDs and choosing a **Role** as configured in Step 2.



Modifying Users and User Roles

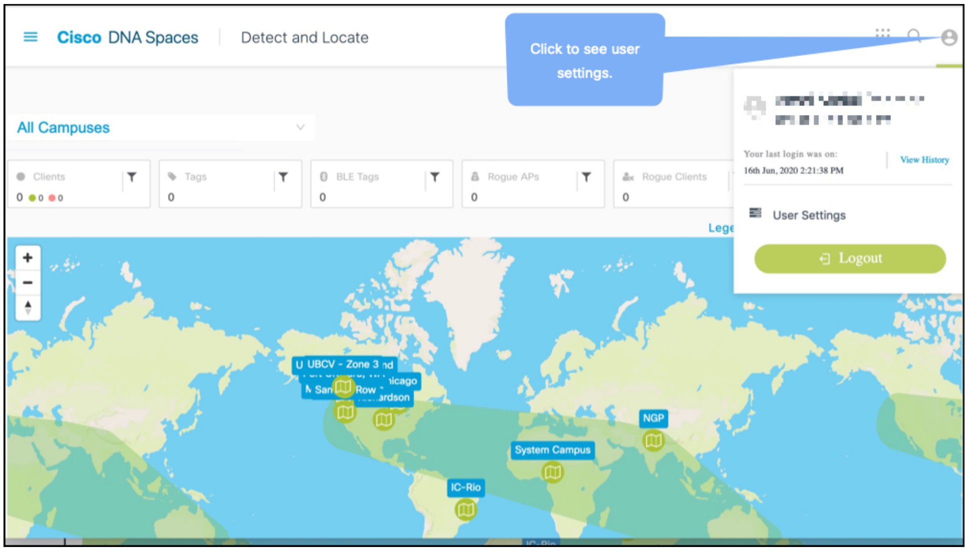
You, as an administrator, cannot modify the personal details of a user. The user also cannot modify his personal details from the **User Management** window.

The Detect and Locate Administrator can modify User Roles only. The Detect and Locate Administrator can edit the role of a specific user by editing user details from **User Management** > **App Users**.

Users listed under **User Management** > **Administrators** are administrators defined in the Cisco Spaces dashboard. This type of user cannot be edited from Detect and Locate, and can be edited from the Cisco Spaces dashboard only.

Step 1 To modify user details, users must log in to their respective accounts on the Detect and Locate dashboard and navigate to **User Settings**.

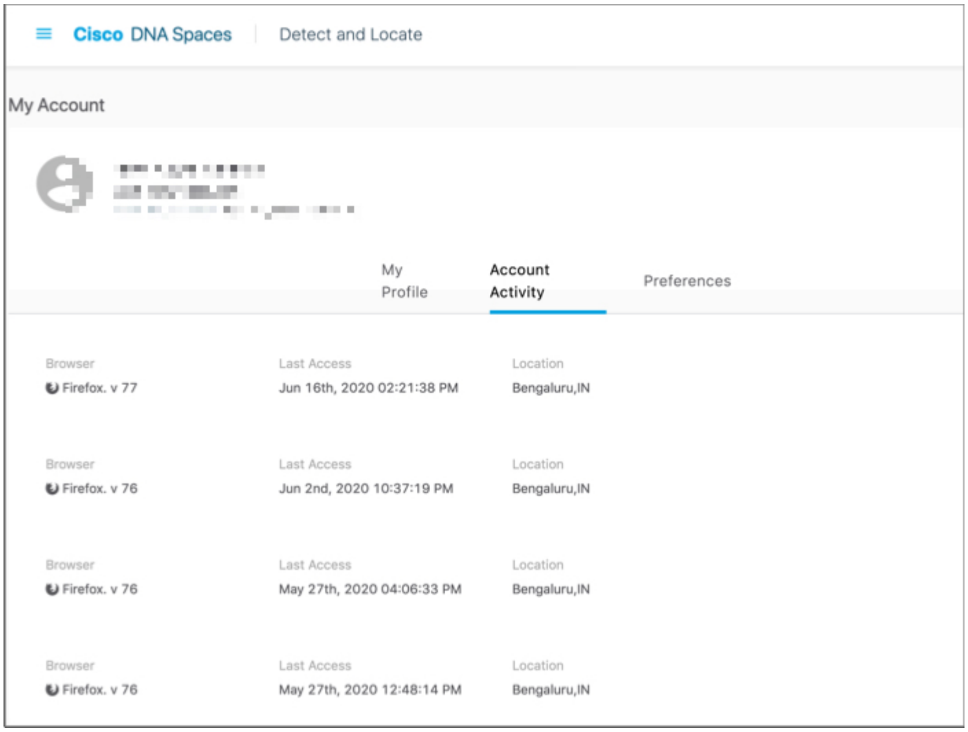
Figure 57: Modifying personal details from User Settings



Step 2 From the **Preferences** tab, you can set the following

- Map auto refresh (in seconds): Select how often your location list and map refreshes automatically to reflect your assets' movement.
- Client display icon: Decide how a client is to be represented on the Detect and Locate dashboard.
- AP Label Setting
- Enable Sticky Clients

Step 3 From the **Account Activity** tab, you can observe dasboard access activity, such as browsers used, access time, and location.



[redacted]

Browser	Last Access	Location
Firefox. v 77	Jun 16th, 2020 02:21:38 PM	Bengaluru,IN
Firefox. v 76	Jun 2nd, 2020 10:37:19 PM	Bengaluru,IN
Firefox. v 76	May 27th, 2020 04:06:33 PM	Bengaluru,IN
Firefox. v 76	May 27th, 2020 12:48:14 PM	Bengaluru,IN

PART VIII

FAQs

CHAPTER 17

Manage FAQs

How Can I Get Support?

Write to spaces@cisco.com to get support for issues related to your Cisco Spaces: Detect and Locate account.

What Information is Stored in My Cisco Spaces: Detect and Locate Account and for How Long is it Stored?

The following information is stored in your Cisco Spaces: Detect and Locate account:

- Location of your clients
- Maps

The information is retained until your Cisco Spaces: Detect and Locate account is deleted.

PART IX

API

CHAPTER 18

API

Using Rest APIs

You can use REST APIs to retrieve, add, or modify information on Cisco Spaces: Detect and Locate. The REST APIs are divided into five categories:

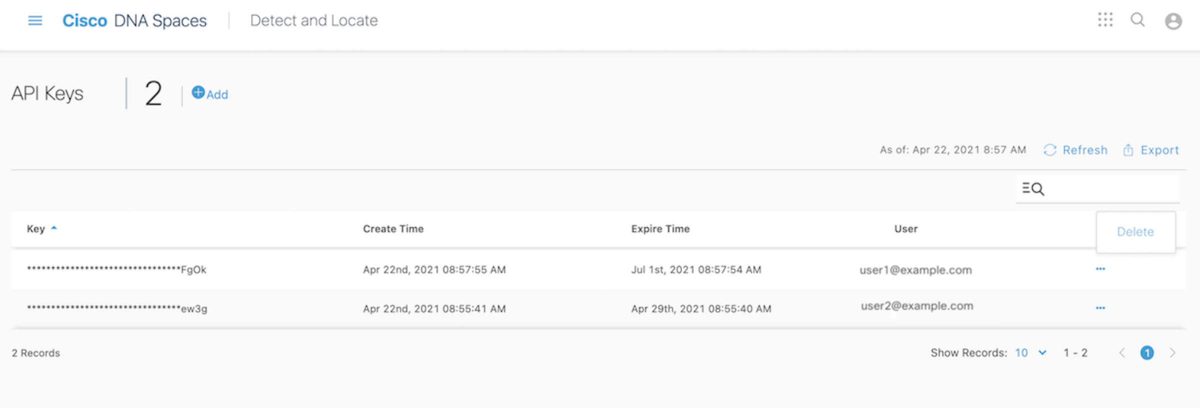
- **Active clients' location APIs**: APIs to retrieve client count and location data.
- **Clients location history APIs**: APIs to get a MAC address and the details for a given device.
- **Notifications APIs**: APIs for subscription-based notifications.
- **Map APIs**: APIs to upload, navigate the maps hierarchy, retrieve, and delete a map element.
- **Access point APIs**: APIs to get access point details.

API Key

To use REST APIs, you must generate an API Key. An API key is a Cisco-proprietary JSON Web Token (JWT) that is required in each HTTP request header to authenticate and authorize users.

You can generate an API Key from Cisco Spaces: Detect and Locate. Navigate to **Notifications** > **API Keys** and then click **Add**. You are prompted to configure the number of days after which the key should expire. Valid range is between 7 days and 365 days. After the key is generated, ensure that it is stored safely.

Figure 58: API Keys



API Keys | 2 | Add

As of: Apr 22, 2021 8:57 AM   Refresh   Export

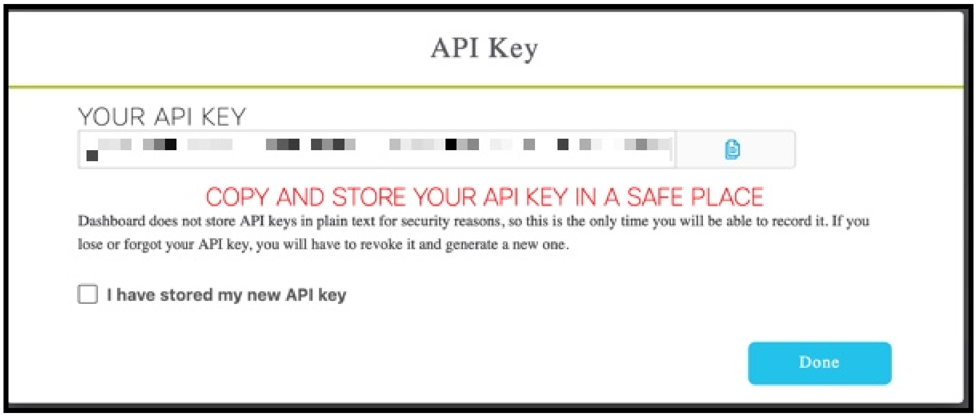
Key	Create Time	Expire Time	User	Delete
********************************FgOk	Apr 22nd, 2021 08:57:55 AM	Jul 1st, 2021 08:57:54 AM	user1@example.com	···
********************************ew3g	Apr 22nd, 2021 08:55:41 AM	Apr 29th, 2021 08:55:40 AM	user2@example.com	···

2 Records   Show Records: 10   1 - 2   1

The **API Keys** window shows the key names (only partially displayed), the date and time at which they were created, the date and time at which they are going to expire, and email IDs of the users who created the keys. To delete a key, click on the three dots icon in the **Actions** column and then click **Delete**. If you delete a key, the key is not revoked and you can still use it until its expiry date and time.

Note The API key is visible only at creation time, and hence must be stored securely. Cisco Spaces: Detect and Locate does not save the API key values. Each authenticated user can have up to five keys.

Figure 59: Copy the API Key



API Key

YOUR API KEY

[redacted]

COPY AND STORE YOUR API KEY IN A SAFE PLACE

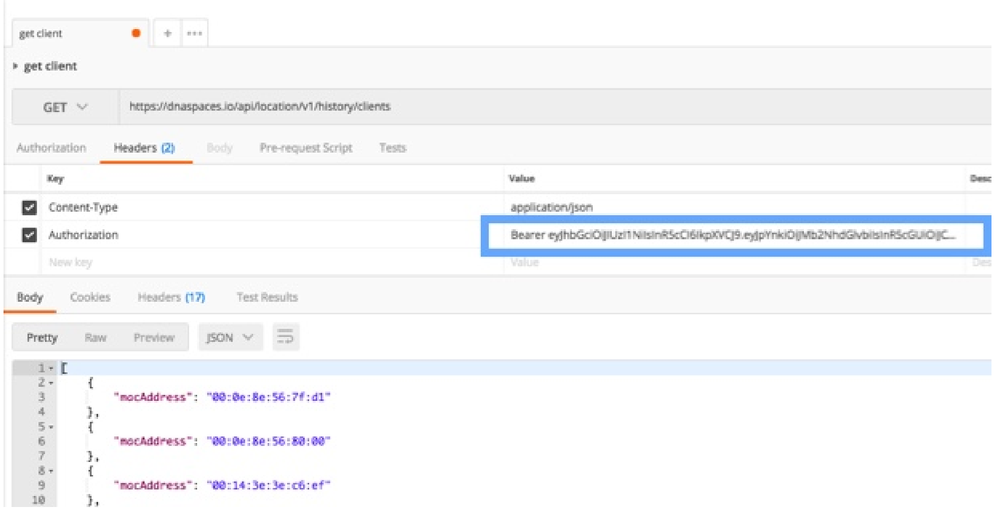
Dashboard does not store API keys in plain text for security reasons, so this is the only time you will be able to record it. If you lose or forgot your API key, you will have to revoke it and generate a new one.

□ I have stored my new API key

Done

The following is an example from the POSTMAN client, where an API key has been used as an **Authorization header**.

Figure 60: API Keys



get client

GET https://dnaspaces.io/api/location/v1/history/clients

	Key	Value	Desc
☑	Content-Type	application/json	
☑	Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYnkiOiJMb2NhdGlvbiIsInR5cGUiOiJC...	
	New key	Value	Des

```
[
    {
        "mocAddress": "00:0e:8e:56:7f:d1"
    },
    {
        "mocAddress": "00:0e:8e:56:80:00"
    },
    {
        "mocAddress": "00:14:3e:3e:c6:ef"
    },
```