



Cisco Spaces: Detect and Locate Configuration Guide

First Published: 2019-01-29

Last Modified: 2022-09-01

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

PREFACE

Audience vii

Conventions vii

Related Documentation viii

Communications, Services, and Additional Information viii

Cisco Bug Search Tool viii

Documentation Feedback viii

PART I

Product Overview 9

CHAPTER 1

Product Overview 1

Introduction to Cisco Spaces: Detect and Locate 1

Licensing 3

PART II

Getting Started 5

CHAPTER 2

Setup 7

Requesting a Cisco Spaces: Detect and Locate Account 7

CHAPTER 3

Data Source 9

Configuring Location Data Source 9

Configuring Location Data Source 9

CHAPTER 4

Deployment Information 11

Deployment Information 11

PART III **Track and Trace** 13

CHAPTER 5 **Manage Maps** 15

- Manage Maps 15
 - Uploading Maps to Cisco Spaces: Detect and Locate 15
 - Viewing the Map on Cisco Spaces: Detect and Locate 15
 - Create Zones 20
-

CHAPTER 6 **Sticky Clients** 23

- Sticky Clients 23
-

CHAPTER 7 **Client History** 27

- Client History 27
 - Viewing Client History and Playback 27
-

CHAPTER 8 **Location Accuracy** 33

- Location Accuracy 33
 - Testing Location Accuracy 33
-

CHAPTER 9 **Global Search** 39

- Global Search 39
 - Global Search 39
-

CHAPTER 10 **Device Tracking** 41

- Device Tracking 41
 - Enable or Disable Device Tracking 41
 - Configuring Thresholds and Cutoffs 42
 - Filtering Tracked Devices 43
 - Filtering Tracked Devices 43
-

CHAPTER 11 **Manage Columns** 45

- Manage Columns 45

CHAPTER 12	Manage Session Expiry	47
	Session expiry	47
	Manage Sessions Expiry	47

PART IV	Manage Notifications	49
----------------	-----------------------------	-----------

CHAPTER 13	Using Northbound Notifications	51
	Using Northbound Notifications	51
	Location Update (Northbound Notification)	51
	Absence (Northbound Notification)	53
	Association (Northbound Notification)	54
	In/Out (Northbound Notification)	56

PART V	Hyperlocation and FastLocate	59
---------------	-------------------------------------	-----------

CHAPTER 14	Configuring Hyperlocation	61
	Enabling Cisco Hyperlocation	61
	How to Configure Cisco Hyperlocation	62

CHAPTER 15	Configure Cisco FastLocate	65
	Configuring Cisco FastLocate	65
	How to Configure Cisco FastLocate	65

PART VI	Manage Users	69
----------------	---------------------	-----------

CHAPTER 16	Manage Users	71
	Manage Users	71
	Configure User Roles and Invite Users	71
	Modifying Users and User Roles	72

PART VII	FAQs	75
-----------------	-------------	-----------

CHAPTER 17	Manage FAQs	77
-------------------	--------------------	-----------

How Can I Get Support? 77

What Information is Stored in My Cisco Spaces: Detect and Locate Account and for How Long is it Stored? 77

PART VIII **API** 79

CHAPTER 18 **API** 81

Using Rest APIs 81



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, on page vii](#)
- [Related Documentation, on page viii](#)
- [Communications, Services, and Additional Information, on page viii](#)

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 .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	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.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
<>	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: Connector Configuration Guide](#)

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

- [Product Overview, on page 1](#)



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, on page 1](#)
- [Licensing, on page 3](#)

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 Wi-Fi devices: 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.
- Active RFID Wi-Fi Tags: This information is displayed to help troubleshoot applications that use the Tag data.
- Rogue Access Points: These are APs that the 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 controller has detected and labeled as Rogue. The client MAC address is displayed along with the estimated location.
- Unassociated Wi-Fi devices: The location of these types of devices and their number is calculated on a best-effort basis and displayed.



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.



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.

Figure 1: Detect and Locate dashboard

Cisco Spaces is a location platform which tracks only active devices. Active devices are those devices that send a Wi-Fi probe packet at a periodic frequency of five minutes or less, and these probes are used to calculate location of the devices. How often devices send probes is device-driven, and hence not deterministic.

You cannot compare the Cisco Spaces client counts (both associated and probing) with the counts on the controller as there are fundamental differences in the design of both these Cisco components. Both the controller and Cisco DNA Center consider associated devices as active. Associated devices are devices that are merely associated to the network. And since Cisco DNA Center depends on Cisco Spaces for device locations, Cisco DNA Center displays such devices that are merely associated as un-positioned devices.

Tethering of a Cisco CMX device to Cisco Spaces is a design that should be used to help a customer transition to Cisco Spaces. This allows a customer an initial view of how devices are displayed on Cisco Spaces. Here too, you cannot compare the device counts on Cisco CMX and Cisco Spaces. For tethered devices, accuracy troubleshooting must be performed on Cisco CMX.

The controller does not require an active device to be constantly probing. While Cisco Spaces requires a a periodic probe frequency of five minutes or less. Hence, client devices that are shown active on the controller can be missing on Cisco Spaces. We call these as non-locatable devices.

Following is the list of possible reasons that devices could be indicated as missing on Cisco Spaces.

- Device is reported by an AP that has not been placed on map. If most of APs connected to the controller are not added to map, then devices reported by these APs will be missing.
- Associated clients probe less to save battery power and this has a direct impact on locating them accurately. Associated clients do not send probes when they enter an ultra-power reserve mode (sleeping mode and screen blanked out). This behavior prevents Cisco Spaces from locating a device. When the user unlocks the home screen or start streaming content, the device is active again and starts sending probes to the wireless network. Cisco Spaces thus unable to locate such inactive or sleeping devices.
- 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 controller even though they are not sending Wi-Fi probes, and such devices are considered as non-locatable devices

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

<https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html>.

Licensing

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



PART II

Getting Started

- [Setup, on page 7](#)
- [Data Source, on page 9](#)
- [Deployment Information, on page 11](#)



CHAPTER 2

Setup

- [Requesting a Cisco Spaces: Detect and Locate Account](#), on page 7

Requesting a Cisco Spaces: Detect and Locate Account

Request an account on Cisco Spaces by sending an email to cisco-dnaspaces-support@external.cisco.com requesting for a demo or live account creation on the Cisco Spaces dashboard. For more information, see [Getting Started with DNA Spaces Dashboard](#).



CHAPTER 3

Data Source

- [Configuring Location Data Source, on page 9](#)

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 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.



CHAPTER 4

Deployment Information

-
- [Deployment Information, on page 11](#)

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 controller
- APs you have placed on the uploaded map.

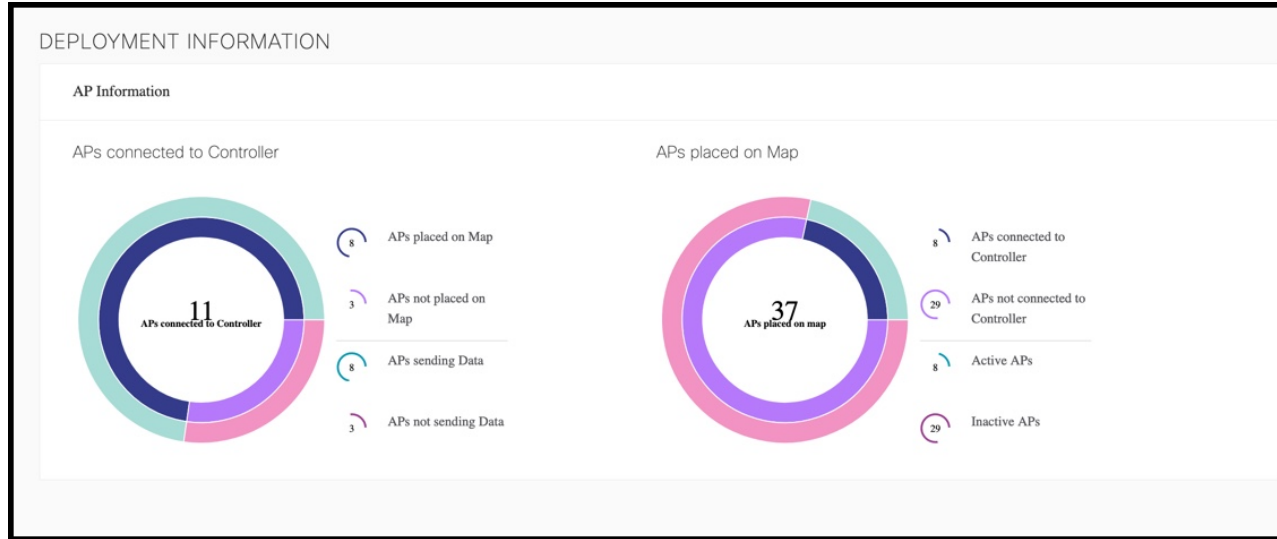
There are two graphs displayed on the **Deployment Information** page. One graph contains information collected from the controller and the other contains the same information collected from the Cisco Spaces maps. You can now compare the information in the two graphs and check if the information is the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

From the following image, you can observe the **APs connected to Controller** graph which provides information regarding the controller. This graph indicates that while 11 APs are connected to the controller, only eight are actually sending data to the controller. Three APs are not sending any data to the 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 regarding the Cisco Spaces maps. The graph shows that there are 37 APs on Cisco Spaces maps. This number includes access points that are active, inactive, and stale. Out of this, eight APs are connected to the controller and 29 are not connected to any controller, even though they are present on the Cisco Spaces maps.

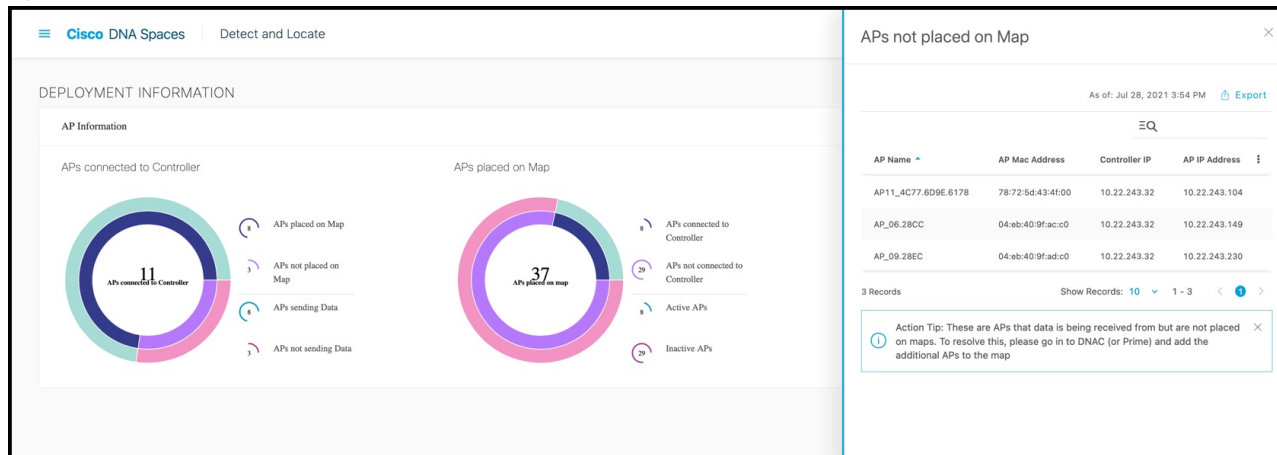
You can also identify which APs are inactive and why they are inactive. Inactive APs are placed on the Cisco Spaces map, but do not report the data they receive. Data is not reported because the APs are either not connected to the controller or they are connected but not sending the measured data. You 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 controller (**APs not connected to the controller**).

Figure 2:



Click on each metric to see a detailed list of APs.

Figure 3:





PART **III**

Track and Trace

- [Manage Maps, on page 15](#)
- [Sticky Clients, on page 23](#)
- [Client History, on page 27](#)
- [Location Accuracy, on page 33](#)
- [Global Search, on page 39](#)
- [Device Tracking, on page 41](#)
- [Manage Columns, on page 45](#)
- [Manage Session Expiry, on page 47](#)



CHAPTER 5

Manage Maps

- [Manage Maps](#), on page 15

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

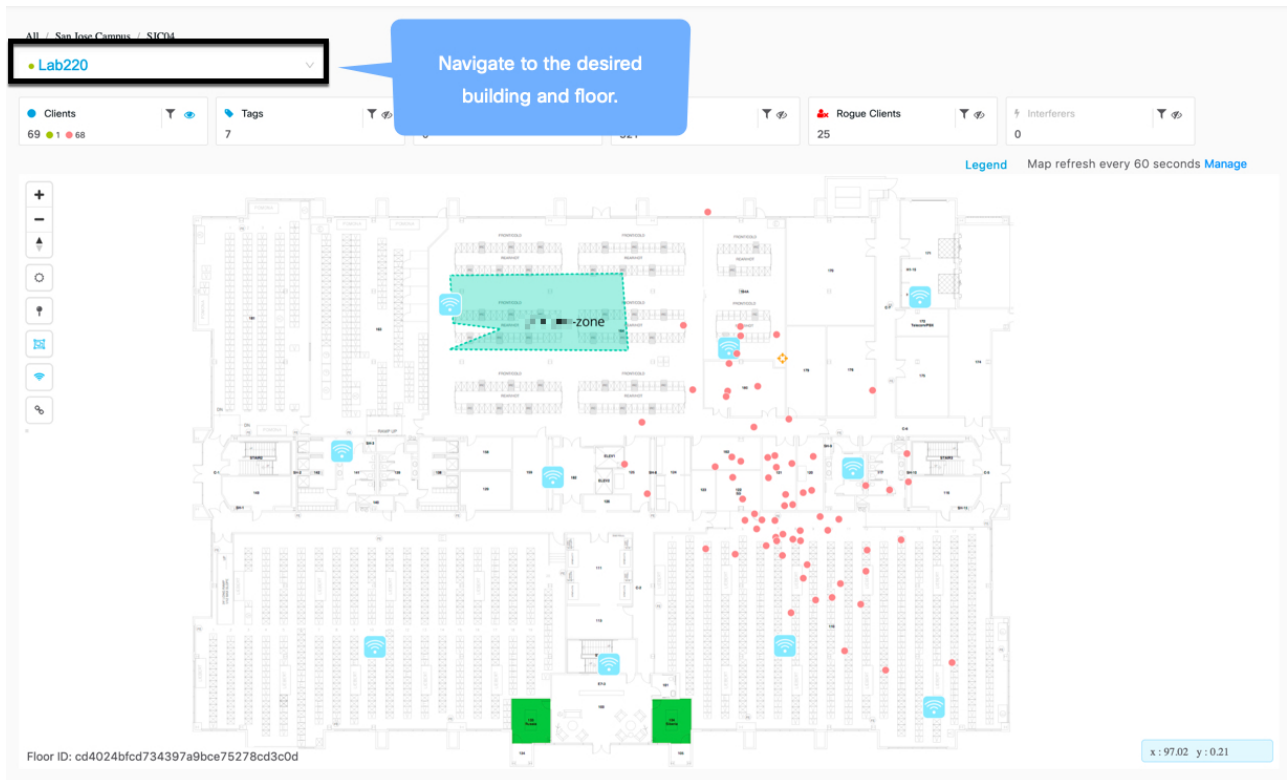
If Cisco Spaces: Detect and Locate is launched through Cisco Spaces, maps are automatically synchronized into through Cisco CMX tethering.

-
- 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

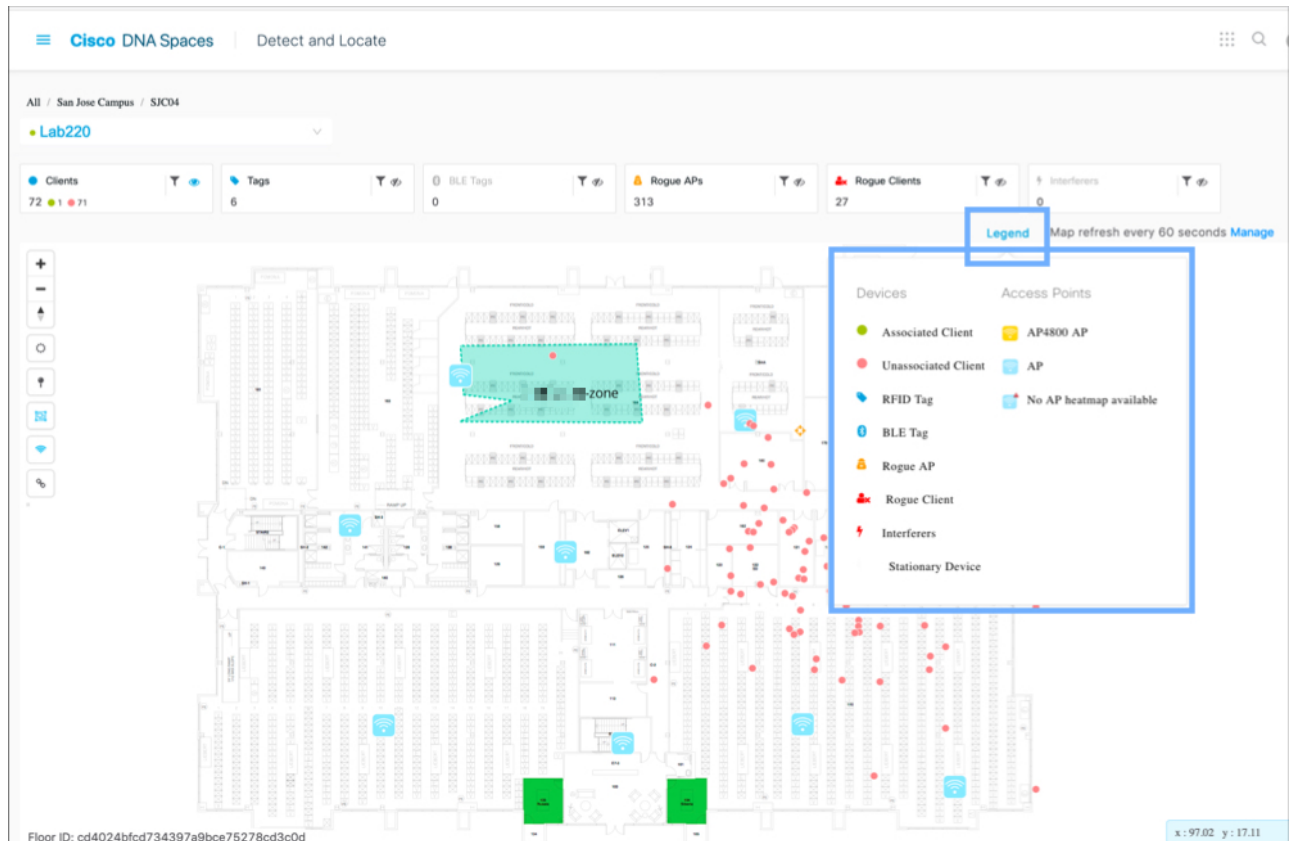
-
- Step 1** From the Cisco Spaces: Detect and Locate dashboard, use the drop-down list to navigate to the desired campus, building, and floor.

Figure 4: Cisco Spaces: Detect and Locate Dashboard



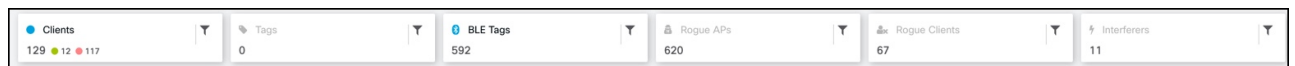
Step 2 Click **Legend** to understand the various markings on the map.




Figure 5: Legend

**Step 3**

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


Figure 6: 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 7: Dashboard: Left Toolbar







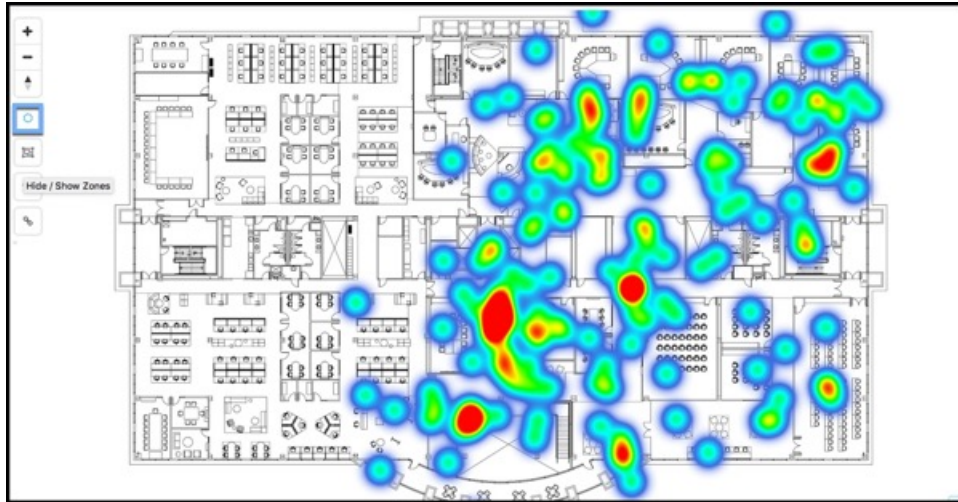
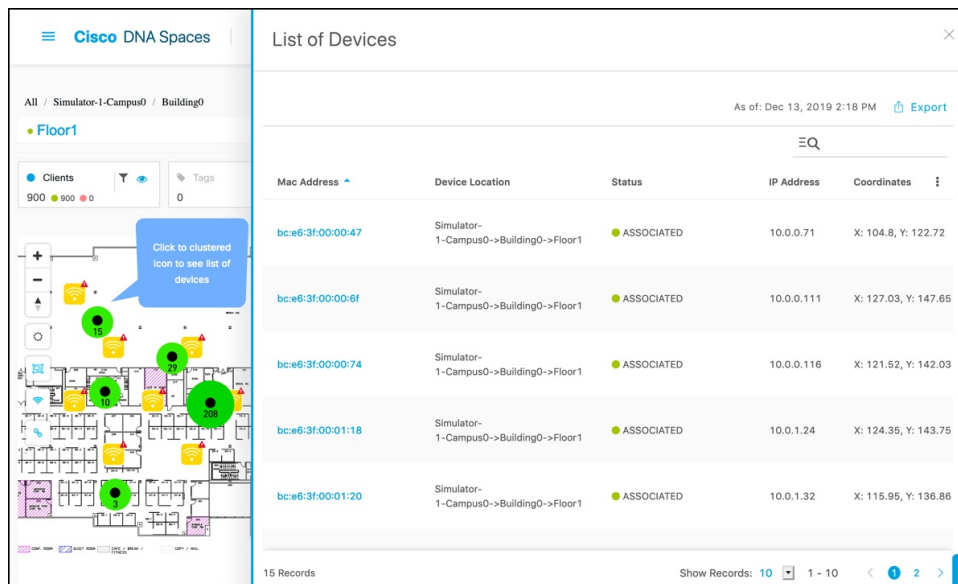
- Zones : Show or hide the zones on a specific floor.
- Access Point : Show or hide all the APs that have been deployed on a specific floor. If the map has been uploaded to Detect and Locate, your map indicates which APs have device location () and which APs have issues with device location and hence may need troubleshooting. ()
- Heatmap: Display the movement of various clients as a heatmap.

Figure 8: Heatmap



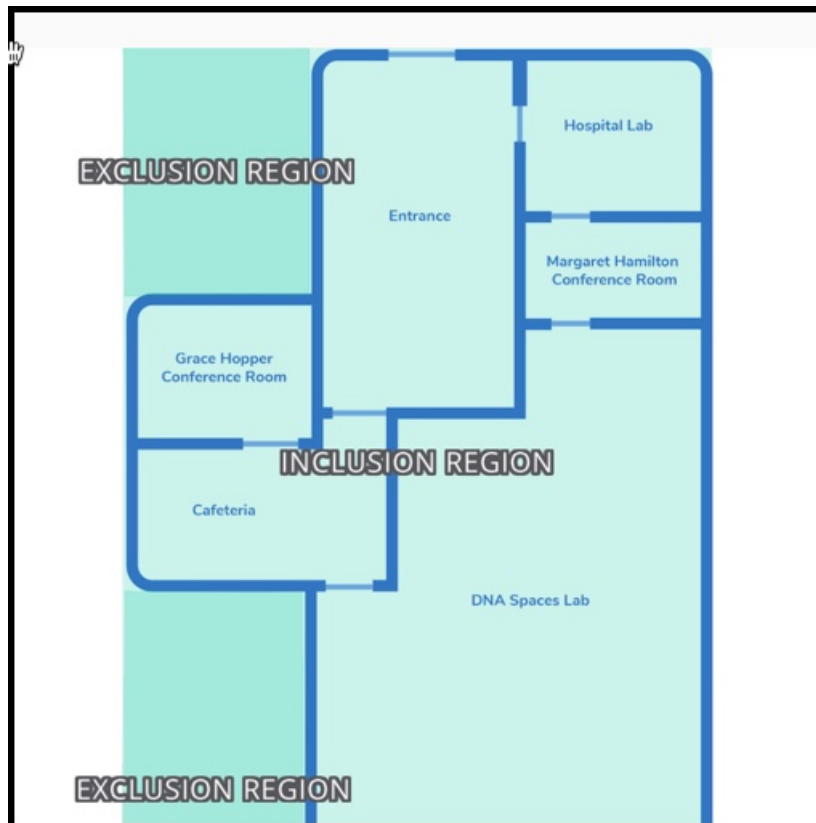
- **Clustering:** Enable clustering to group devices that are closely located and possibly overlapping. Click on the clustered icon to view list of devices in a separate window.

Figure 9: Clustering



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

Figure 10: Show/Hide Inclusion and Exclusion Regions

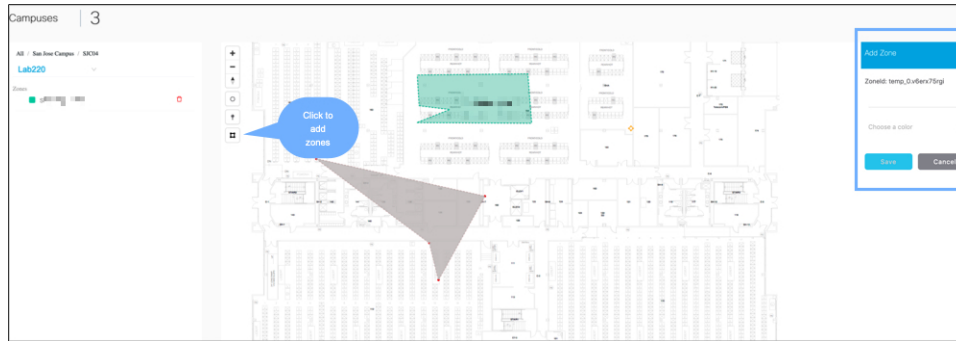


- Note**
- Only one inclusion zone per floor is possible.
 - You can add multiple exclusion zones per floor for areas where device tracking is unnecessary.

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 11: Create Zones





CHAPTER 6

Sticky Clients

- [Sticky Clients, on page 23](#)

Sticky Clients

Usually, an associated client is in closest proximity of the access point it is connected to, in comparison 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 12: Enable Sticky Clients

My Profile Account Activity **Preferences**

Map refresh time (in seconds) 60.00

5 60

Client display icon

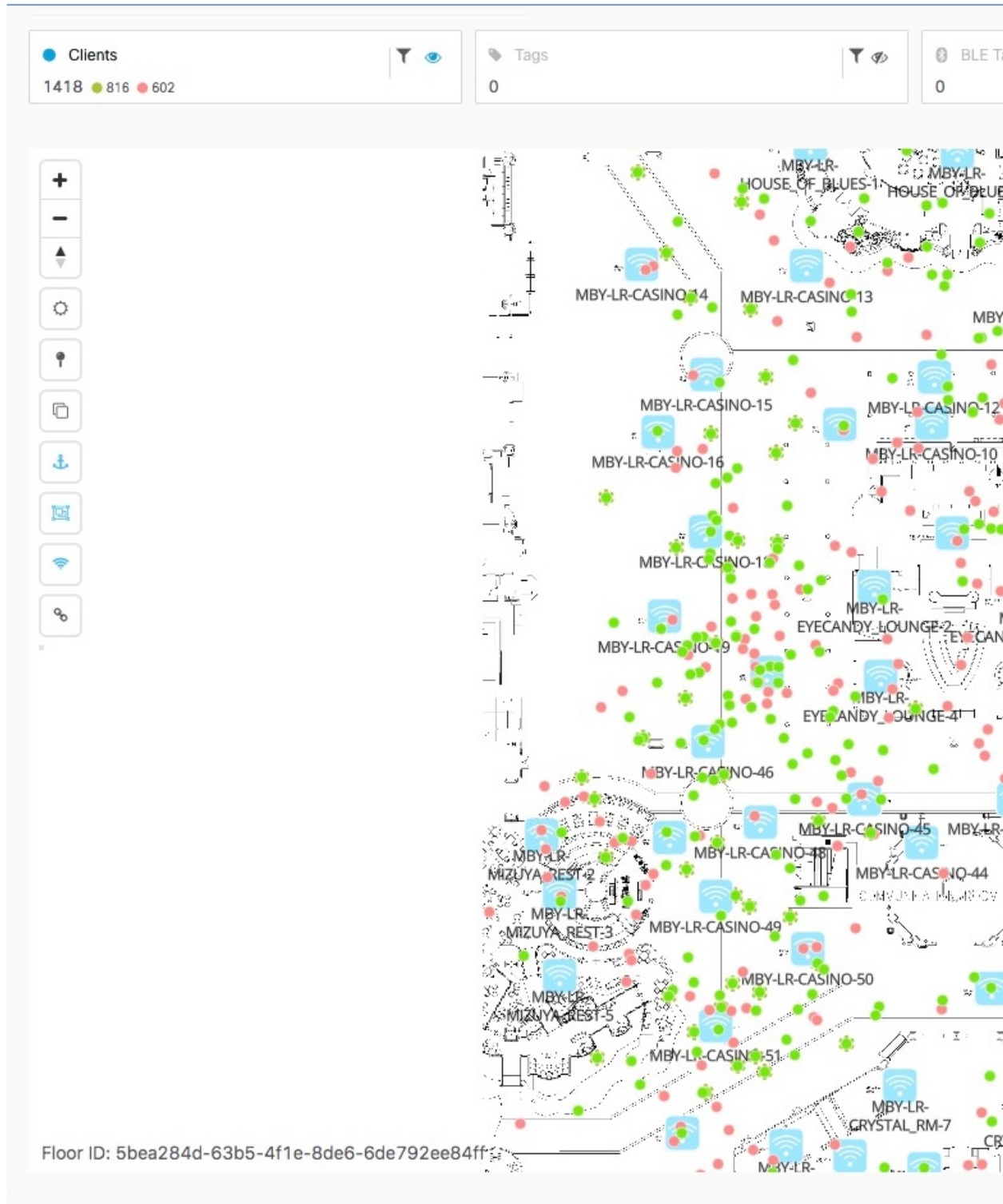
Circle Person

AP Label Setting

AP Name	AP Mac Address	AP Model	Hide Lab
---------	----------------	----------	----------

Enable Sticky Clients

Figure 13: Sticky Clients Displayed As Green Star Icon





CHAPTER 7

Client History

- [Client History](#), on page 27

Client History

Viewing Client History and Playback

The Client Playback feature enables you to locate and track the movement of clients in a venue. You can track the activity of only one client at a time.



Note Tracking information of a client is restricted to 30 days.

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

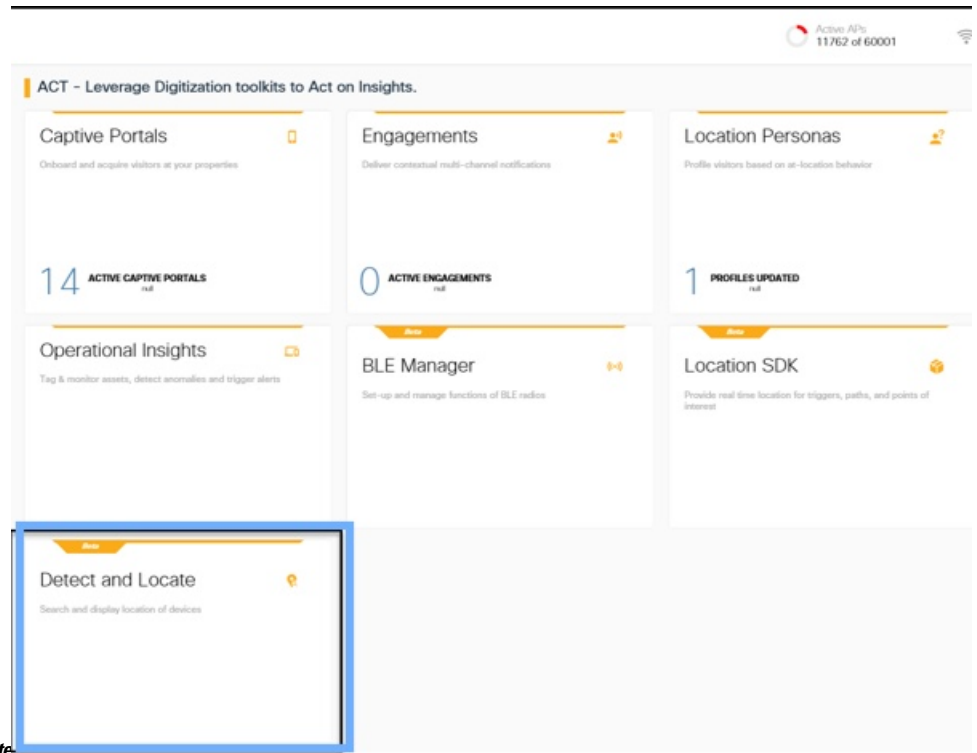
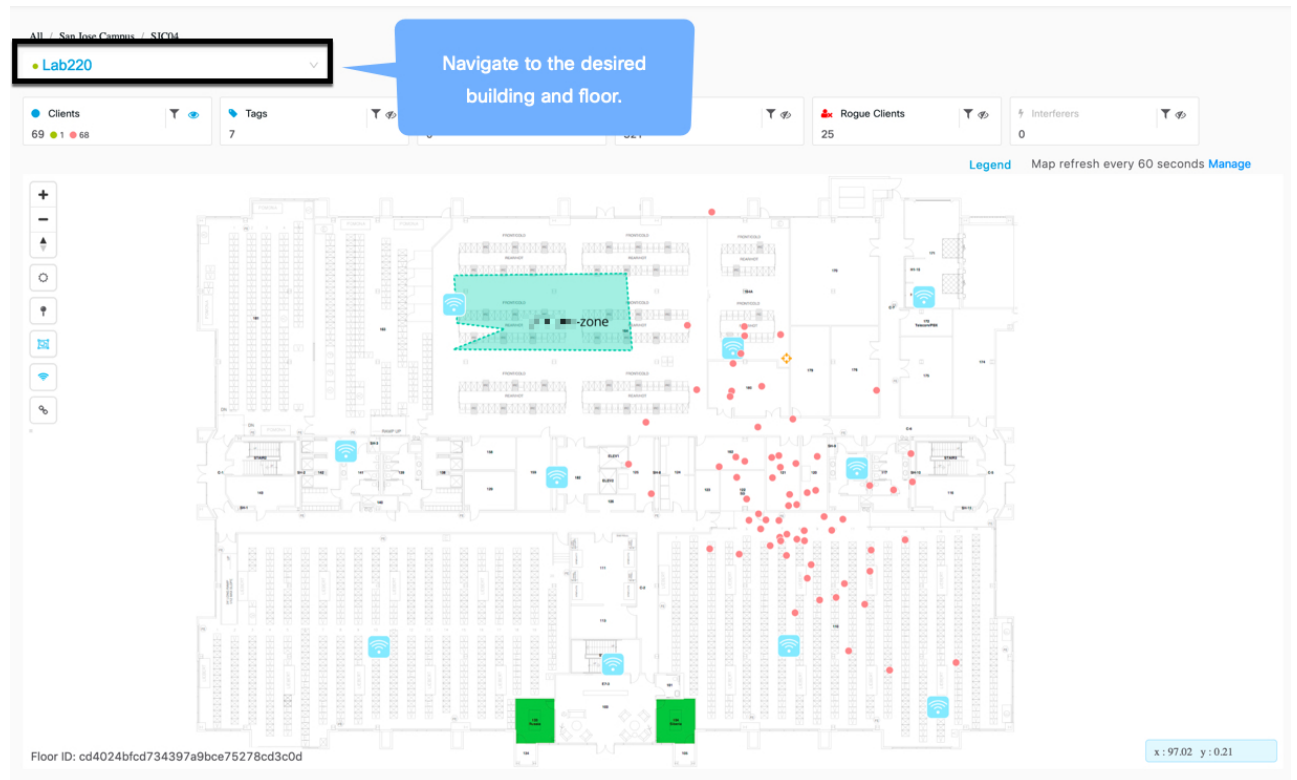


Figure 14: Cisco Spaces: Detect and Locate

- Step 2** From the Cisco Spaces: Detect and Locate dashboard, use the drop-down list to navigate to the desired campus, building, and floor.

Figure 15: Cisco Spaces: Detect and Locate Dashboard



Step 3 Ensure that all the tracked clients (connected and detected) are visible on the dashboard by using the **Show/Hide** button, which is represented by the eye icon of **Clients** on the top pane.

Figure 16: Eye Icon



Step 4 Click a green dot icon on the map to select a client, and view **Details**.

Figure 17: Cisco Spaces: Detect and Locate Dashboard

The screenshot displays the Cisco DNA Spaces interface. On the left, a floor plan is shown with numerous green dots representing client locations. A blue callout bubble points to the floor plan with the text "Select a device from the dashboard". On the right, a "List of Devices" panel is open, showing details for a selected device. The panel has tabs for "Overview", "History", and "Accuracy Test". The "Overview" tab is active, displaying the following information:

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
	10:00:01:01:00:00
	nmsp-sim-1
	ssid0
	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 5 Click **History** to see the client locations plotted over the past 24 hours (default setting).

Figure 18: Cisco Spaces: Detect and Locate Client History

The screenshot displays the Cisco Spaces Client History view. At the top, a timeline for "Mon, Jun 17th" is shown, with a time slot of 11:00 to 12:00. A blue callout bubble points to the timeline with the text "Time slot displayed can be varied". Below the timeline, a map shows a path of green dots with a red flag at the end. A blue callout bubble points to the red flag with the text "Red Flag indicates final point of the path". Another blue callout bubble points to a control icon on the left with the text "Hide or show blue paths".

Step 6 Observe the **Client History** represented in two forms:

- **Linear Time Frame:** Client history is represented as dots on a linear time frame, with two blue lines representing the start and end time. Location information is represented as dots, and you can hover your cursor to see the location for a given time.
- **Map:** Client location is plotted on a map as green and red dots. Red indicates that the device is still probing, and is not associated to the network. A client could be probing either because it is manually disconnected from the network or because of network issues. Green indicates that the device is connected. You can also observe that the dots plotted on the map in the form of green and red dots and connected with a blue line.

Step 7 Observe the client history which is represented as a heat map. A heat map is the plotting of the location chirps of a device, and indicates the locations travelled by the device. It helps identify suspicious device behavior and can also be used for tracking missing equipment.



CHAPTER 8

Location Accuracy

- [Location Accuracy](#), on page 33

Location Accuracy

Testing 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 (the administrator) 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.



Note

- The display refresh time is three seconds and cannot be reconfigured.
 - Location Accuracy testing is not supported on APs with external antennas. However, location detection is supported on these APs.
 - The location sample count that is displayed during an accuracy test is based on a best-effort estimate of location values collected during back end processes. This sample count may differ from actual samples that are captured in an accuracy test.
-

Step 1

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

Figure 19: Detect and Locate: Dashboard

The screenshot shows the Cisco DNA Spaces interface. On the left, there is a map of a building floor plan with various colored markers representing devices. The main panel is titled 'Global Search' and shows a search for 'IP Address 10.0.2.97'. A blue callout box points to the search input field with the text 'Search for devices'. Below the search bar, there are tabs for 'History' and 'Accuracy Test'. The 'Accuracy Test' tab is active, showing details for the device: MAC Address (bc:e6:3f:00:02:61), 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 (nmosp-sim-1), SSID (ssid2), Max RSSI Detected (-79 dBm), Username (Clientbc:e6:3f:00:02:61), and Band (2.4 GHz).

Step 2 Ensure that the **Status** of the device is **ASSOCIATED** and the **Source** is **COMPUTE**. To begin, click **Accuracy Test**.

Figure 20: Detect and Locate: Initiate Accuracy Test

The screenshot shows the 'List of Devices' panel in the Cisco DNA Spaces interface. The panel has three tabs: 'Overview', 'History', and 'Accuracy Test'. The 'Accuracy Test' tab is active. A blue callout box points to the 'Accuracy Test' tab with the text 'Click to start accuracy test'. The device details are: 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 (nmosp-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), and Device Location (Simulator-1-Campus0->Building0->Floor1).

Step 3 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 21: Detect and Locate: Initiate Accuracy Test

Client : 6c:19:c0:e5:87:3a ×

Overview History Accuracy Test

Report Name	X	Y	Test time (minutes)
6c:19:c0:e5:87:3a-12-03-2020	21.1	138.3	5


Unique test name **Start Test**

Stops in **35:00**
Data Collection **New**
Data Points **0**

+

-

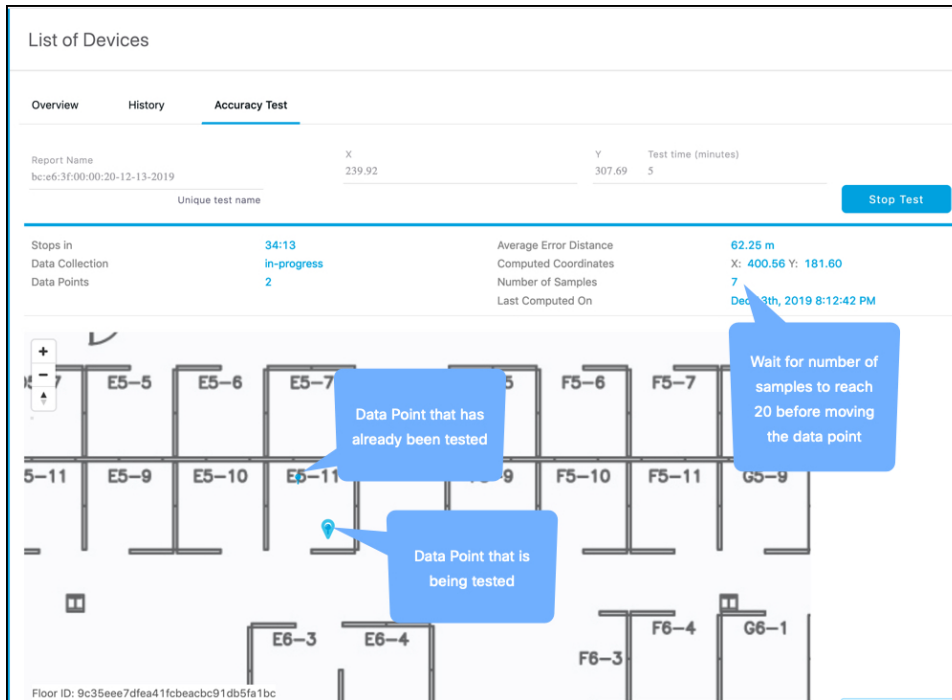
↑



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

Step 4

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.



Step 5 Repeat for multiple locations for a more accurate understanding of location accuracy.

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


Overview History **Accuracy Test**

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 floor plan visualization shows a detailed layout of a building with various rooms and corridors. Several rooms are highlighted in green, and one central room is highlighted in blue. A small orange box is also visible in the upper-middle section of the plan. To the left of the floor plan, there are three vertical navigation buttons: a plus sign (+), a minus sign (-), and an upward-pointing arrow (▲). A small logo is visible in the bottom right corner of the floor plan area.



CHAPTER 9

Global Search

- [Global Search, on page 39](#)

Global Search

Global Search

You can now perform a global search on all the assets tracked by your Cisco Spaces: Detect and Locate account. You can search assets based on any of the following parameters:

- Manufacturer
- IP Address
- SSID
- Username
- MAC Address



Note

- The information you enter in the **Search** field is case-insensitive.
 - You can also search by entering only a part of a string. For example, entering **bc** in the search field returns all the results containing the characters **bc**.
-



CHAPTER 10

Device Tracking

- [Device Tracking](#), on page 41
- [Filtering Tracked Devices](#), on page 43

Device Tracking

Enable or Disable Device Tracking

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

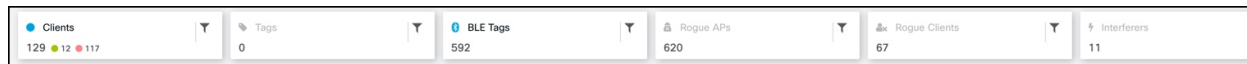
Choose **Configure > Tracking** to enable or disable the tracking of devices.

- Wireless Clients
- Interferers
- Rogue Access Points
- RFID
- Rogue Clients

View the enabled components from the Cisco Spaces: Detect and Locate dashboard.

Enable that the respective **Show/Hide** button (represented by the eye icon) so that you can view the component on the dashboard.

Figure 22: Dashboard: Total Count Toolbar



Cisco Spaces: Detect and Locate maintains a device eviction time of 10 minutes. As long as you receive updates (RSSI, AOA, Info, Stats) from the controller, the device is kept active and is displayed on the dashboard. If updates (RSSI, AOA, Info, Stats) are not received for a particular device within this eviction time, the device is removed from the system.

Configuring Thresholds and Cutoffs

Choose **Configure > Location Setup** to configure various thresholds and cutoffs.

Table 2: Thresholds and Cutoffs

Thresholds and Cutoffs	Descriptions
Relative discard RSSI time (secs)	Enter the time, in seconds, after which the RSSI measurement should be considered obsolete and discarded from use in location calculations. This time is from the most recent RSSI sample, and not an absolute time. For example, if this value is set to 3 minutes, and two samples are received at 10 minutes and 12 minutes, both the samples will be retained. However, an additional sample received at 15 minutes is discarded.
Absolute discard RSSI time (mins)	Enter the time, in minutes, after which the RSSI measurement should be considered obsolete and discarded from use in location calculations regardless of the most recent sample.
RSSI Cutoff (dBm)	Enter the RSSI cutoff value, in dBm, at which you want the server to discard AP measurements.

Figure 23: Configuring Thresholds and Cutoffs

The screenshot shows the 'Location Setup' configuration page. On the left is a navigation menu with options: Tracking, Fast Locate, Filtering, and location Setup (which is highlighted). The main content area is titled 'Location Setup' and contains three configuration items:

- Relative discard RSSI time (secs)**: The value is 60. A blue 'Save' button is to the right.
- Absolute discard RSSI time (mins)**: The value is 60. A blue 'Save' button is to the right.
- RSSI Cutoff (dBm)**: The value is -75. A blue 'Save' button is to the right.

Filtering Tracked Devices

Filtering Tracked Devices

You can filter tracked devices by various parameters from the **CONFIGURE > Filtering** tab.

Parameters	Description
RSSI Cutoff	Specify the cutoff value for filtering out weak probing clients. The cut off value allows Cisco Spaces: Detect and Locate to filter out weak probing clients in the initial stage.
Enable Locally Administered MAC Filtering:	Toggle button that allows you to enable or disable locally administered MAC filtering.
Exclude Probing Only client:	Toggle button allows you to exclude or include probing-only clients.
Allow MAC Address:	List of MAC addresses that are allowed.
Disallow MAC Addresses:	List of MAC addresses that are not allowed.
Enable MAC Filtering:	This toggle button allows you to enable or disable MAC filtering.
Allow Location SSID Filtering:	List of SSIDs that are allowed.
Disallowed Location SSID Filtering:	List of SSIDs that are not allowed.




CHAPTER 11

Manage Columns

- [Manage Columns, on page 45](#)

Manage Columns

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



CHAPTER 12

Manage Session Expiry

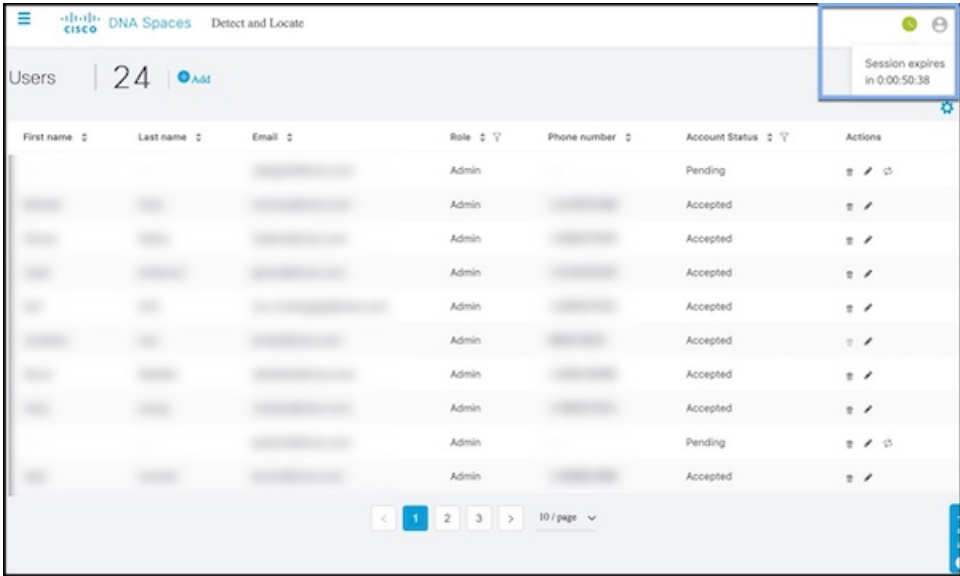
- [Session expiry, on page 47](#)

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 24: Session Expiry





PART **IV**

Manage Notifications

- [Using Northbound Notifications, on page 51](#)



CHAPTER 13

Using Northbound Notifications

- [Using Northbound Notifications](#) , on page 51

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 25: Location Update

The screenshot shows a 'Webhooks' configuration window. At the top is the title 'Webhooks' with a close button. Below it is a 'Name*' field. The 'Type' dropdown is highlighted with a blue box and set to 'LocationUpdate'. Under 'Conditions:', 'Device Type' is set to 'All' and 'Status' is a dropdown. The 'Assigned site*' field has a blue line and an 'All' checkbox. Below that is a 'MAC address list' field. The 'Receiver' field is highlighted with a blue box and shows 'http' in a dropdown, followed by a colon, a slash, and fields for 'host address', 'port', and 'url'. Below the receiver is a 'Headers' section with a '+' icon and 'Key' and 'Value' labels. The 'MAC Hashing*' section has a checked toggle switch. At the bottom is a 'Hash Key*' field and 'Cancel' and 'Save' buttons.

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 26: Absence

The screenshot shows a configuration window titled "Webhooks" with a close button (X) in the top right corner. The form contains the following fields:

- Name***: A text input field.
- Type**: A dropdown menu with "Absence" selected. This field is highlighted with a blue rectangular box.
- Conditions:**
 - Device Type**: A dropdown menu with "All" selected.
- MAC address list**: A text input field.
- Receiver**: A dropdown menu with "http" selected, followed by a colon and a slash. Below these are three input fields labeled "host address", "port", and "url".
- Headers**: A section with a plus sign (+) and two input fields labeled "Key" and "Value".
- MAC Hashing***: A text input field at the bottom.

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 27: Association

The screenshot shows a 'Webhooks' configuration window. At the top, there is a 'Name*' field. Below it is a 'Type' dropdown menu, which is highlighted with a blue border and currently shows 'Association'. Underneath is a 'Conditions:' section with a 'Device Type' dropdown set to 'Client'. An 'Association*' toggle switch is turned on. Below that is a 'MAC address list' text input field. At the bottom, there is a 'Receiver' dropdown set to 'http', followed by fields for 'host address', 'port', and '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 28: Absence

Webhooks X

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 subscription:

```
{
  tenantId: '2001',
  id: "552a1a14-20cb-4581-855d-f3c9f120248e",
  name: "Test InOut Notification",
  type: "InOut",
  userid: "testuser",
  enabled: true,
  internal: 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 **V**

Hyperlocation and FastLocate

- [Configuring Hyperlocation, on page 61](#)
- [Configure Cisco FastLocate, on page 65](#)



CHAPTER 14

Configuring Hyperlocation

- [Enabling Cisco Hyperlocation, on page 61](#)

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

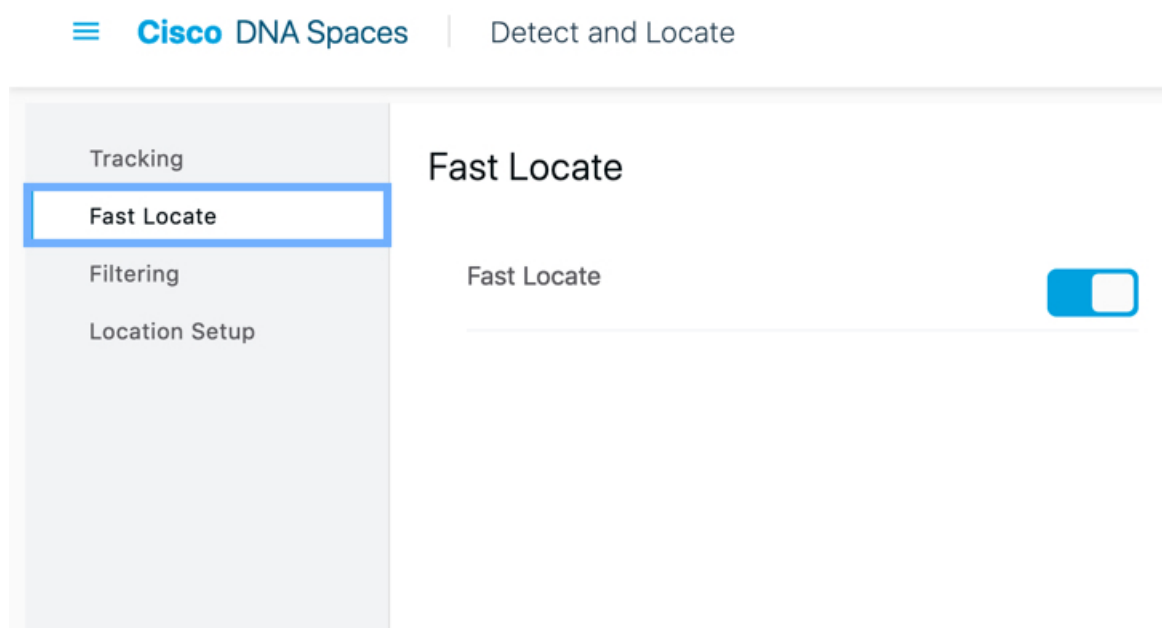
Step 1 Enable Hyperlocation on controller.

For more details about how to enable hyperlocation on a controller, see [Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide](#)

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

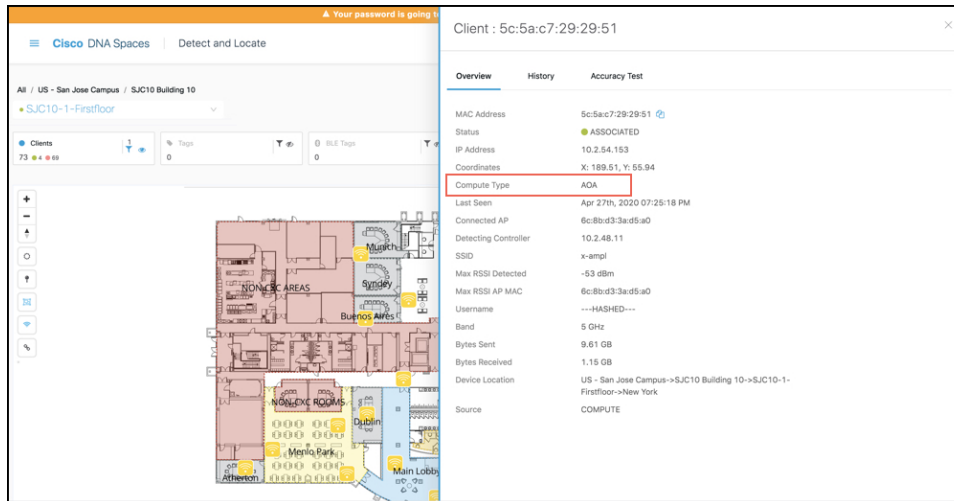
Navigate to Cisco Spaces: Detect and Locate dashboard. On the left-navigation pane, click **Configure** and enable the **Fast Locate** option.

Figure 29: 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.



The screenshot displays the Cisco DNA Spaces Detect and Locate interface. On the left, a floor plan of the SJC10-1-Firstfloor is shown with various rooms labeled, including Murkch, Synsky, Burros Aires, Non-Exec Rooms, Dublin, Meria Park, and Main Lobby. The right panel shows details for a client with MAC address 5c:5a:c7:29:29:51. The 'Compute Type' field is highlighted in red and shows 'AOA'. Other fields include MAC Address, Status (ASSOCIATED), IP Address, Coordinates, Last Seen, Connected AP, Detecting Controller, SSID, Max RSSI Detected, Max RSSI AP MAC, Username, Band, Bytes Sent, Bytes Received, Device Location, and Source (COMPUTE).

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-amp1
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 65](#)

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 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 Aironet 9120 Series Access Points
- Cisco Aironet 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 controller. For more information on versions of controller compatible with Cisco Spaces, see [Compatibility Matrix](#).
- If a Cisco CMX and a Cisco Spaces account are both connected to the same 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 controller.

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

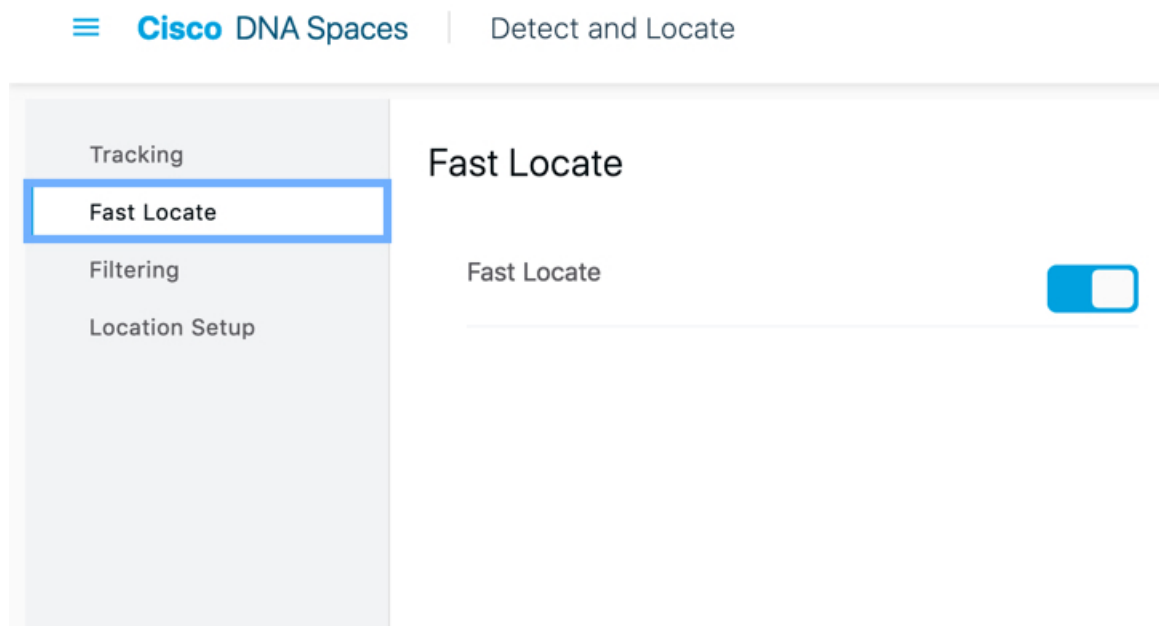
For instructions on how to enable hyperlocation on Cisco Catalyst 9800 Series Wireless Controllers, see the [Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide](#).

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 30: Enabling Cisco FastLocate on Cisco Spaces: Detect and Locate



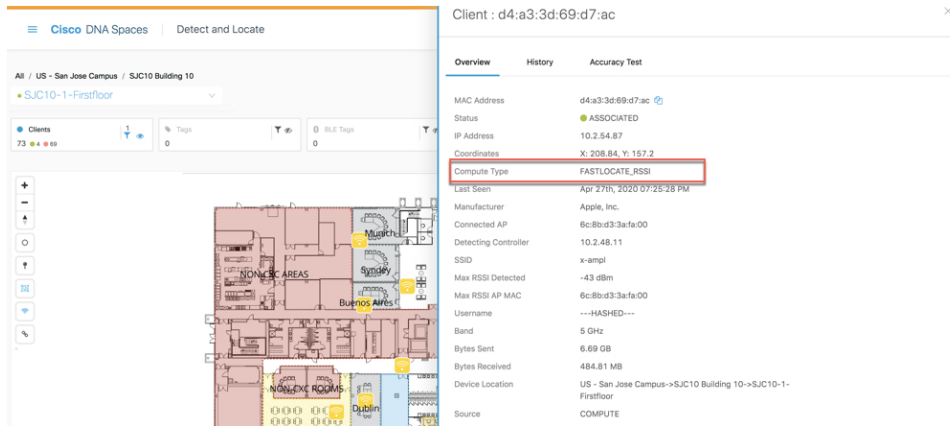
Step 3

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.



The screenshot displays the Cisco DNA Spaces interface. On the left, a map of the SJC10-1-Firstfloor is shown with various rooms and areas labeled, including 'NON-COMMERCIAL AREAS', 'Sydney', 'Buenos Aires', and 'Dublin'. The right pane shows the details for a client device with MAC address d4:a3:3d:69:d7:ac. The 'Compute Type' is highlighted in red and set to 'FASTLOCATE_RSSI'.

Overview	History	Accuracy Test
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 **VI**

Manage Users

- [Manage Users, on page 71](#)



CHAPTER 16

Manage Users

- [Manage Users](#), on page 71

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 3: 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:

- Name:** Enter a name for the user role.
- Permission:** Choose a permission from the drop-down list.
- 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

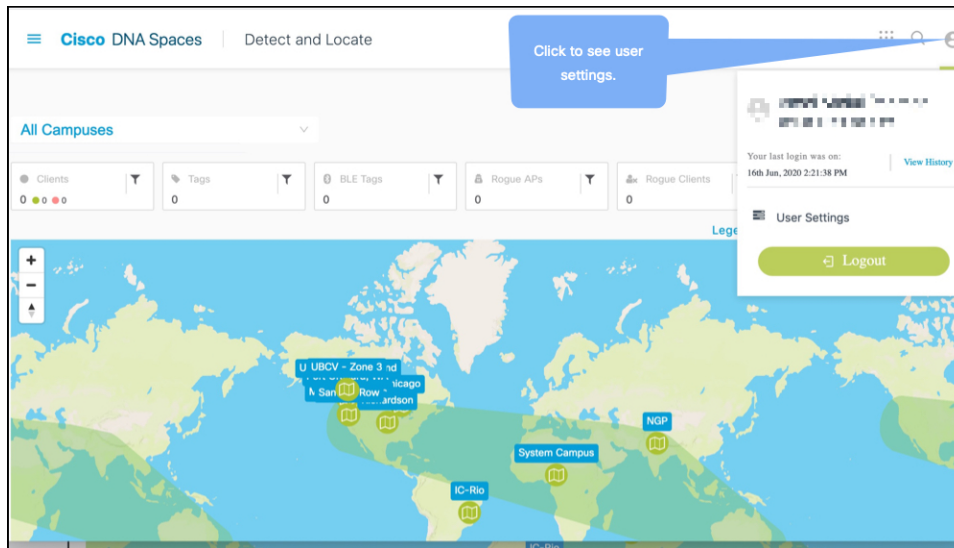
You, as an administrator, cannot modify the personal details of a user. The user also cannot modify his personal details from the **User Management** window.

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 31: 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 dashboard access activity, such as browsers used, access time, and location.

☰ Cisco DNA Spaces | Detect and Locate

My Account



My Profile | **Account Activity** | Preferences

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 **VII**

FAQs

- [Manage FAQs, on page 77](#)



CHAPTER 17

Manage FAQs

- [How Can I Get Support?](#) , on page 77
- [What Information is Stored in My Cisco Spaces: Detect and Locate Account and for How Long is it Stored?](#) , on page 77

How Can I Get Support?

Write to cisco-dnaspaces-support@external.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 **VIII**

API

- [API, on page 81](#)



CHAPTER 18

API

- [Using Rest APIs](#) , on page 81

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 32: API Keys

Key	Create Time	Expire Time	User	Actions
.....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	...

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.

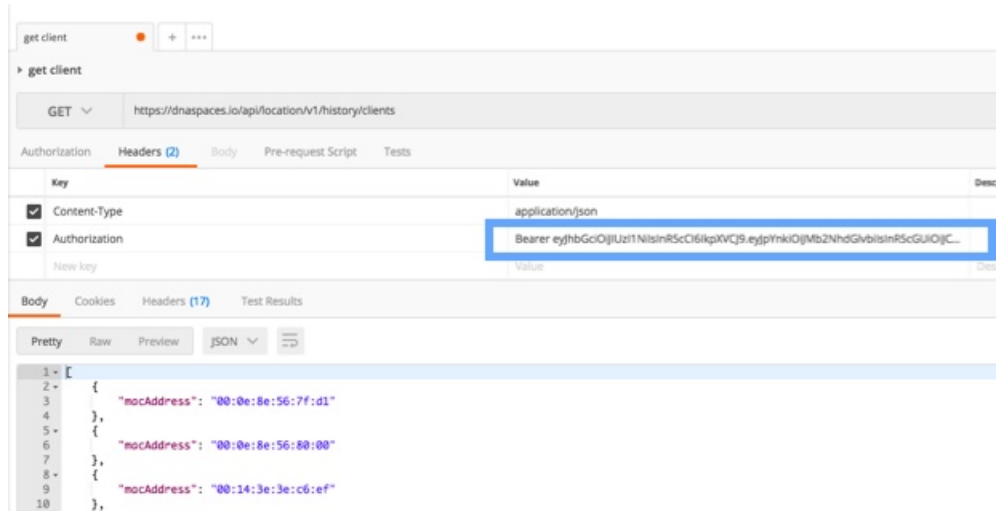


Note The API key is visible only at creation time, and hence must be stored securely. Cisco Spaces: Detect and Locate does not save the API key values. Each authenticated user can have up to five keys.

Figure 33: Copy the API Key

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

Figure 34: API Keys



The screenshot displays a REST client interface for a GET request to `https://dnspaces.io/api/location/v1/history/clients`. The request headers are configured as follows:

Key	Value	Desc
<input checked="" type="checkbox"/> Content-Type	application/json	
<input checked="" type="checkbox"/> Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpbnkiOiJMb2NhZGlvbGlzInR5cGU6IjE2In0.eyJpbnkiOiJMb2NhZGlvbGlzInR5cGU6IjE2In0.	

The response body is shown in JSON format, containing an array of three objects:

```
1 - [
2 - {
3 -   "macAddress": "00:0e:8e:56:7f:d1"
4 - },
5 - {
6 -   "macAddress": "00:0e:8e:56:80:00"
7 - },
8 - {
9 -   "macAddress": "00:14:3e:3e:c6:ef"
10 - },
```

