

Cisco Spaces: Detect and Locate Configuration Guide

First Published: 2019-01-29

Last Modified: 2026-07-14

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 NONINFRINGEMENT 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.

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)

© 2019–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

PREFACE

Audience ix

Conventions ix

Related Documentation x

Communications, services, and additional information x

Cisco Bug Search Tool xi

Documentation feedback xi

PART I

Product Overview 13

CHAPTER 1

Product Overview 1

Introduction to Cisco Spaces: Detect and Locate 1

CHAPTER 2

Licensing 3

Traditional Licensing 3

Split Licensing 3

License Types and Features 4

Practical Example 4

Device History 5

Webhook Creation 7

PART II

Getting Started 9

CHAPTER 3

Setup 11

Onboard To Cisco Spaces 11

CHAPTER 4 **Data Source** 13

Configuring Location Data Source 13

Configuring Location Data Source 13

PART III **Setup** 15

CHAPTER 5 **Explore the Dashboard** 17

Navigate to Your Location on the Dashboard 17

Understand Map Legends 18

Customize Your View Using the Device Toolbar 19

Left Toolbar 21

Sticky Clients 25

CHAPTER 6 **Customize Your Dashboard Using Filters** 27

Customize Your Dashboard with Filters 27

Set Up the Filter 27

Using Multiple Device Filters for Multiple Conditions 29

Filter Condition Dropdown Menu 30

Understanding Filtering by SSID 30

Filter Effect on the Dashboard 31

CHAPTER 7 **Global Search** 33

Global Search in Detect and Locate 33

Search Your Assets 33

Search Rules For Each Search Types 34

Search Results 35

No Result Cases 36

Other Options When MAC Address Not Found 37

Device Tracing 37

Search From Location History 38

Partial Values and Invalid Characters 38

Manage Columns in the Search Results 38

CHAPTER 8 **Client History** 39

Details and History of a Device 39

Device Detail Window 39

Overview Tab 40

History Tab 42

Devices With Location History Records 42

Four Device Location History Representations 42

CHAPTER 9 **Location Accuracy** 47

Location Accuracy 47

Restrictions for Location Accuracy 47

Test Location Accuracy 47

CHAPTER 10 **How to Track Devices** 53

Device Tracking 53

Devices Tracked by Cisco Spaces: Detect and Locate 53

Enable or Disable Device Tracking in Cisco Spaces 53

Device Visibility 54

Enable Device Visibility 54

View Enabled Device Types 55

Keep Devices Visible with Regular Updates 56

Eviction Times 56

Filter Tracked Devices 56

Configure Cutoff for Location Accuracy 56

Configure Filter Values For Tracked Devices 56

Parameters to Filter Tracked Devices 57

SSID Validation 57

CHAPTER 11 **Manage Columns** 61

Manage Columns 61

CHAPTER 12 **Manage Session Expiry** 63

Session expiry 63
Manage Sessions Expiry 63

PART IV Deployment Information 65

CHAPTER 13 Deployment Information 67
Access Point Deployment Information 67

PART V Hyperlocation and FastLocate 73

CHAPTER 14 Configuring Hyperlocation 75
Enabling Cisco Hyperlocation 75
How to Configure Cisco Hyperlocation 76

CHAPTER 15 Configure Cisco FastLocate 79
Configuring Cisco FastLocate 79
How to Configure Cisco FastLocate 79

PART VI Manage Notifications 83

CHAPTER 16 Using Northbound Notifications 85
Using Northbound Notifications 85
Location Update (Northbound Notification) 85
Absence (Northbound Notification) 87
Association (Northbound Notification) 88
In/Out (Northbound Notification) 90

PART VII Manage Users 93

CHAPTER 17 Manage Users 95
Manage Users 95
Configure User Roles and Invite Users 95
Modifying Users and User Roles 96

PART VIII FAQs 99

CHAPTER 18 Manage FAQs 101

How Can I Get Support? 101

What Information is Stored in My Cisco Spaces: Detect and Locate Account and for How Long is it Stored? 101

PART IX API 103

CHAPTER 19 API 105

API Key 105

API Rate Limiting 107



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 ix
- Related Documentation, on page x
- Communications, services, and additional information, on page x

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

Cisco Spaces Configuration Guide

Connector

- *Cisco Spaces: Connector Configuration Guide*
- *Cisco Spaces: Connector Command Reference Guide*
- *Release Notes for Cisco Spaces: Connector*

IoT Service

- *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

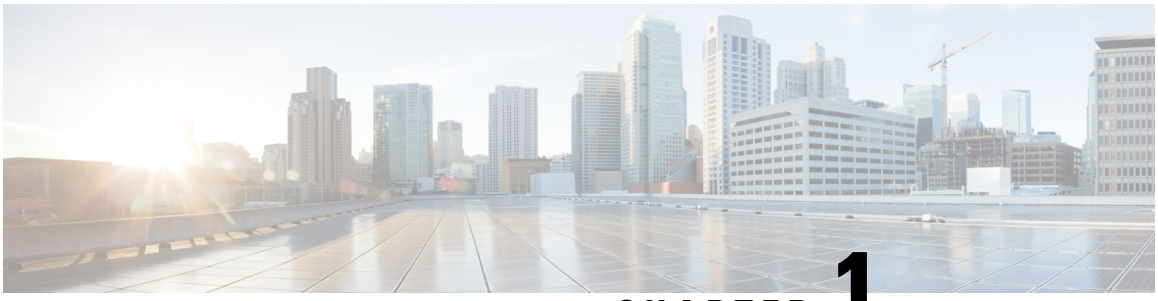
To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



PART I

Product Overview

- Product Overview, on page 1
- Licensing, on page 3



CHAPTER 1

Product Overview

- Introduction to Cisco Spaces: Detect and Locate, on page 1

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.

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 (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.

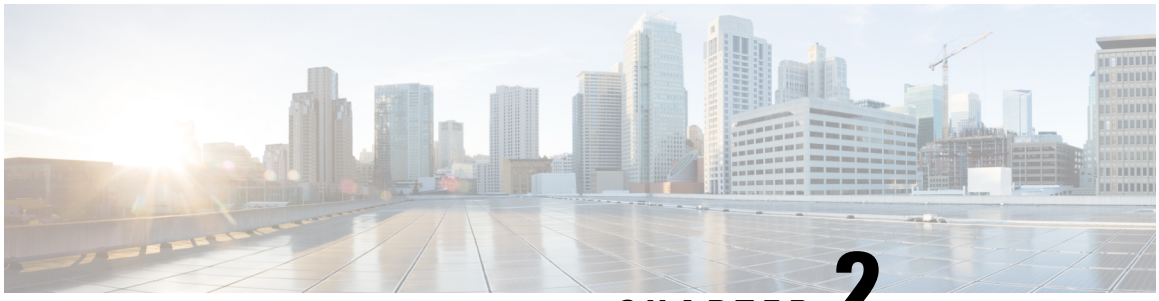
The Wireless Controller does not require active devices to probe continuously. In contrast, Cisco Spaces requires a probe frequency of five minutes or less. Therefore, devices shown as active on the Wireless Controller might not appear on Cisco Spaces. These are termed non-locatable devices.

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.



CHAPTER 2

Licensing

- Traditional Licensing, on page 3
- Split Licensing, on page 3
- License Types and Features, on page 4
- Practical Example, on page 4
- Device History, on page 5
- Webhook Creation, on page 7

Traditional Licensing

Before the introduction of split licensing, a Cisco Spaces account had a single license that applied uniformly across all location hierarchy nodes within the organization. Nodes could include campuses, buildings, floors, or other organizational units. Every location adhered to the same licensing terms and features, regardless of the specific needs or usage patterns of different locations.

Split Licensing

Using the split licensing feature provides you greater flexibility and granularity in license assignment within an organization. Here is a breakdown of how it works and its advantages:

1. Customizable licensing at different levels:
    - **Location hierarchy nodes:** Administrators assign different licenses to specific nodes within the location hierarchy. This feature ensures that each campus, building, or floor have a tailored license based on its unique requirements.
    - **Use cases:** For example, a high-traffic campus building may need advanced features such as access to **History** and **Webhooks**, while a smaller branch office might only need basic functionalities.
2. Access to advanced features:
    - Devices located in these nodes with qualified licenses have access to advanced features such as:
        - **History:** Logging and tracking device interactions, usage patterns, or other historical data.
        - **Webhooks:** Real-time data integration and automation by sending HTTP POST requests to specified URLs when certain events occur.

3. Uses Cisco Smart Licensing:
   - **Smart Licensing:** A flexible and automated licensing model from Cisco that simplifies the activation and management of licenses. Split Licensing uses Cisco Smart Licensing to manage and apply these specialized licenses efficiently.
   - **Administrative Efficiency:** Administrators can easily manage, track, and adjust licenses from a centralized platform. Th correct licenses are applied where needed. You can avoid overuse or underuse of licenses.
4. Benefits:
   - **Cost-Effective:** Organizations can optimize costs by only purchasing advanced licenses for locations that truly need them.
   - **Scalable:** As the organization grows or its needs change, administrators can quickly adjust the licensing without major overhauls.
   - **Tailored Solutions:** Different parts of the organization have the exact features and capabilities that is needed, enhancing productivity and efficiency.

License Types and Features

Table 2: License Types and Features

Licenses	Detect and Locate Advanced (History, Fast Locate)	Detect and Locate Advanced (API and Webhooks)
Unlimited	Y	Y
Act	Y	Y
Smart Operations	Y	Y
Smart Operations Base	Y	Y
Smart Venues	N	N
Extend	N	Y
SEE	N	N

For more information on Cisco Smart Licensing, see the Cisco Smart Licensing section in the *Cisco Spaces Configuration Guide*.

Practical Example

Consider a university with various campuses and buildings:

- **Main Campus:** needs advanced analytics and automation. This location is assigned a license that has **History** and **Webhooks**.

- **Satellite Campus:** is smaller, with basic needs. This location is assigned a standard license.
- **Research Building:** requires specialized tools for real-time monitoring. This location is assigned a customized license.

Using split licensing ensures that each location has the appropriate tools and capabilities. You optimize operational efficiency and resource allocation.

Device History

Device history is supported for specific license types (see the License Type and Features section).

Click a device, a detailed information window is displayed.

If the license qualifies, the **History** tab displays historical data for that device.



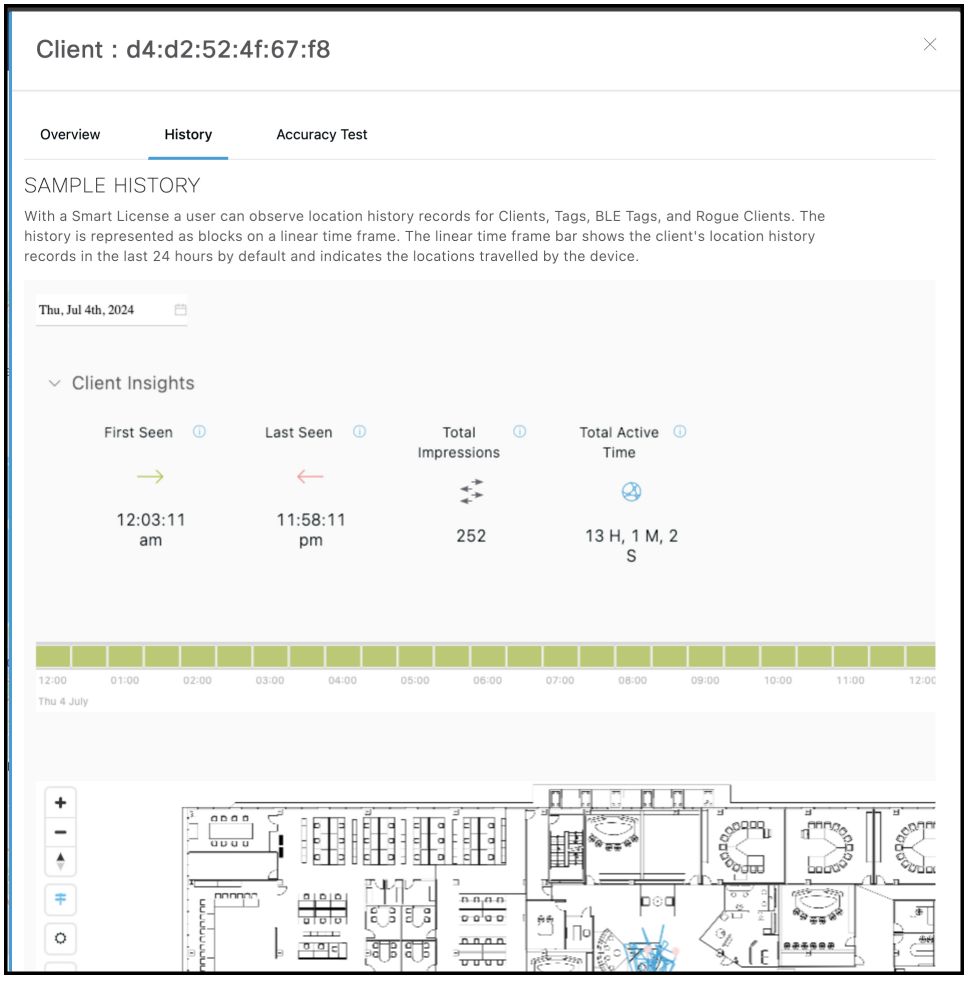
Note Observe the **Timeline** legend. The block color of the timeline is green for associated clients. For all other devices, the block color is pink (including probing clients).

Figure 1: License Qualifies



If you do not have a license that qualifies, the **History** tab displays a sample history window that demonstrates potential capabilities.

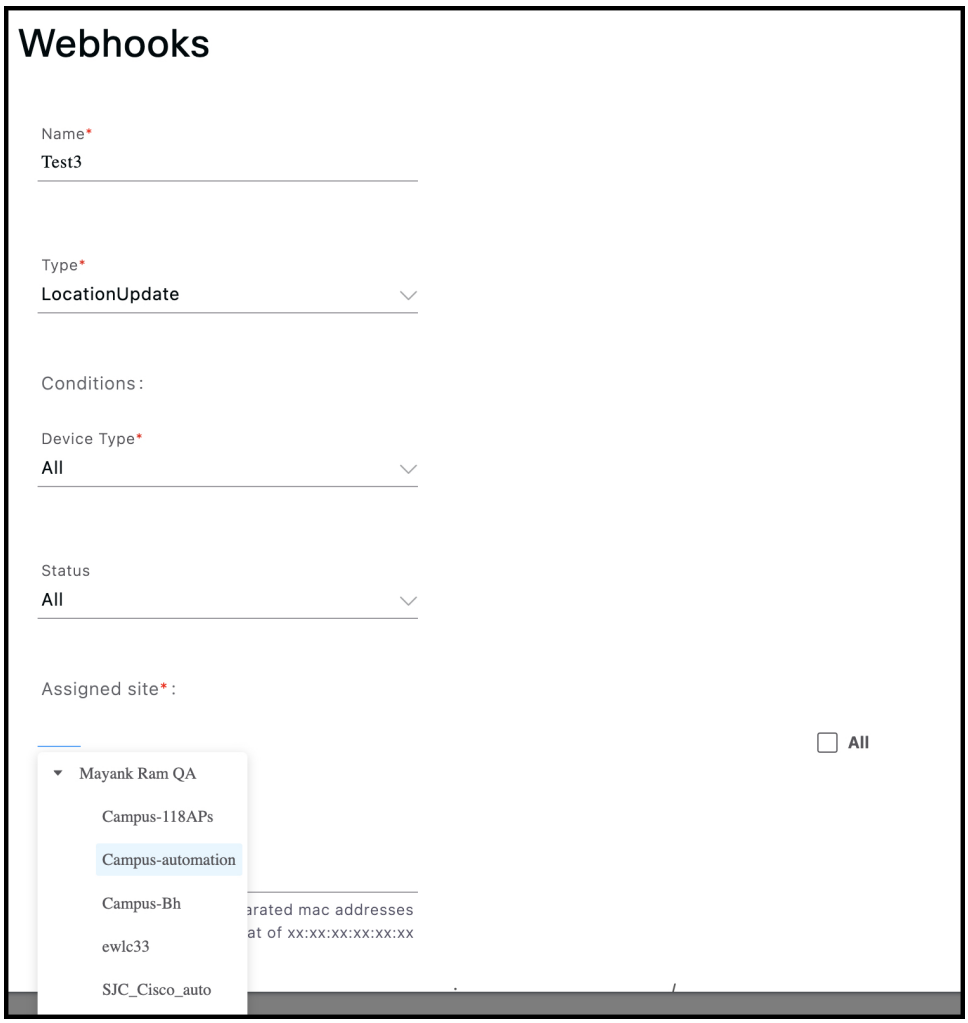
Figure 2: License Does Not Qualify



Webhook Creation

You can configure webhooks to send notifications to chosen endpoints. While webhook configuration is independent of the account-level license, data delivery through webhooks is restricted to location hierarchies with a license type that qualifies (See License Types and Features, on page 4).

Figure 3: License Does Not Qualify



License Propagation

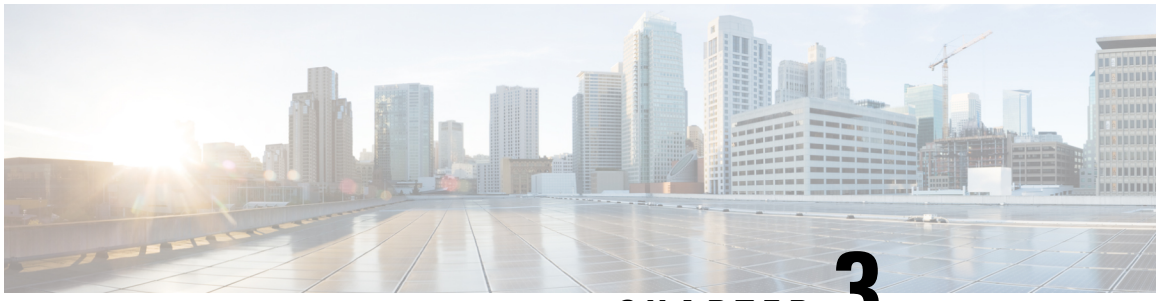
Licenses propagate from parent nodes to child nodes within the location hierarchy.



PART II

Getting Started

- Setup, on page 11
- Data Source, on page 13



CHAPTER 3

Setup

- Onboard To Cisco Spaces, on page 11

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.

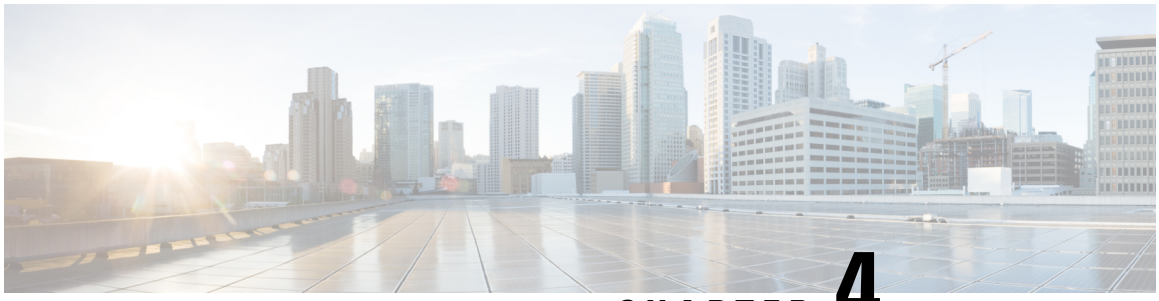
Procedure

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.



CHAPTER 4

Data Source

- Configuring Location Data Source, on page 13

Configuring Location Data Source

Configuring Location Data Source

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

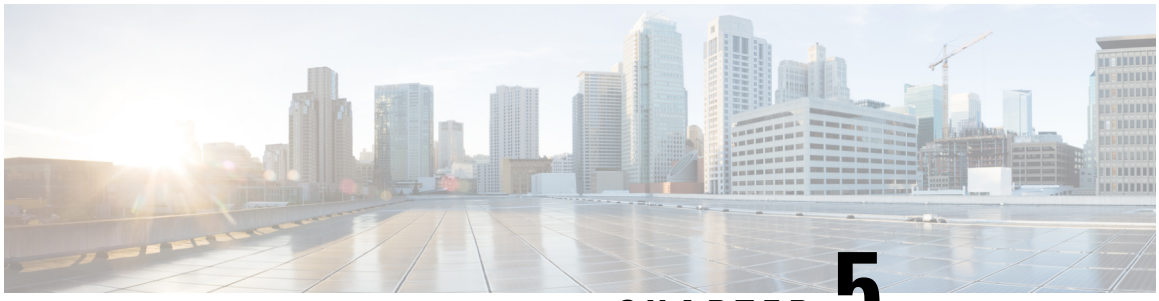
- Cisco Spaces Connector Configuration. Refer to Cisco DNA Spaces Connector Configuration Guide
- Cisco AireOS Wireless Controller configuration: You can configure the Detect and Locate using wireless controller as data source. For more information, see **Configuring Cisco Wireless Controllers and Cisco 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

Setup

- Explore the Dashboard, on page 17
- Customize Your Dashboard Using Filters, on page 27
- Global Search, on page 33
- Client History, on page 39
- Location Accuracy, on page 47
- How to Track Devices, on page 53
- Manage Columns, on page 61
- Manage Session Expiry, on page 63



CHAPTER 5

Explore the Dashboard

- Navigate to Your Location on the Dashboard, on page 17
- Understand Map Legends, on page 18
- Customize Your View Using the Device Toolbar, on page 19
- Left Toolbar, on page 21
- Sticky Clients, on page 25

Navigate to Your Location on the Dashboard

You can see the location hierarchy of your network in a drop-down list on the Cisco Spaces: Detect and Locate dashboard.

Use this drop-down list to navigate to the desired campus, building, or floor.

Figure 4: Map Hierarchy

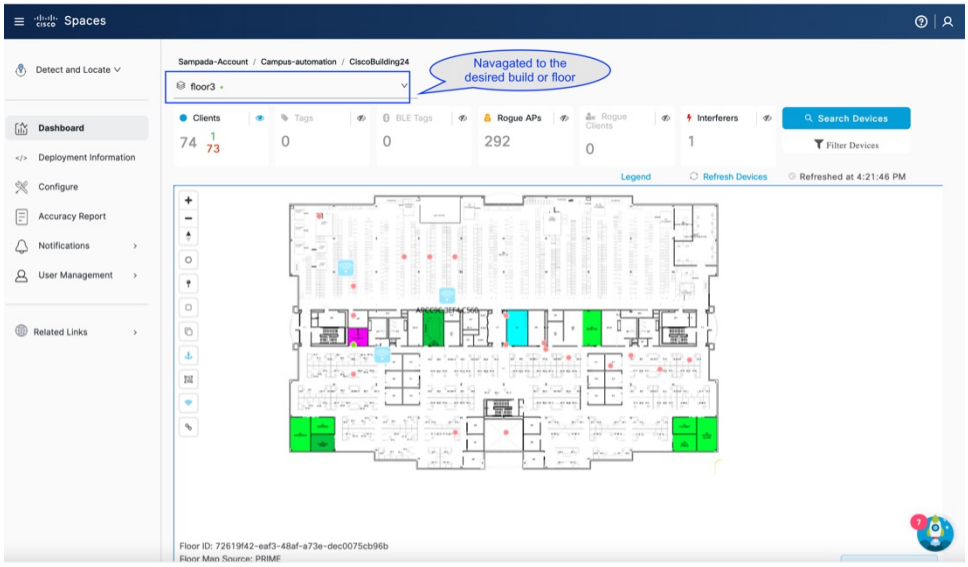
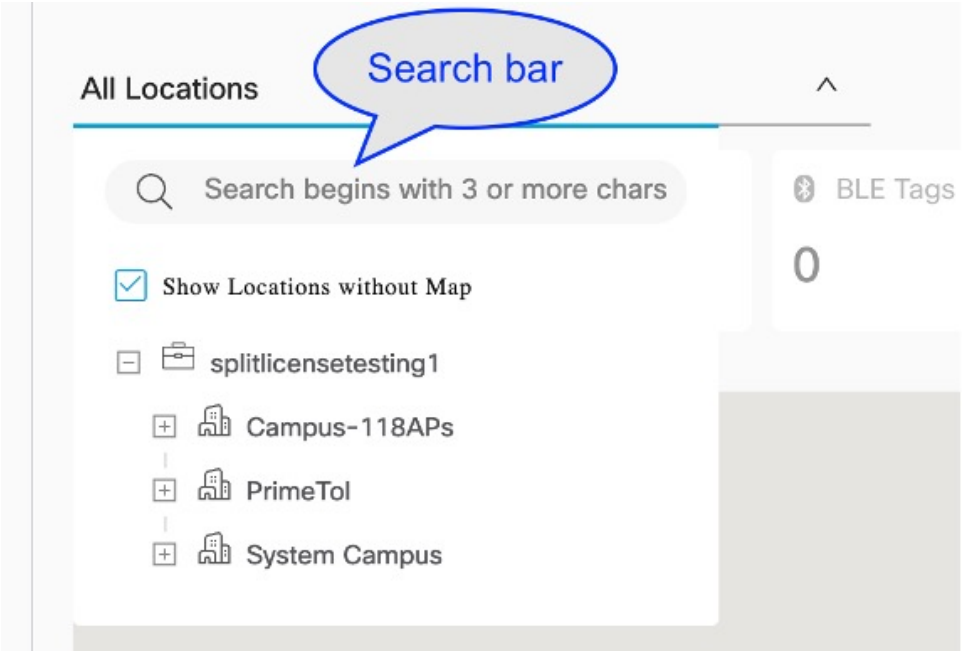


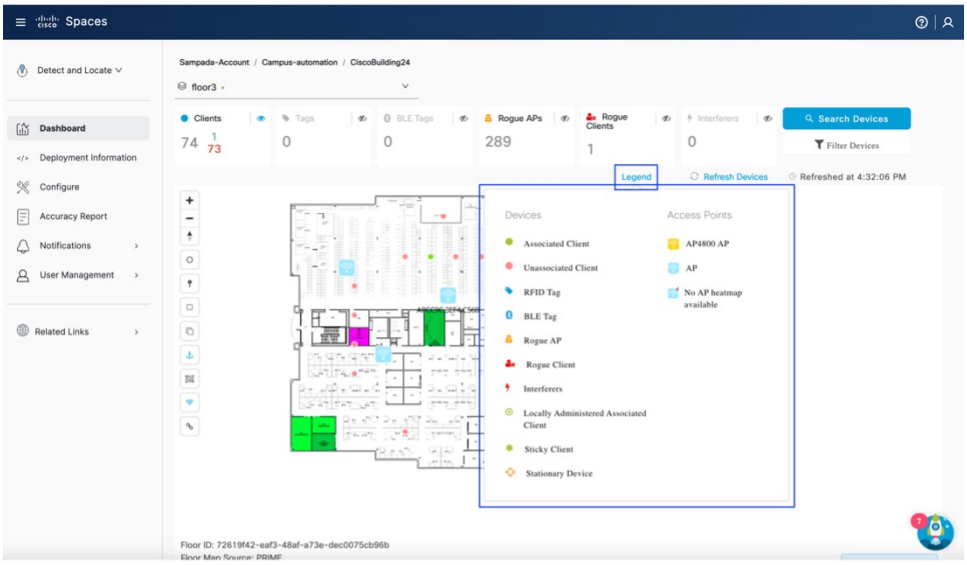
Figure 5: Map Hierarchy, a Closer Look



Understand Map Legends

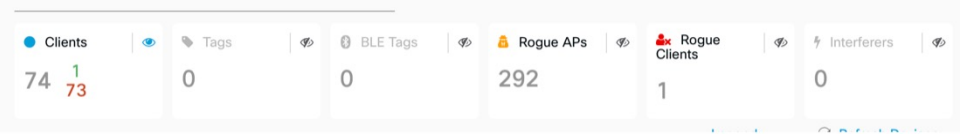
The map on the Detect and Locate dashboard has various markings. Click the **Legend** button to understand the various markings.

Figure 6: Legend of a Map



Customize Your View Using the Device Toolbar

Figure 7: Device Toolbar



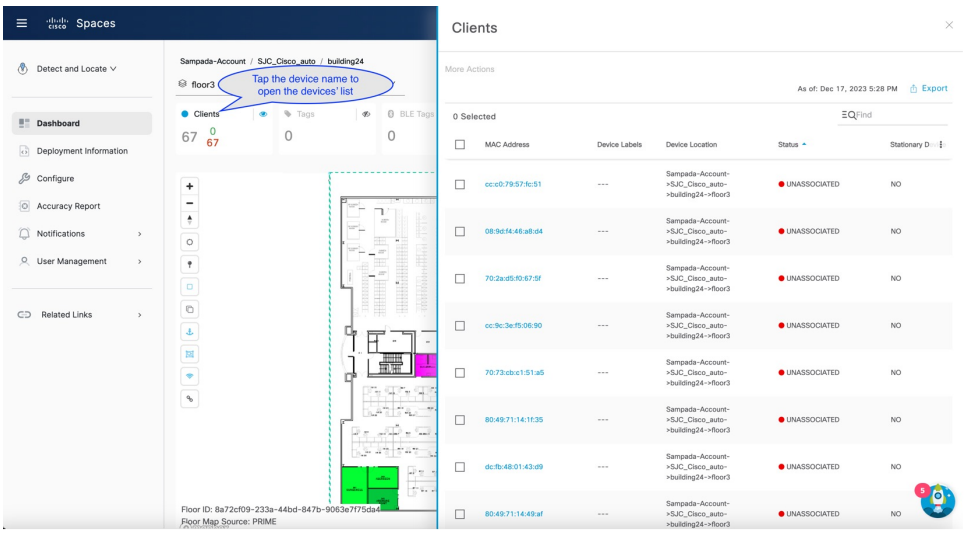
The device toolbar allows you to customize the view of the dashboard. Each device type on the device toolbar has an associated eye icon . Click the eye icon to show or hide this type of device on the map. Choose any combination of the icons and click the corresponding eye icons to customize your view.

Here is a description of each device type on the device toolbar, and some additional icons present on the map.

- **Clients:** Represent both connected and detected clients. The number in green (the first number) indicates the number of connected clients, and the number in red (the second number) indicates detected clients. These various client types are represented on the map as:
  - **Clustered Probing Clients:** A dot associated with a number on the map ( ). This dot signifies a cluster of probing clients. You can zoom in to view individual clients.
  - **Probing Clients:** A red dot on the map indicates probing clients.
  - **Connected Clients:** A green dot on the map indicates connected clients.
- **BLE Tags:** Represent Bluetooth Low Energy tags attached to track devices.
- **Tags:** Represent vendor-specific information in raw format from Wi-Fi tags.
- **Rogue Access Points:** Represent APs that are not part of or managed by the Wi-Fi infrastructure.
- **Rogue Clients:** Indicate clients connected to rogue access points.
- **Interferers:** Represent devices that can create radio frequency interference.

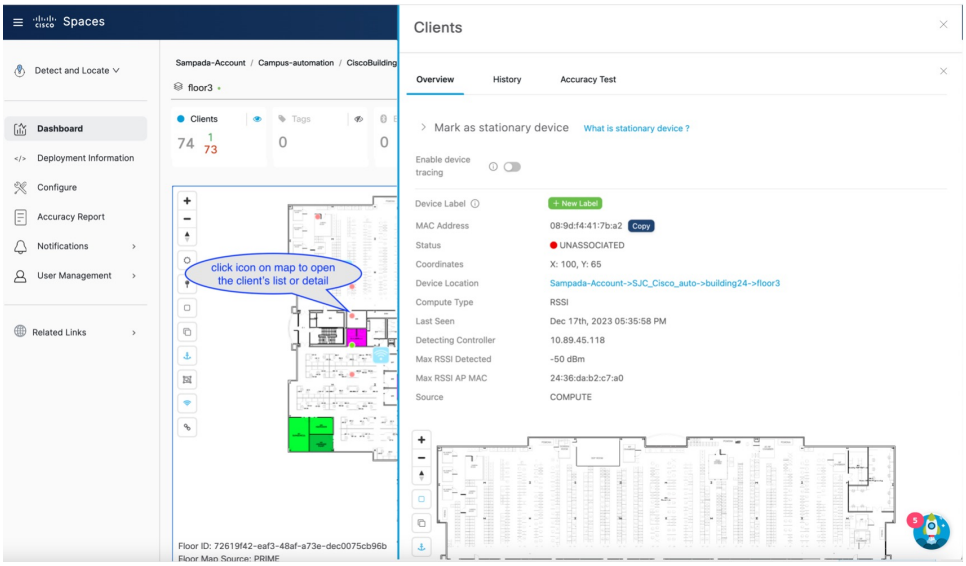
1. To open a list of devices of a particular type, click the device type on the device toolbar. The device list appears on the right side of the page. This list shows all devices of this type from the selected hierarchy.

Figure 8: Open List of Devices by Clicking the Device Type on the Device Toolbar



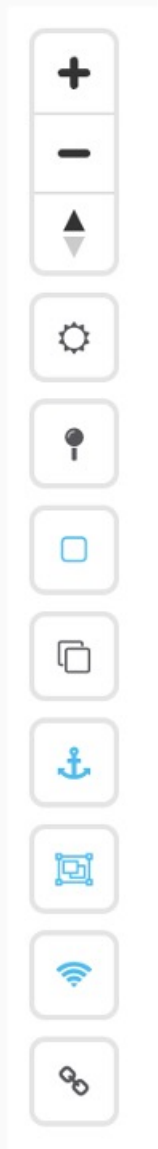
2. You can also click the device icon on the map to open either a device list or detailed information of one device on the right side of the page.

Figure 9: Open Device Information by Clicking the Device Icon on the Map



Left Toolbar

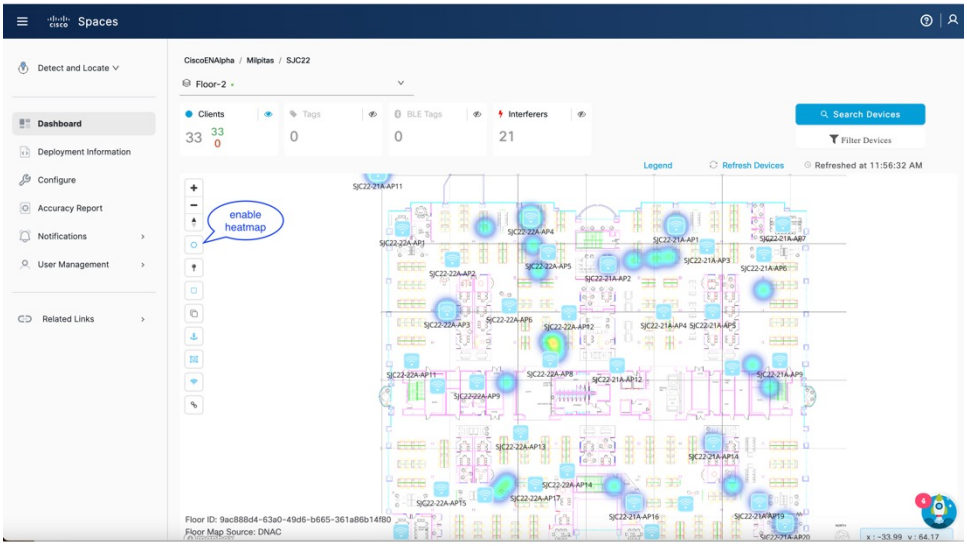
Figure 10: Left Toolbar



You can show or hide the following elements using the left toolbar. You can also enable or disable clustering using the left toolbar:

1. **Heatmap:** Displays (or hides) the movement of various clients as a heatmap.

Figure 11: Display Heatmap



2. **GPS markers:** Displays (or hides) GPS markers. Green markers indicate valid locations, while red markers indicate invalid ones. Hover over the markers for detailed information.

Figure 12: Display GPS Markers



3. **Floor boundary:** Displays (or hides) floor boundary.

Figure 13: Display Floor Boundary and Inclusion and Exclusion Regions

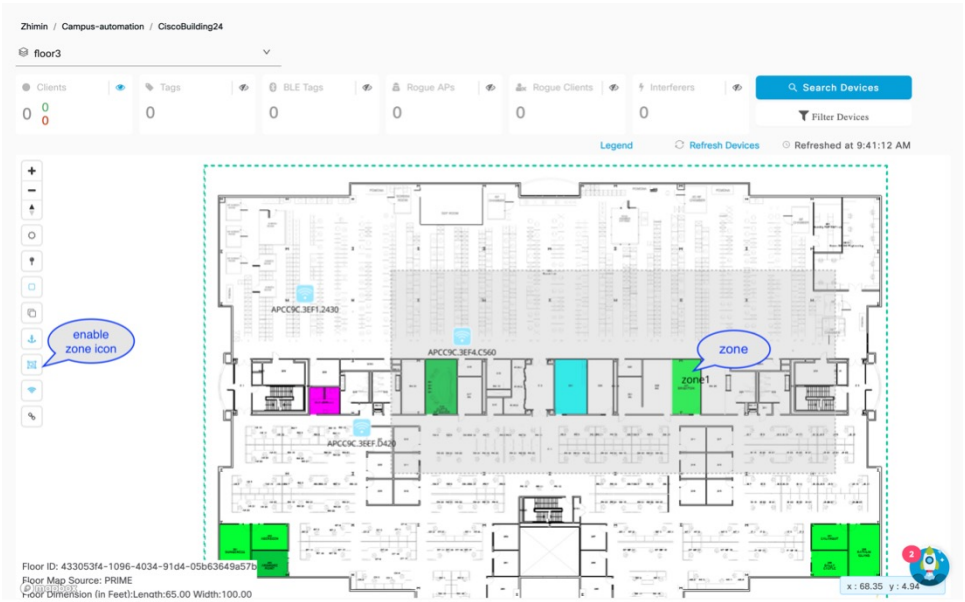


4. **Inclusion Exclusion Regions:**  Displays (or hides) inclusion and exclusion regions.

5. **Anchor tags:**  Displays (or hides) anchor tags.

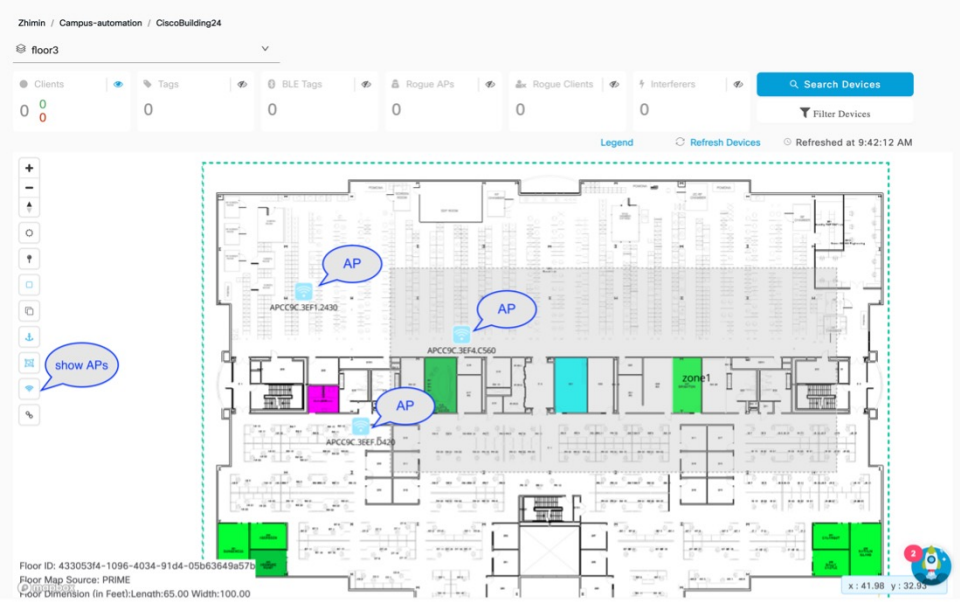
6. **Zones:**  Displays (or hides) zones on a specific floor.

Figure 14: Display Zones



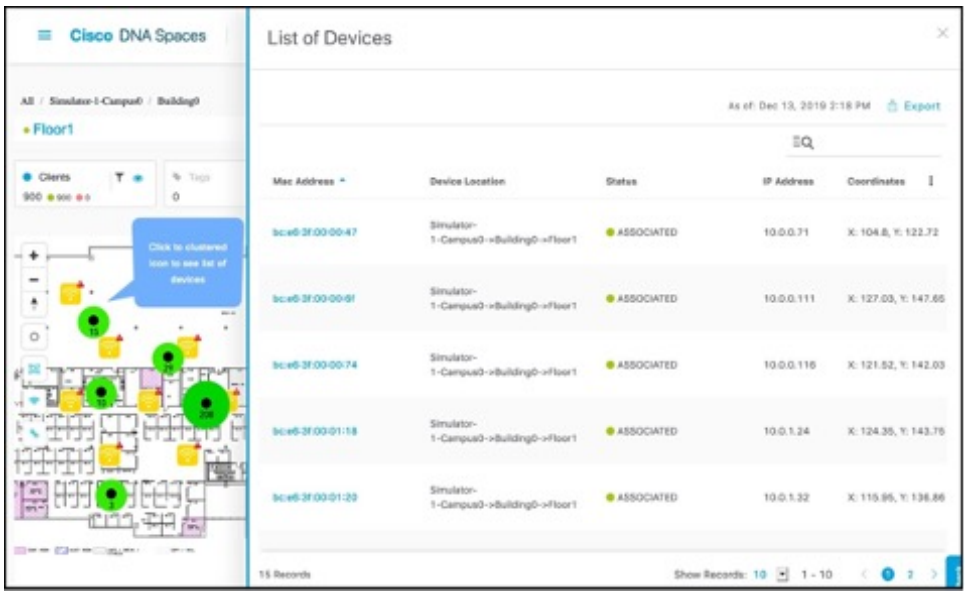
7. **Access Point:** Displays (or hides) APs deployed on a specific floor. If you uploaded a map to Detect and Locate, you can use this icon to see which APs have device location information ( ) and which APs do not ( ). You can then troubleshoot based on this information.

Figure 15: Display Access Points



8. **Clustering:** Enables (or disables) clustering of closely-located and possibly-overlapping devices into a group. Click on the clustered icon to view the list of devices in a separate window.

Figure 16: Enable Clustering



Sticky Clients

Detect and Locate provides a configuration to tag regular clients as sticky clients.

Typically, a client connects to the AP closest to it. However, there may be instances where a device connects to an AP, moves into the range of another AP, and does not change its association to the closer AP. Such a client is referred to as a sticky client.

For example, a user enters the first floor and connects to the AP on that floor. The user then moves to the third floor and stays there. You might expect the device to connect to the AP on the third floor. But if it does not, and such a client is referred to as a sticky client, as it is stuck to an AP that is farther away.

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

This feature is disabled by default, providing users the option to enable it based on their network requirements.

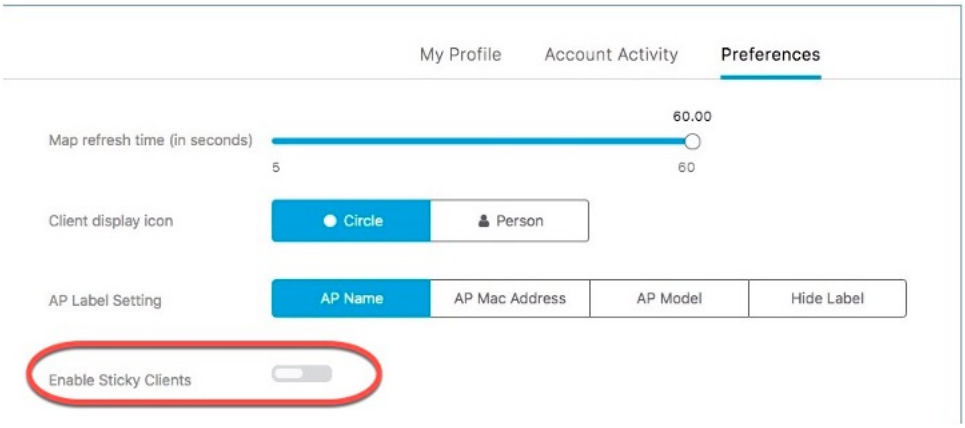
To tag regular clients as sticky clients in Cisco Spaces: Detect and Locate, follow these steps:

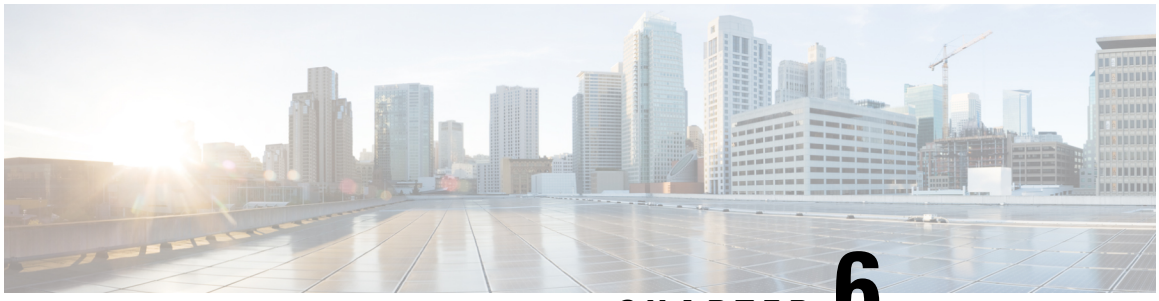
Procedure

To enable the sticky clients feature, navigate to the Detect and Locate dashboard.

a) Click the profile icon in the top-right corner.
b) Select **Preferences**.
c) Click **Enable Sticky Clients**.

Figure 17: Enable Sticky Clients





CHAPTER 6

Customize Your Dashboard Using Filters

- Customize Your Dashboard with Filters, on page 27
- Set Up the Filter, on page 27
- Using Multiple Device Filters for Multiple Conditions, on page 29
- Filter Condition Dropdown Menu, on page 30
- Understanding Filtering by SSID, on page 30
- Filter Effect on the Dashboard, on page 31

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.

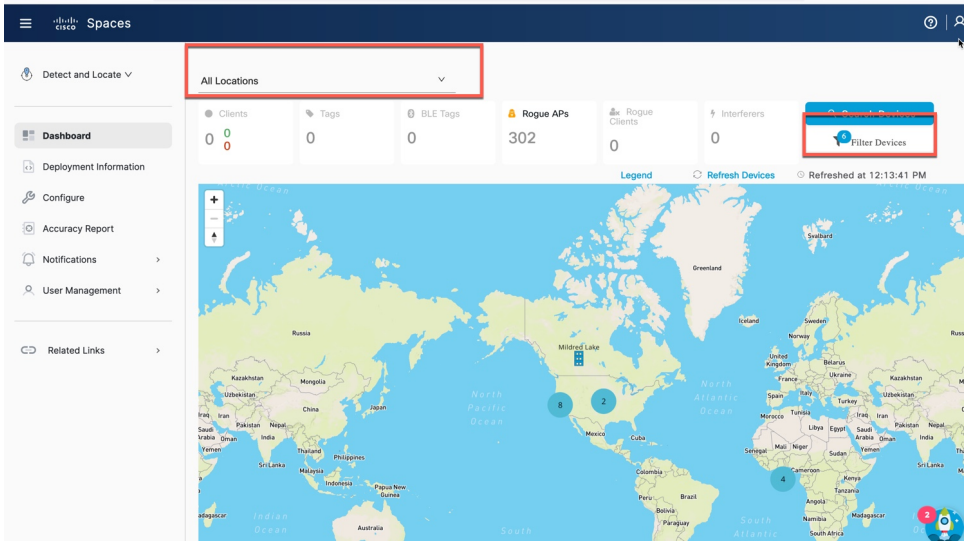
Set Up the Filter

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

Procedure

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

Figure 18: 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 19: Specify the Filter Conditions

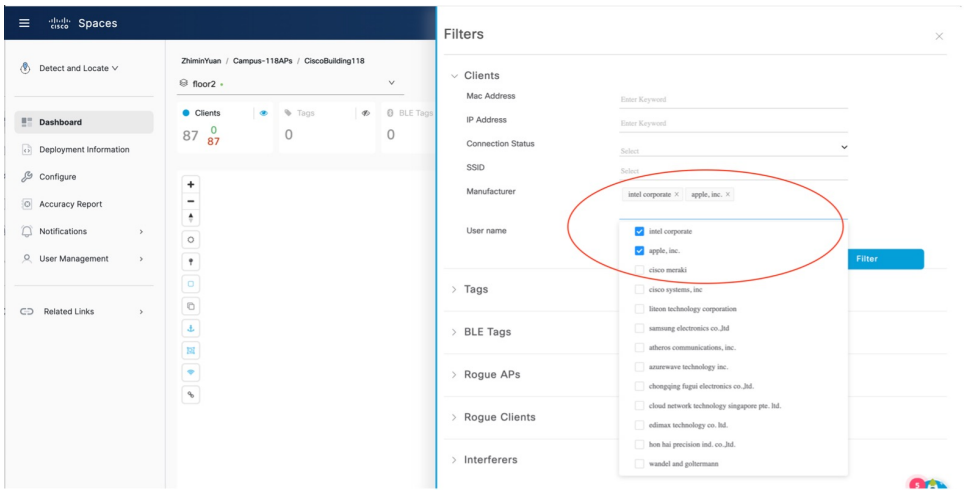
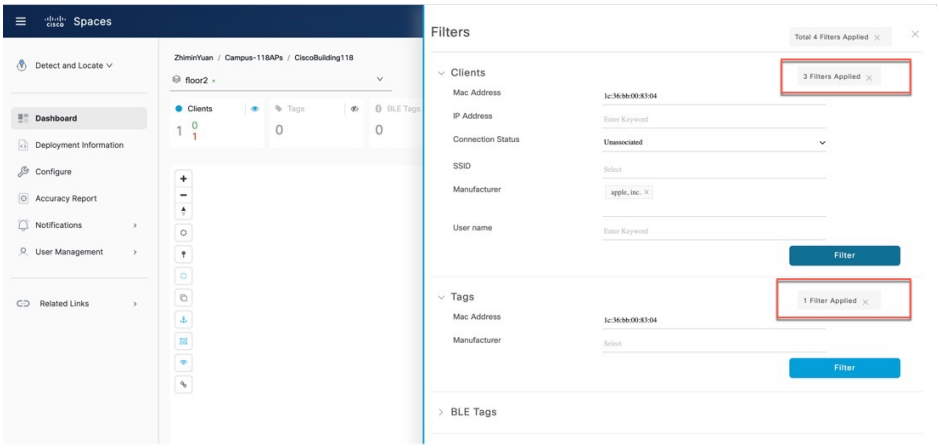


Figure 20: View All Configured Filters

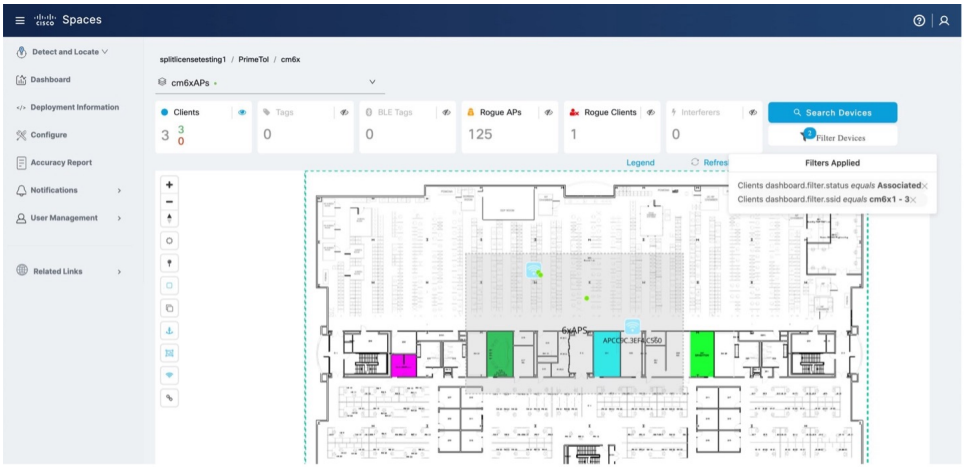


In the same **Filters** window, you can now see the configured filters on the top right of each category. A total of all the filters also appears on the top right.

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.

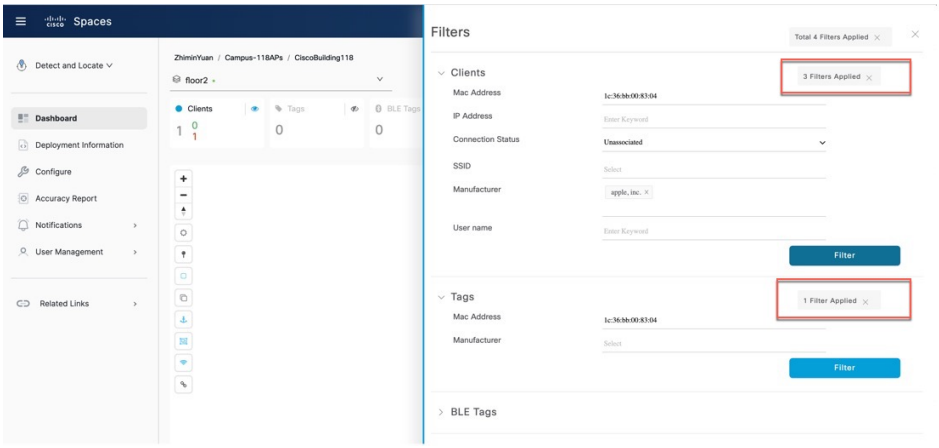
Figure 21: Filter Count on the Filter Devices Button



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.

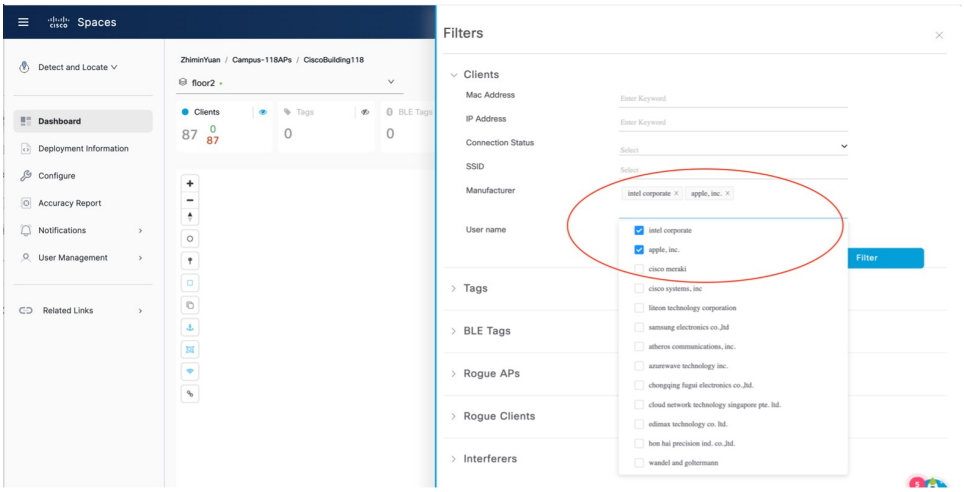
Figure 22: Configuring Multiple Conditions with Multiple Filters



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 23: Filter Conditions Dropdown Menu



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.

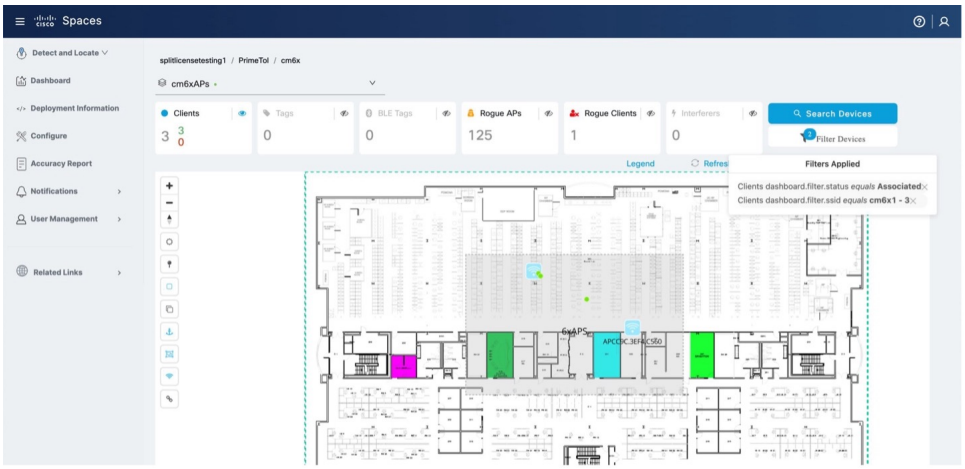
Filter Effect on the Dashboard

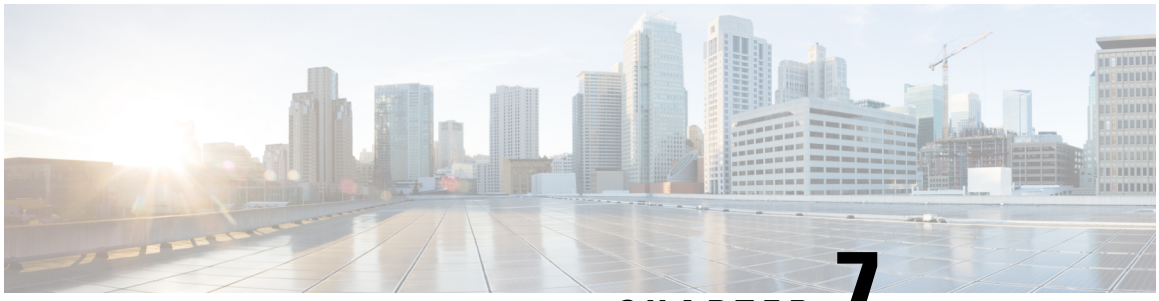
When you apply a filter, the following gets modified:

- 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 24: Effect of Filter on the Dashboard





CHAPTER 7

Global Search

- Global Search in Detect and Locate, on page 33
- Search Your Assets, on page 33
- Search Rules For Each Search Types, on page 34
- Search Results, on page 35
- No Result Cases, on page 36
- Manage Columns in the Search Results, on page 38

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.

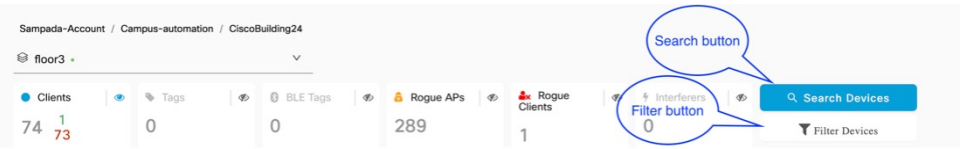
The article covers various aspects of the global search process, including

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

Search Your Assets

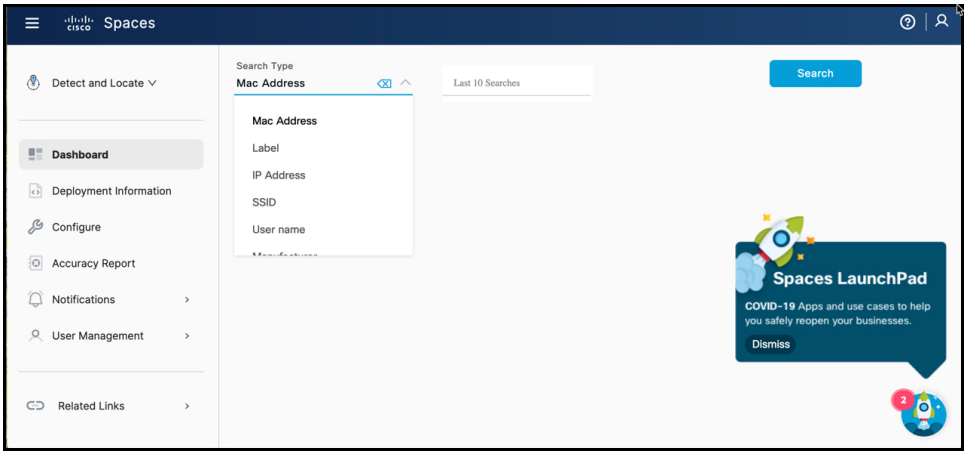
Search your assets by clicking the **Search Devices** button as shown in the image.

Figure 25: Search Devices Button



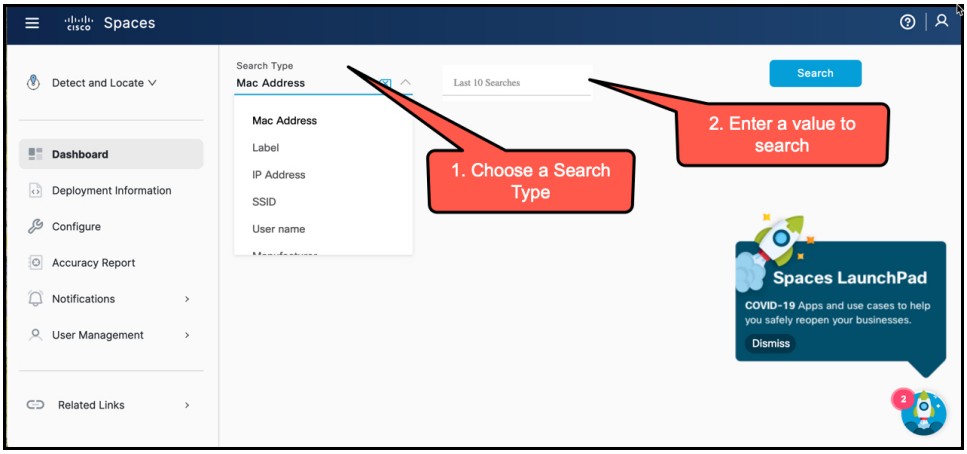
In the window that opens, you can search all assets tracked by your Cisco Spaces: Detect and Locate account.

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



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

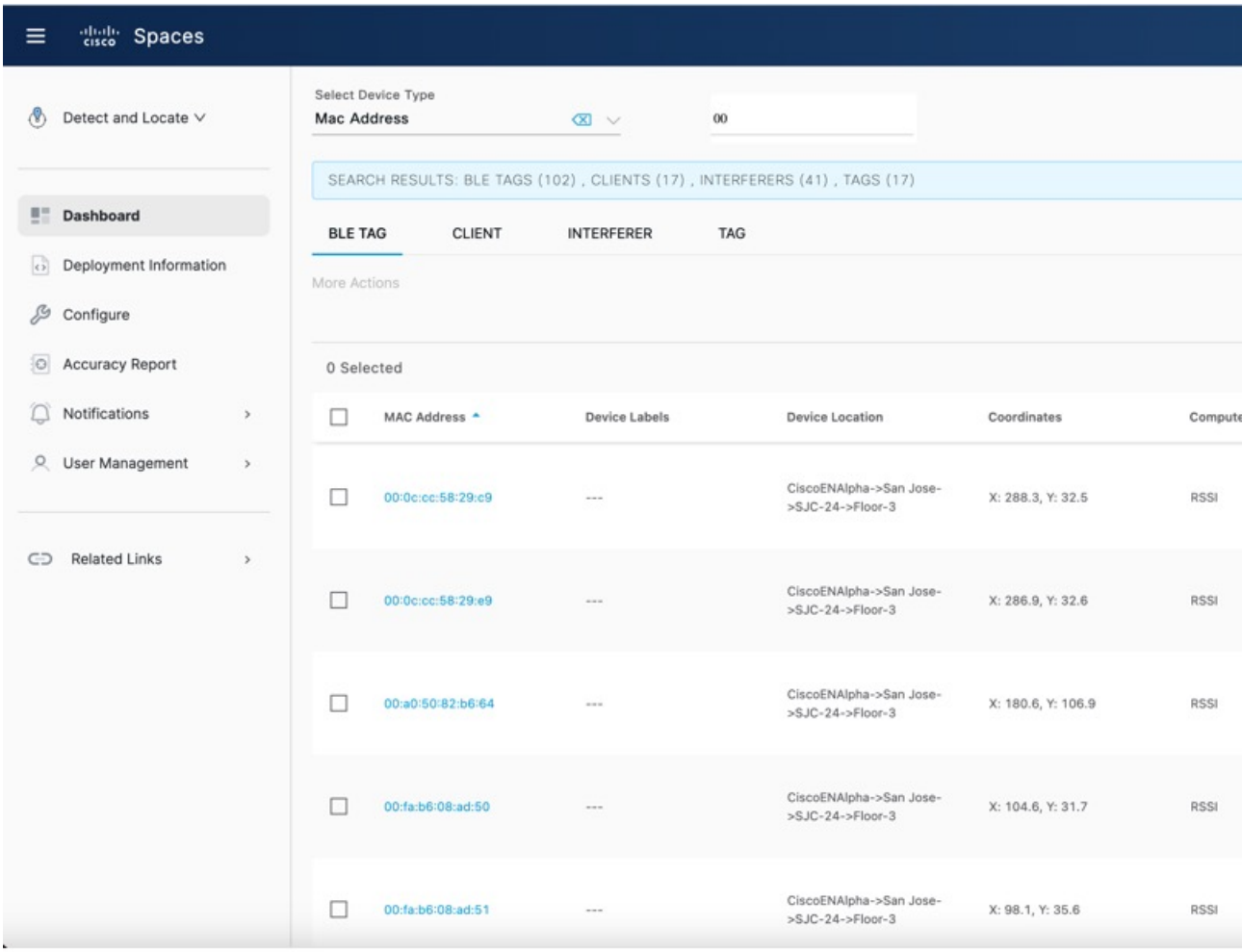
Search By	Matching Type Support	Format Verification
MAC Address	Fuzzy	YES
Label	Absolute	NO
IP Address	Fuzzy	YES for IPv4
SSID	Fuzzy	NO
Username	Fuzzy	NO
Manufacturer	Fuzzy	NO

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

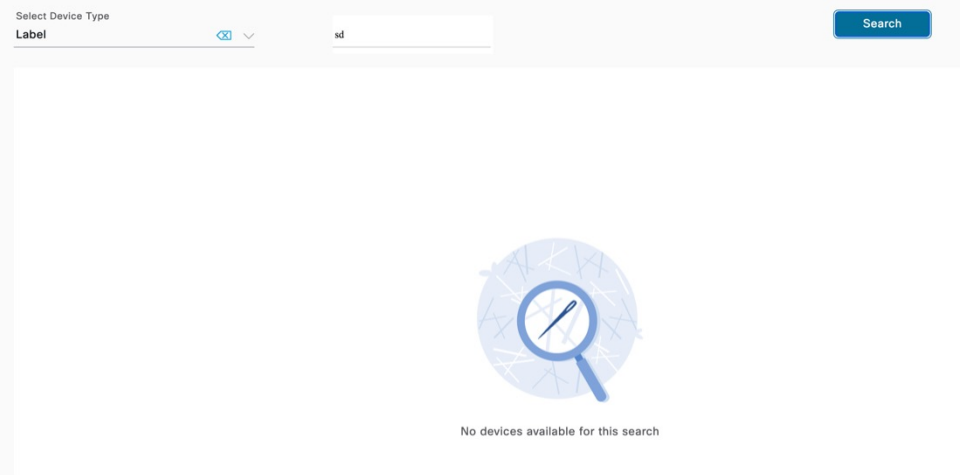


No Result Cases

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

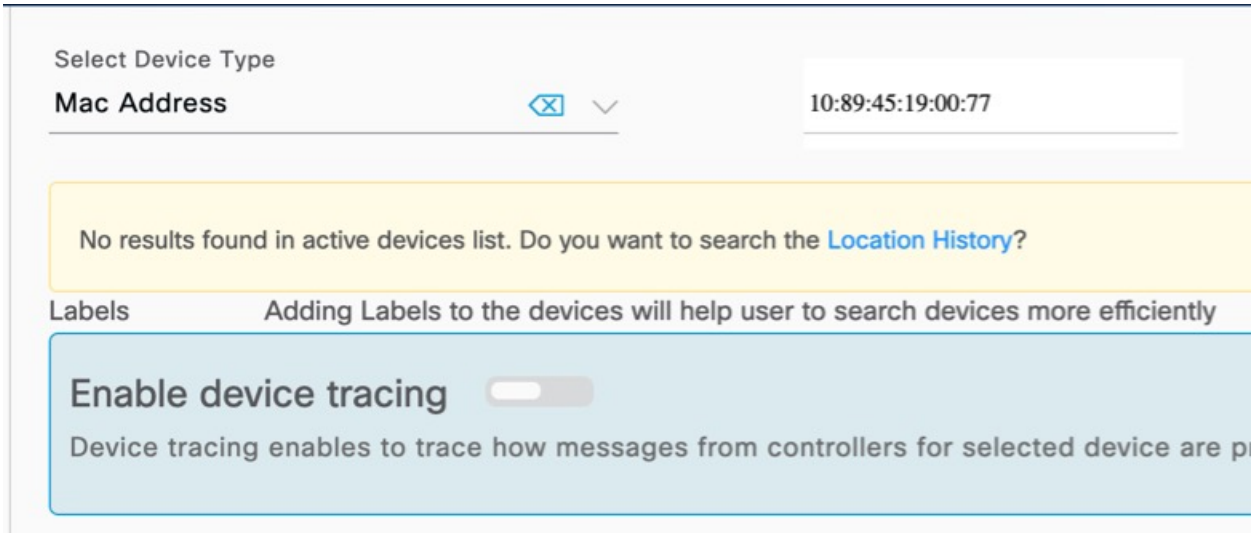


Other Options When MAC Address Not Found

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



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.

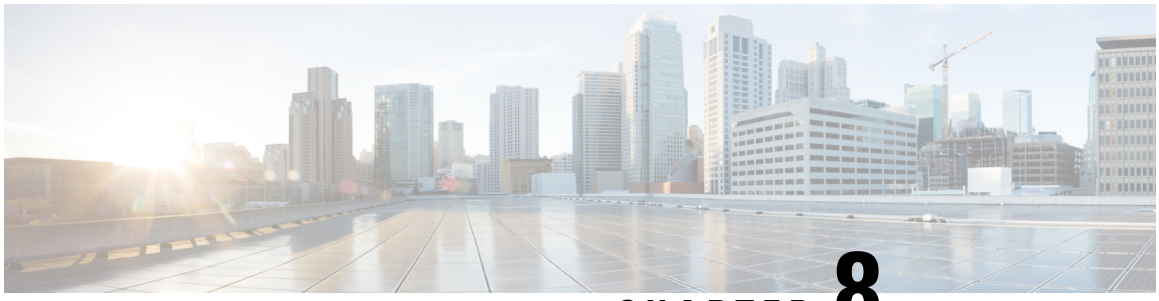
Figure 31: Searching for Partial Value or Invalid Characters



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, on page 39
- Device Detail Window, on page 39

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.

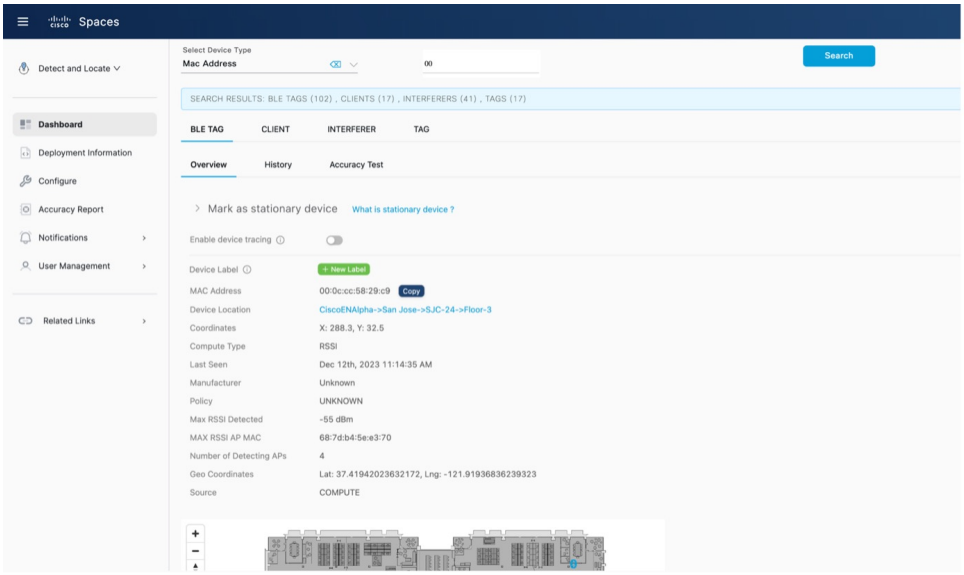
Through detailed device data and insights, you learn how to effectively manage your devices. You can interpret historical location data, and utilize insights for informed decision-making within your network.

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



Procedure

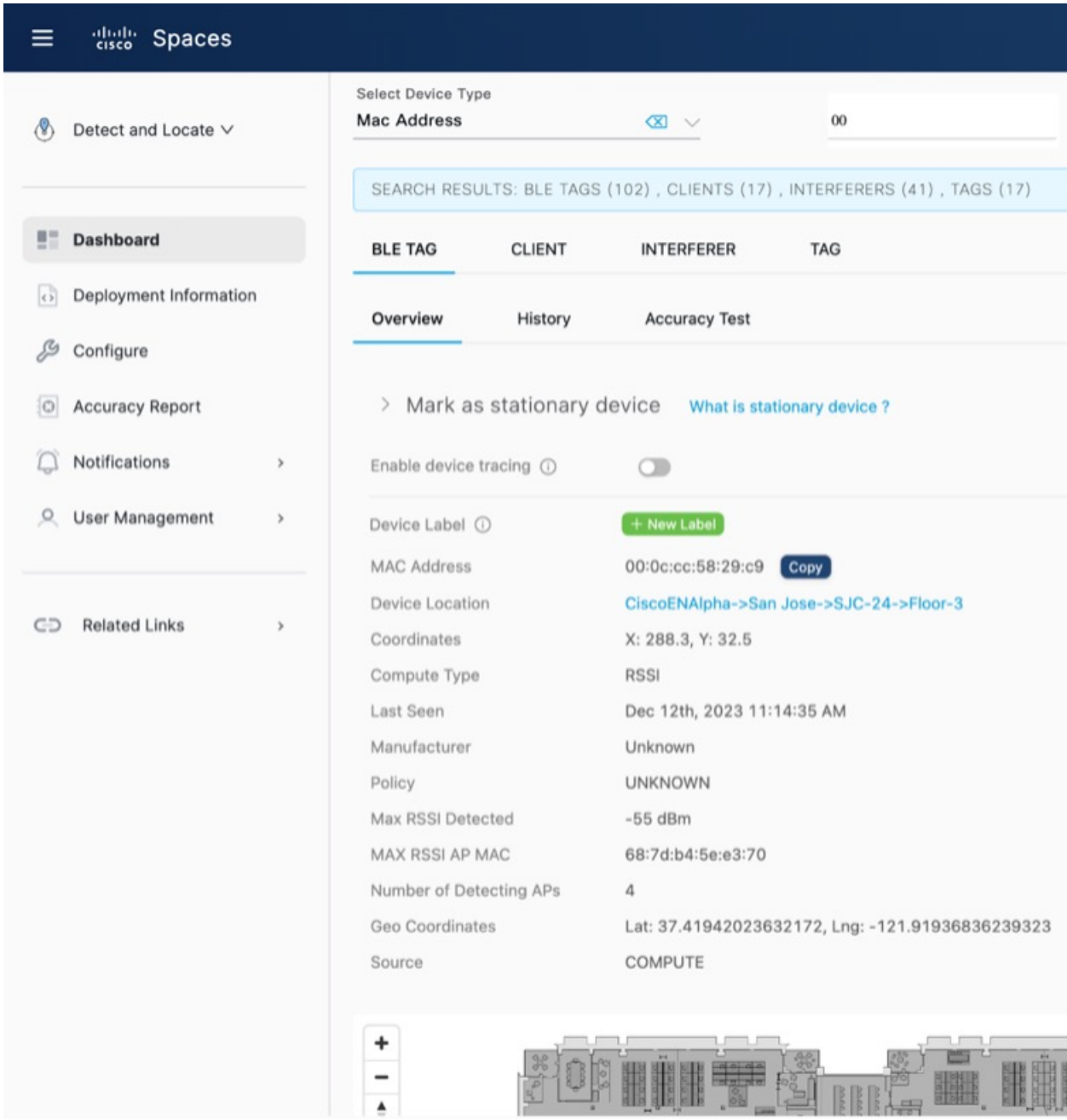
You can access this window with details of a device in any of the following ways:

- **Global search**: Search for a device from the dashboard and click the device from the search results. For more information, 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



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.

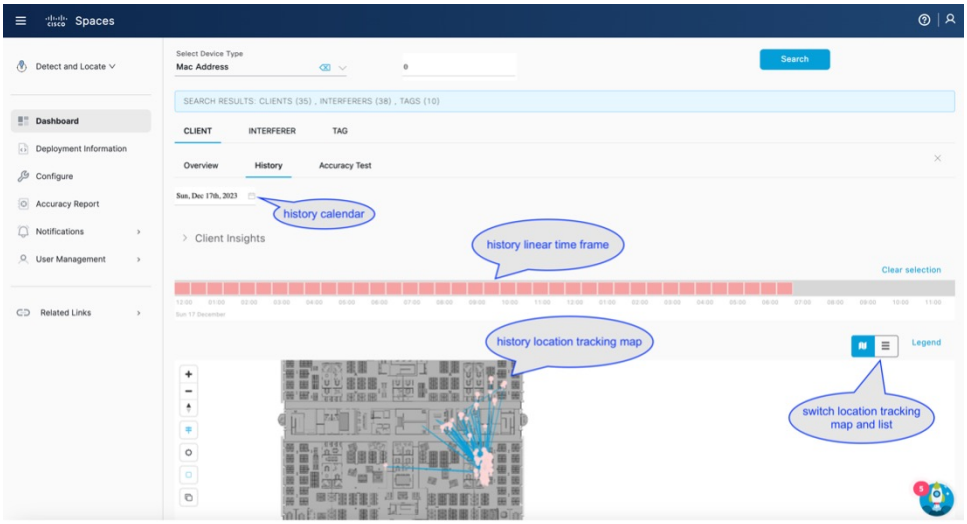
Each of these device history representations is described in detail in this article.

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



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.

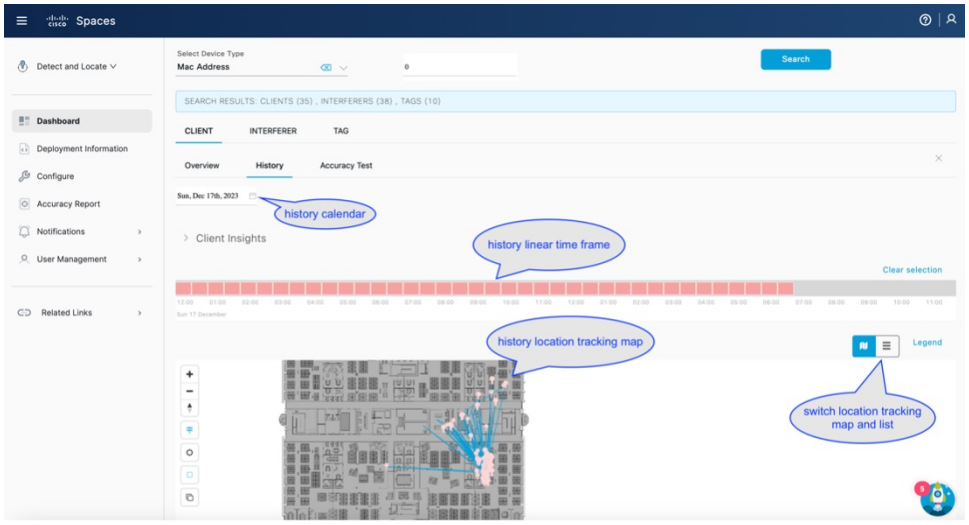
When you click on a particular block, you select the hour. You can observe that the map or list (below this linear time frame) is updated to represent the device's movements for the hour. You can learn more about this from Maps and Lists.

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:

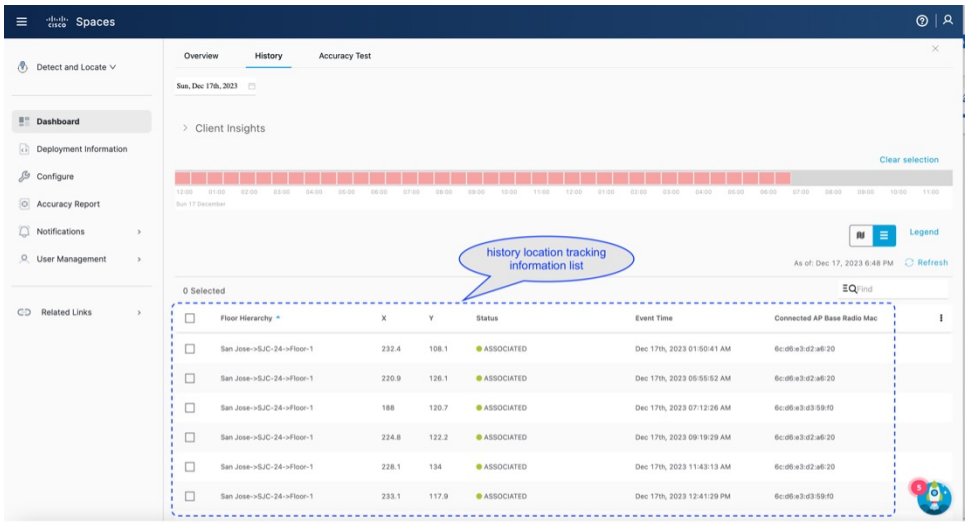
- **Maps**: have pink dots to represent the device's location on the map, and blue lines to indicate the path traversed by the device.

Figure 35: Map Showing a Device's Location History



- **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

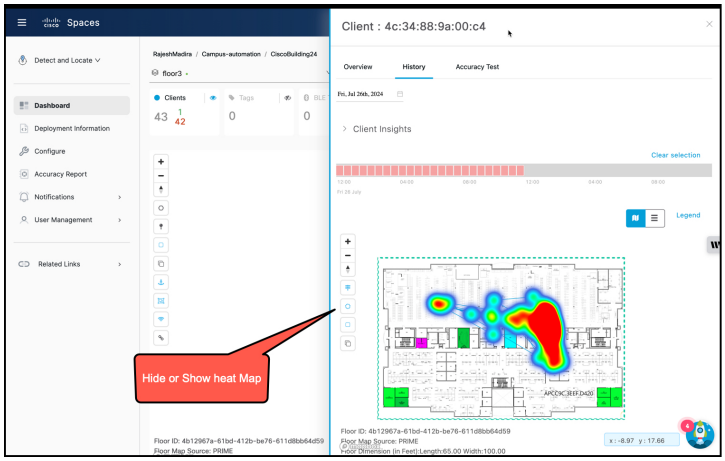


Heat Map

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.

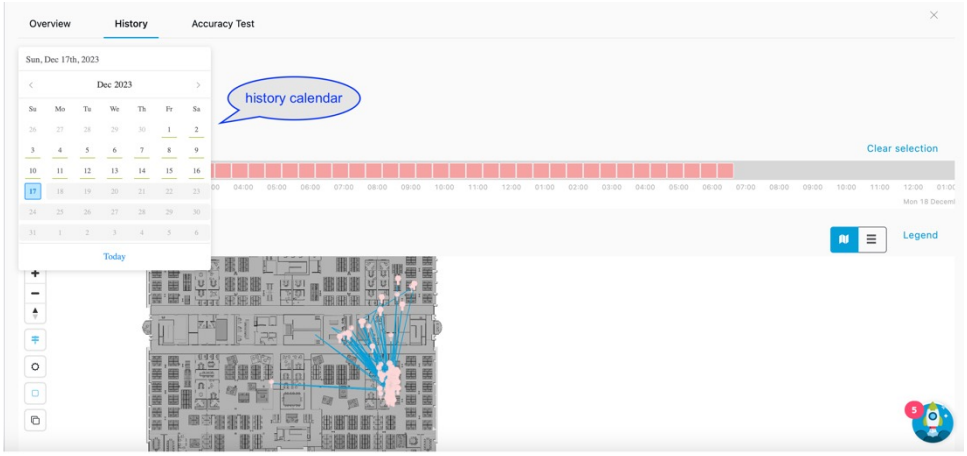
Figure 37: Heatmap of a Device



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



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.

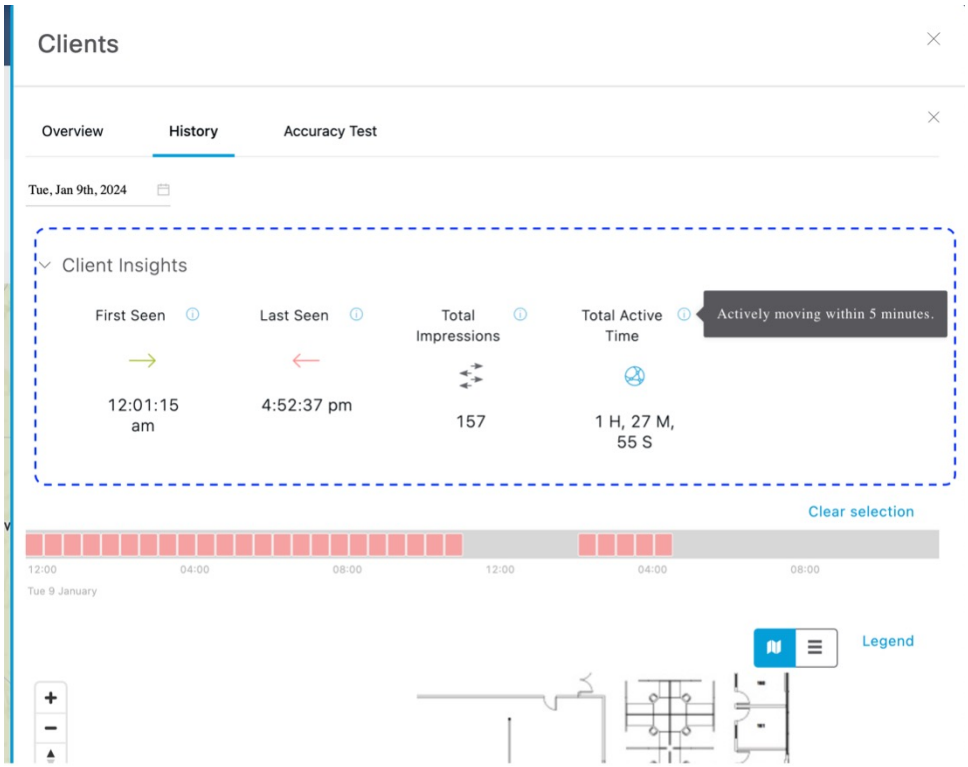
The calendar contains data for 30 days before the current date only. Visual indicators used to reflect the availability of historical records are

- **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

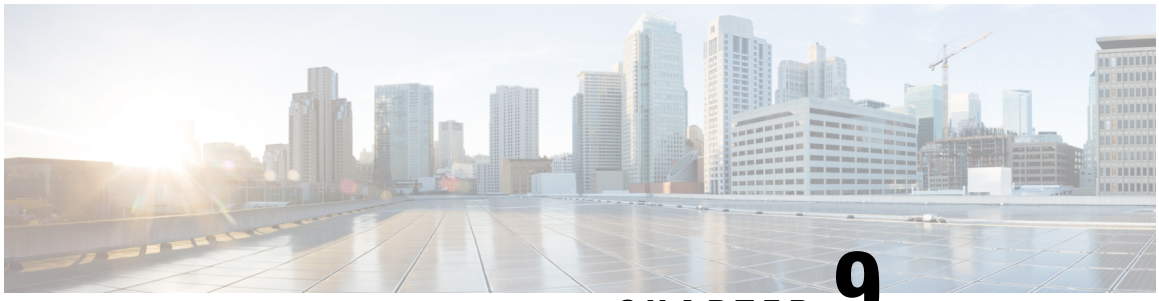


- **First Seen:** is the time and date when the wireless controller first detected the device within a specific period.

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, on page 47

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.

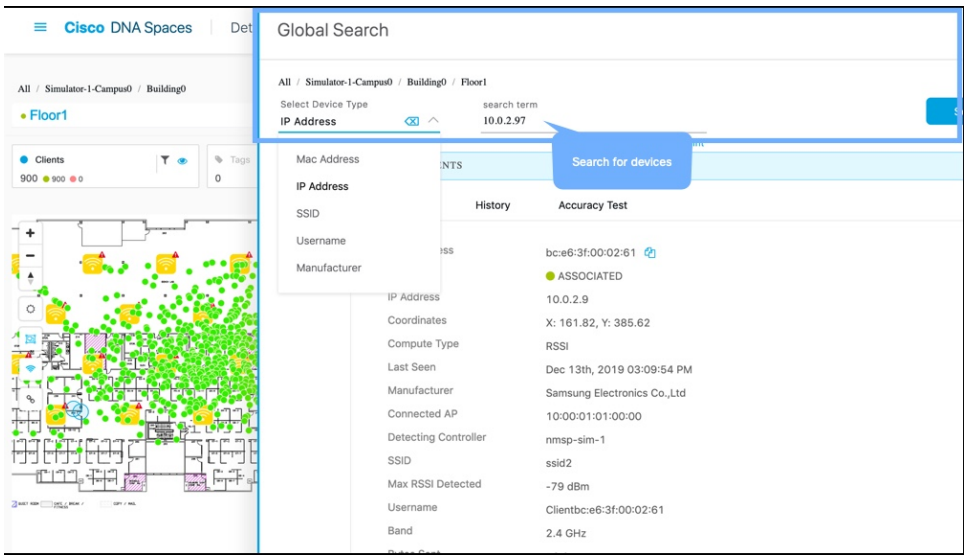
Test Location Accuracy

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

Procedure

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



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

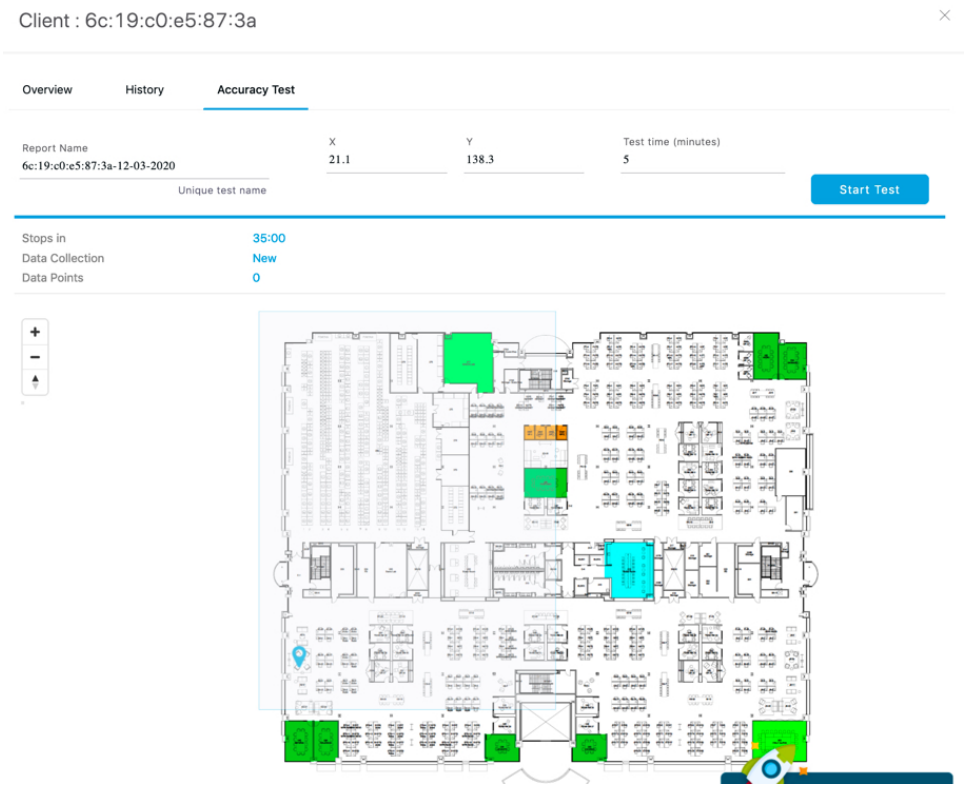
Step 3 In the device details window, click **Accuracy Test** tab.

Figure 41: Detect and Locate; Initiate Accuracy Test



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

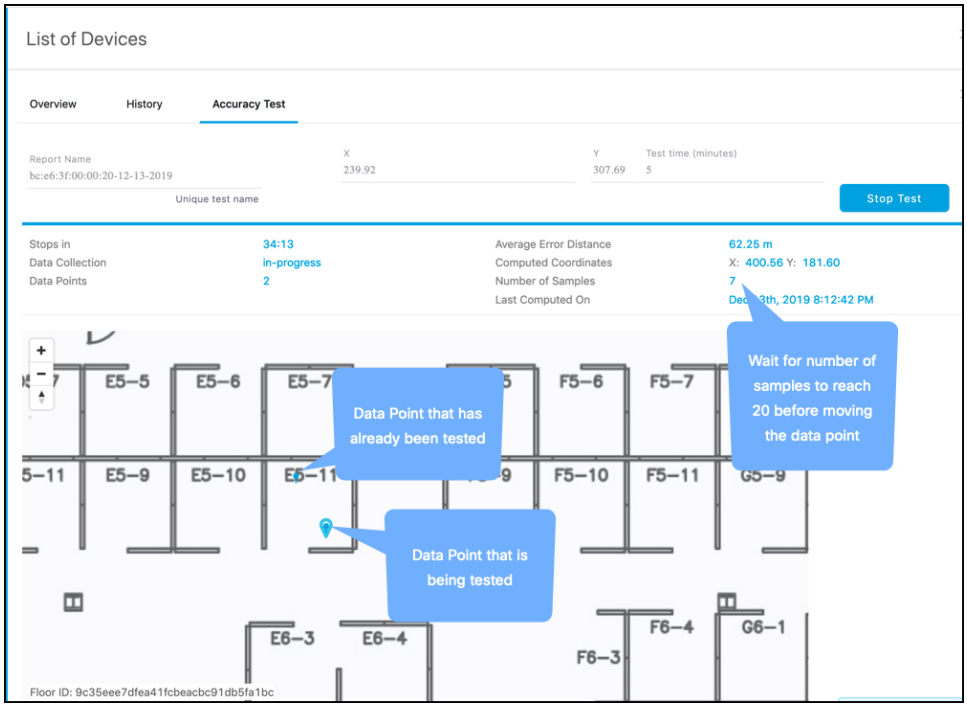


You can observe that the number of samples begins to increase.

Note
The display refresh time is three seconds.

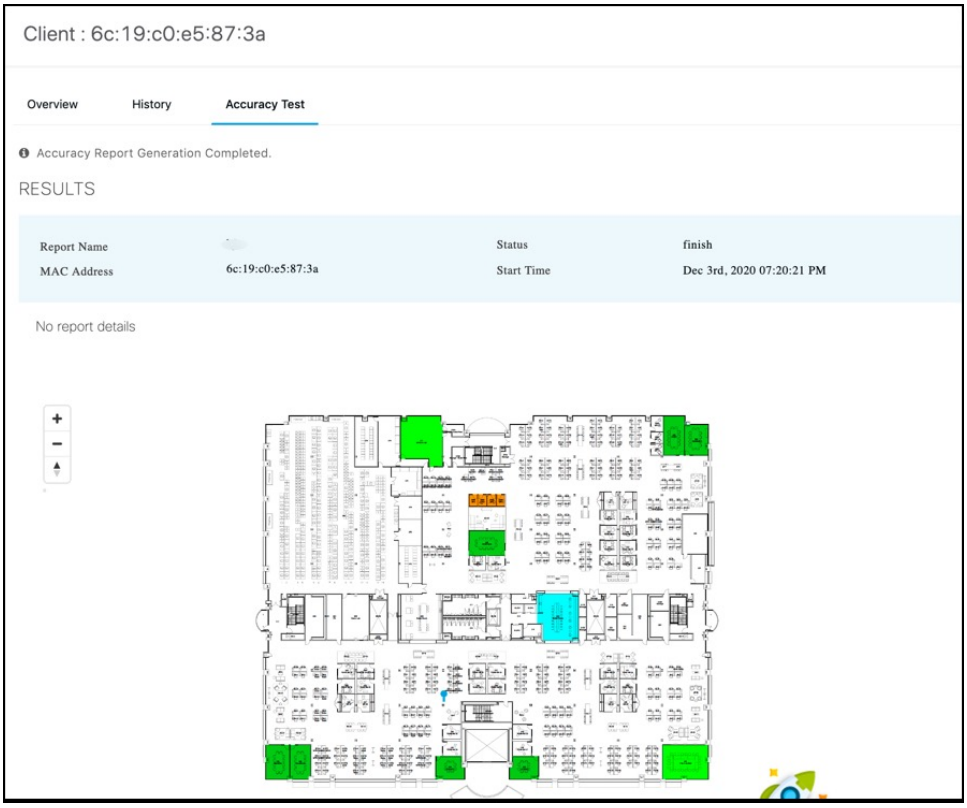
Step 5 Wait for the number of samples to reach 20 and click **Stop Test**. Move the blue pointer representing the data point to a new location and click **Start Test** again.

Figure 43: Sample Size Must Reach 20



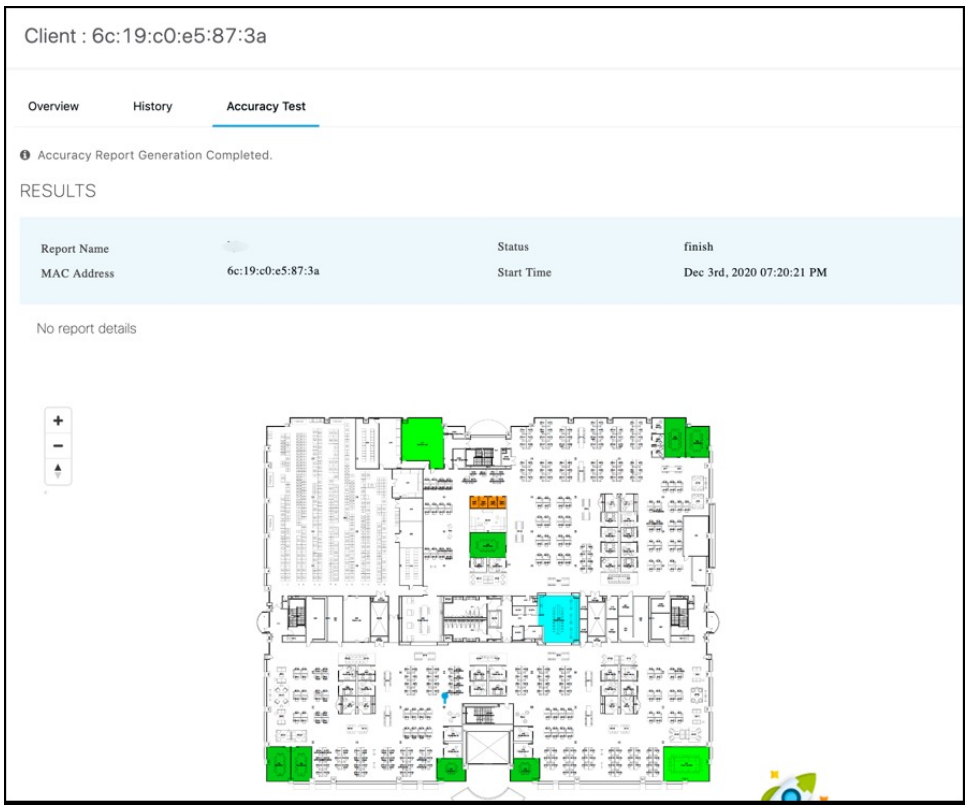
Step 6 Repeat for multiple locations for a more accurate understanding of location accuracy.

Figure 44: Repeat For Multiple Locations



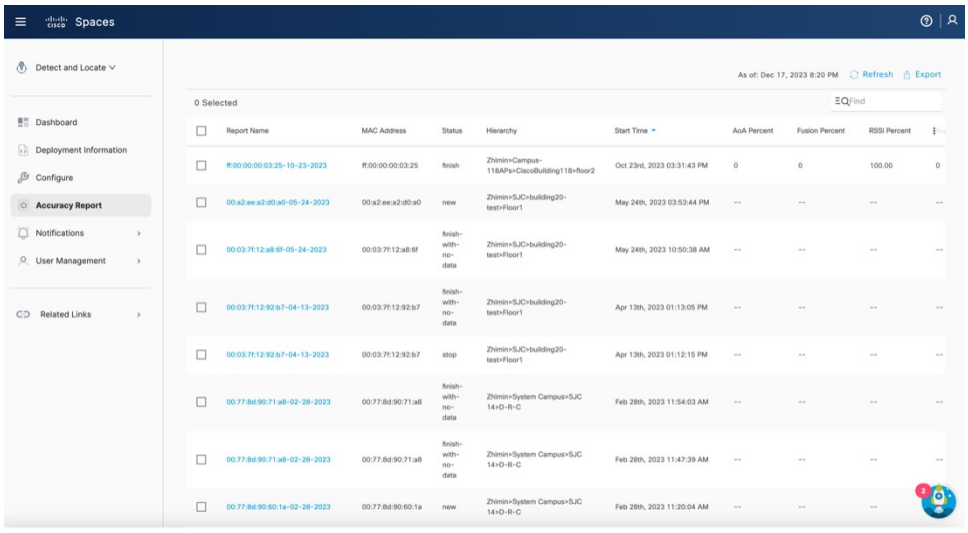
Step 7 Repeat for multiple locations for a more accurate understanding of location accuracy.

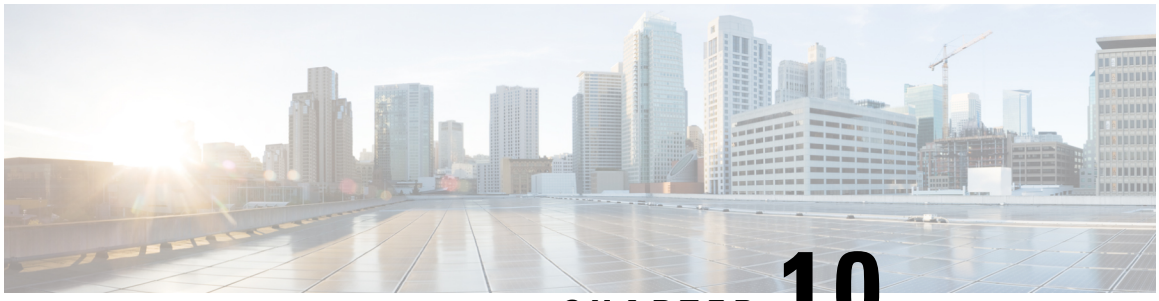
Figure 45: Repeat For Multiple Locations



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





CHAPTER 10

How to Track Devices

- Device Tracking, on page 53
- Device Visibility, on page 54
- Filter Tracked Devices, on page 56

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:

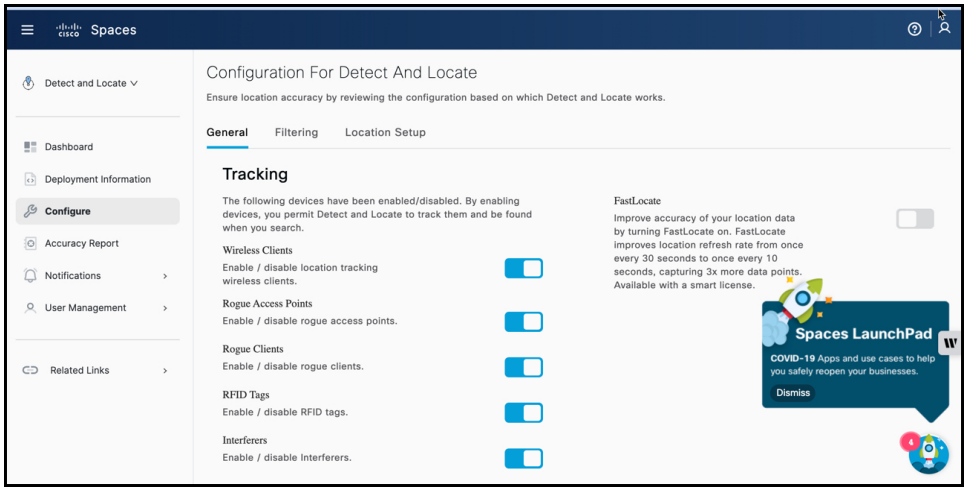
Procedure

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



Device Visibility

Enable Device Visibility

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

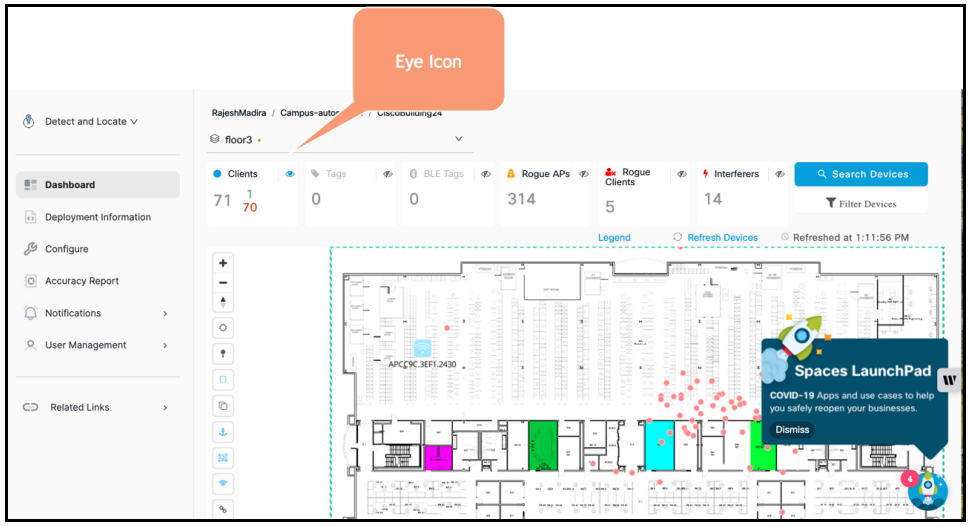
Procedure

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



View Enabled Device Types

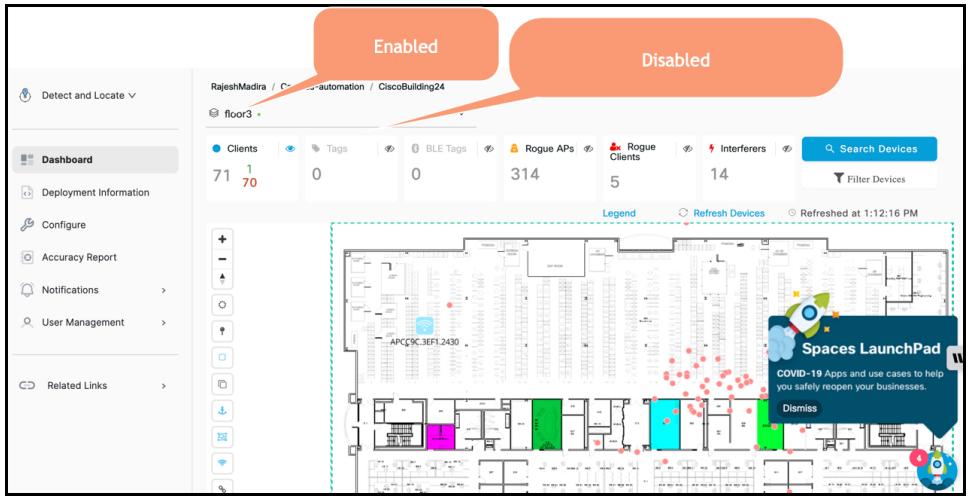
Follow these steps to view the enabled device types:

Procedure

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



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.

Filter Tracked Devices

Configure Cutoff for Location Accuracy

You can configure thresholds or cutoff at which you want the server to discard AP measurements. To configure thresholds and cutoffs.

Procedure

Step 1 Navigate to **Configure > Location Setup**.
Step 2 Enter the RSSI Cutoff (dBm) value in the corresponding field.
Step 3 Specify the desired RSSI cutoff value in dBm.

Configure Filter Values For Tracked Devices

Follow these steps to configure filtering parameters:

Procedure

Step 1 Configure filtering parameters from the **CONFIGURE > Filtering** tab.
Step 2 Specify the **RSSI Cutoff** value to filter out weak probing clients.
Step 3 Toggle the **Exclude Probing Only client** button to include or exclude probing-only clients.
Step 4 Toggle the **Enable MAC Filtering** button to enable or disable MAC filtering.
Step 5 Manage allowed SSIDs using the **Allow Location SSID Filtering** list.
Step 6 Manage disallowed SSIDs using the **Disallowed Location SSID Filtering** list.

Step 7 Toggle the **Enable Locally Administered MAC Filtering** button to enable or disable locally administered MAC filtering.

Parameters to Filter Tracked Devices

You can configure the parameters below to filter the devices that are tracked on the Detect and Locate dashboard:

1. **RSSI Cutoff:** Specifies the cutoff value for filtering out weak probing clients.
2. **Exclude Probing Only client:** Toggle button for including or excluding probing-only clients.
3. **Enable MAC Filtering:** Toggle button for enabling or disabling MAC filtering.
4. **Allow Location SSID Filtering:** List of allowed SSIDs.
5. **Disallowed Location SSID Filtering:** List of disallowed SSIDs.
6. **Enable Locally Administered MAC Filtering:** Toggle button for enabling or disabling locally administered MAC filtering.



Note For more information about the SSID name validation (allowed and disallowed inputs) in the **Configure** > **Filtering** sections, see SSID Validation, on page 57.

SSID Validation

Allowed SSID names for the list of allowed or disallowed values must be from 1 to 32 characters and may contain only printable ASCII characters.

SSID names support these ASCII characters:

- **Numerals**: 48 through 57 hex (0 to 9)
- **Alphabets (uppercase)**: 65 through 90 hex (A to Z)
- **Alphabets (lowercase)**: 97 through 122 hex (a to z)
- **ASCII space**: 20 hex
- **Printable special characters**: 21 through 2F, 3A through 40, and 5B through 60 hex, that is: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Valid SSID names

Some valid SSID names are:

Table 4: Valid SSID examples

Valid SSID	Validation criteria
Home123	Uses only letters and numbers

Valid SSID	Validation criteria
Office_WiFi	Uses underscore (_)
Guest-Access!	Uses dash (-) and exclamation mark (!)
My WiFi 2026	Uses space and numbers
[Secure]Net*	Uses brackets and asterisk (*)
Cafe@Main$	Uses @ and $ special characters
Test#SSID	Uses hash (#)
!Welcome-Home!	Uses exclamation (!) and dash (-)
ABCDEFGHIJKLMNOPQRSTUVWXYZ123456	32 characters, within limit
{Dev}_Lab	Uses curly braces, underscore, and letters
1234567890	Numbers only
A_Z-a.z	Uses underscore (_), dash (-), dot (.)
Main$Net%2026	Uses dollar ($), percent (%), and numbers

Invalid SSID names

These characters are not supported in SSID names:

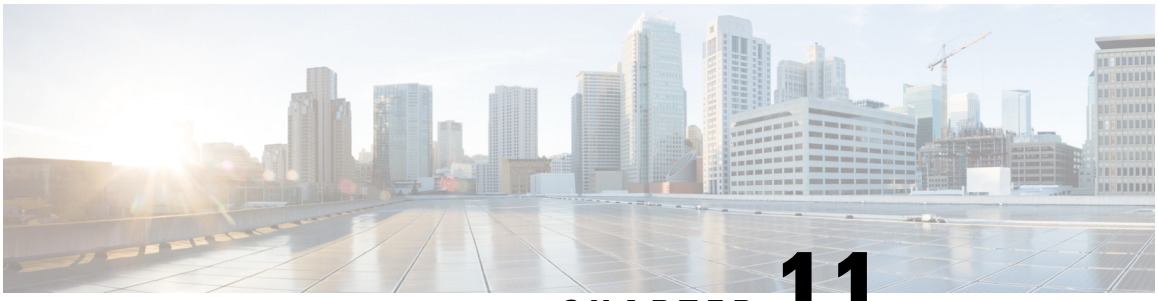
- Non-ASCII characters
- Emoji
- Control characters (e.g., \n, \t)
- Names longer than 32 chars
- Do not use empty names.
- Do not use non-printable or extended Unicode/emoji characters.

Some invalid SSID names are:

Table 5: Invalid SSID examples

Invalid SSID	Validation criteria
CaféWiFi	Contains non-ASCII character "é"
NetName□□	Contains emoji
WiFi/Name/Longer/Than/32/CharactersIsNotValid	Exceeds 32 characters
MyWiFi\nName	Contains control character (\n)
WiFi\tTab	Contains control character (\t)

Invalid SSID	Validation criteria
(empty string)	Cannot be empty
SSID名称	Contains non-ASCII characters (Chinese)
فاي شبكةواي	Contains non-ASCII characters (Arabic)
WiFi□□	Contains emoji
BestWiFiInBangalore*2026202620262026	Exceeds 32 characters



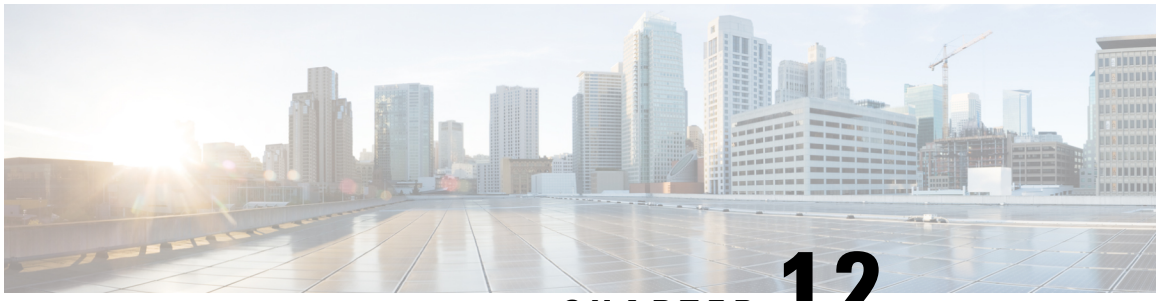
CHAPTER 11

Manage Columns

• Manage Columns, on page 61

Manage Columns

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



CHAPTER 12

Manage Session Expiry

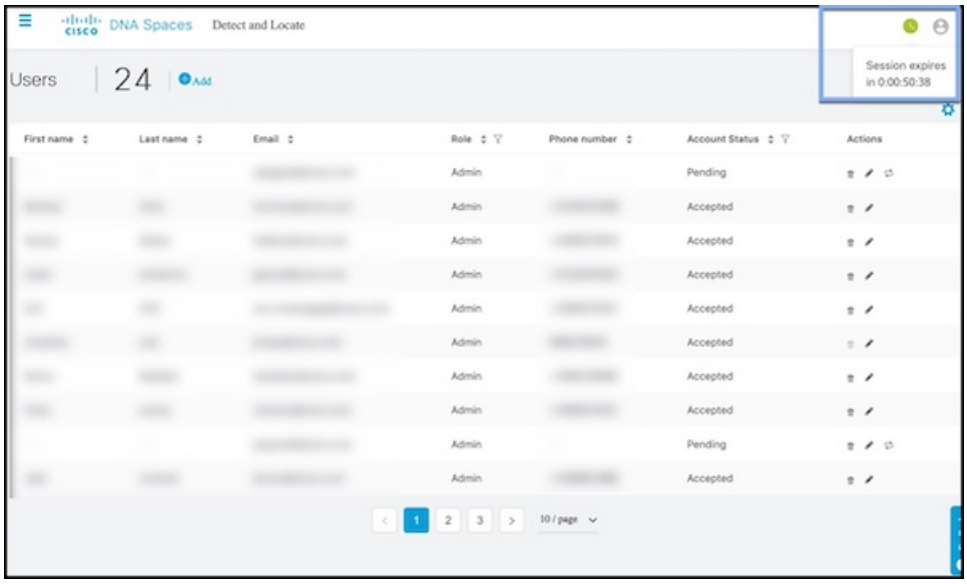
- Session expiry, on page 63

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

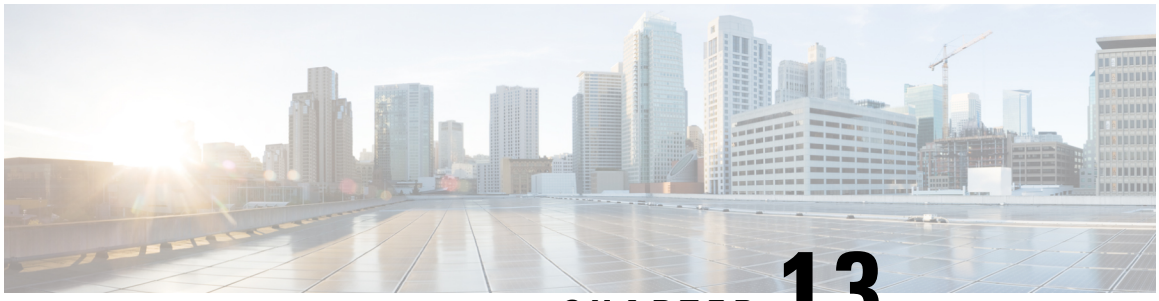




PART IV

Deployment Information

- Deployment Information, on page 67



CHAPTER 13

Deployment Information

- Access Point Deployment Information, on page 67

Access Point Deployment Information

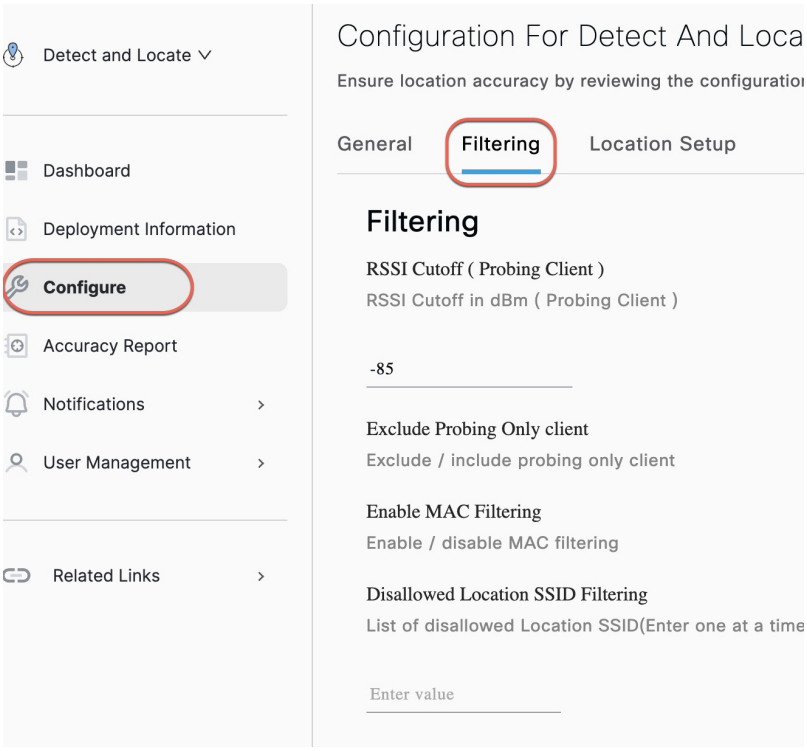
The **Deployment Information** dashboard provides an overview of Access Points (APs) with respect to the Wireless Controller and available floor maps in the account. The dashboard displays information based on devices reporting within the last hour and the **Filtering** settings configured in the Cisco Spaces: Detect and Locate app.

Note The consolidation of reporting APs occurs over an hour period, after which the report is published. The current report may differ from previous reports due to devices entering and leaving the network.

It captures data related to reporting (active) and missing APs only after applying all selected filters to the incoming data. For example, when you enable the **Probing Client** filter, the system excludes packets from probing devices and collects AP data only for the remaining devices. This does not mean other APs stop transmitting data; it simply indicates their data is excluded due to the applied filters.

Another instance of APs not transmitting data occurs when there are no devices to report on a given floor. As a result, APs flagged as inactive due to data unavailability in Cisco Spaces require cross-checking in Cisco Catalyst Center to confirm their uptime and health status. If the APs are confirmed as active in Cisco Catalyst Center, no further action is required.

Figure 51: Configuration for Detect And Locate

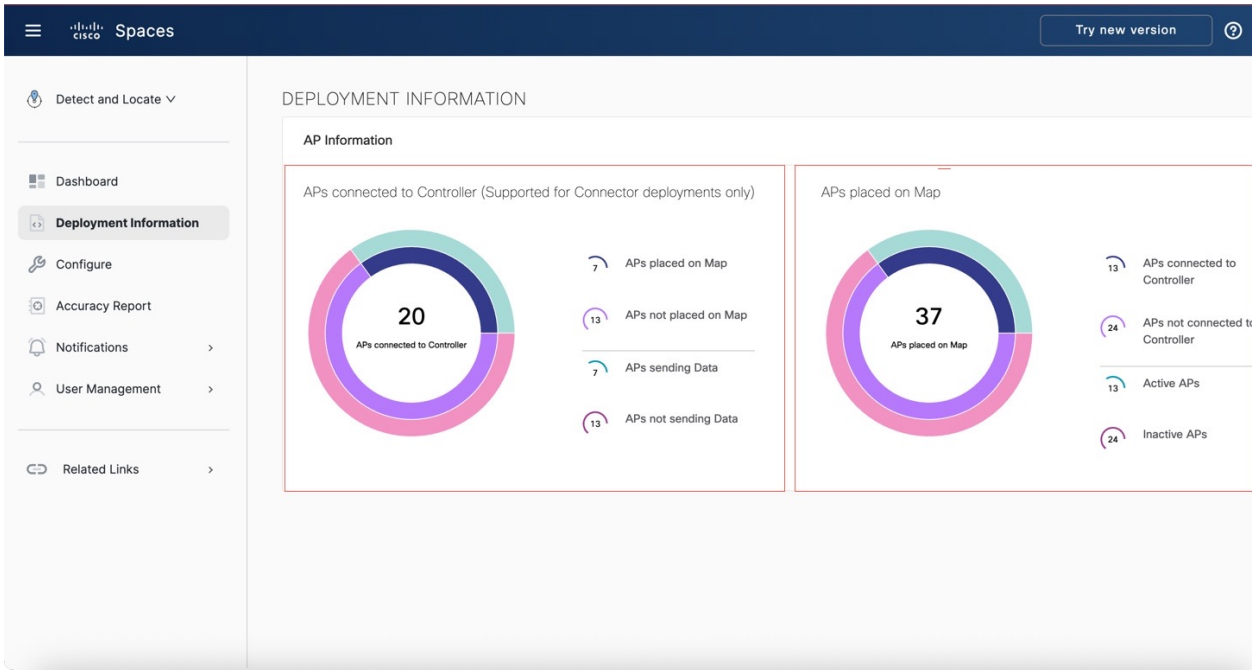


In the **AP Information** area, view this information:

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

The **Deployment Information** window presents two graphs. One graph displays data collected from the wireless controller, while the other shows the same data gathered from the Cisco Spaces maps. Please compare the information in the two graphs.

Figure 52: Deployment Information



Left Graph: Shows APs count in relation to wireless controller

- **APs Placed on Map**: These are the APs that are both connected to a wireless controller and placed on the floor maps across any hierarchy, campus, or floor.

  In the sample image, 20 APs are connected across all wireless controller, and seven of them are placed on the map.

- **APs Not Placed on Map**: These are APs that are connected to an active wireless controller within the tenant but have not been placed on any map across any hierarchy, campus, or floor.

  In the sample image, out of the 20 total connected APs, 13 are not placed on the Cisco Spaces map.

- **APs Sending Data**: These are APs from which RSSI data has been received in the last one hour after the filters are applied.

  In the sample image, 7 APs are sending RSSI data, that indicates that data is received from 7 out of the 20 total APs.

- **APs Not Sending Data**: These are APs from which no RSSI data is received in the last one hour after the filters are applied.

  In the sample image, 13 APs are not sending data, that indicates no RSSI data is reported from these APs, out of the total 20.

Right Graph: Shows Aps count in relation to floor maps

Inactive APs are displayed on the Cisco Spaces map, but they do not report the data they receive. The data is not reported because the APs are either not connected to the Wireless Controller or they are connected but not transmitting the measured data. You can find the specifics of this information by cross-referencing with the graphs.

- **APs Connected to Controller**: These are APs that are currently connected to the wireless controller and also placed on the map across various hierarchies or campuses.

  In the sample image, there are 37 APs placed on the map, out of which 13 are connected to the wireless controller.

- **APs Not Connected to Controller**: These are APs that are placed on the map across any hierarchy, campus, or floor but are not currently connected to any controller in the tenant. This count may include AP's from previously added controllers that were never removed from the map.

  In the sample image, there are 24 such APs placed on the map but not connected to any controller. Do not confuse this with the APs not sending data mentioned earlier. Those APs are connected to a controller but simply not placed on the map. In contrast, the 24 APs here are placed on the map but not connected to any controller.

- **Reporting (Active) APs**: These are APs that are both placed on the map and have reported RSSI data within the last one hour.

  In the sample image, 13 APs are active, placed on the map and sending RSSI data.

- **Inactive APs**: These are APs that are placed on the map but have not reported any RSSI data in the last one hour. This includes APs that may no longer be connected to any wireless controller but are still visually present on the map.

  In the sample image, 24 APs are inactive, meaning no recent RSSI data has been received from them.

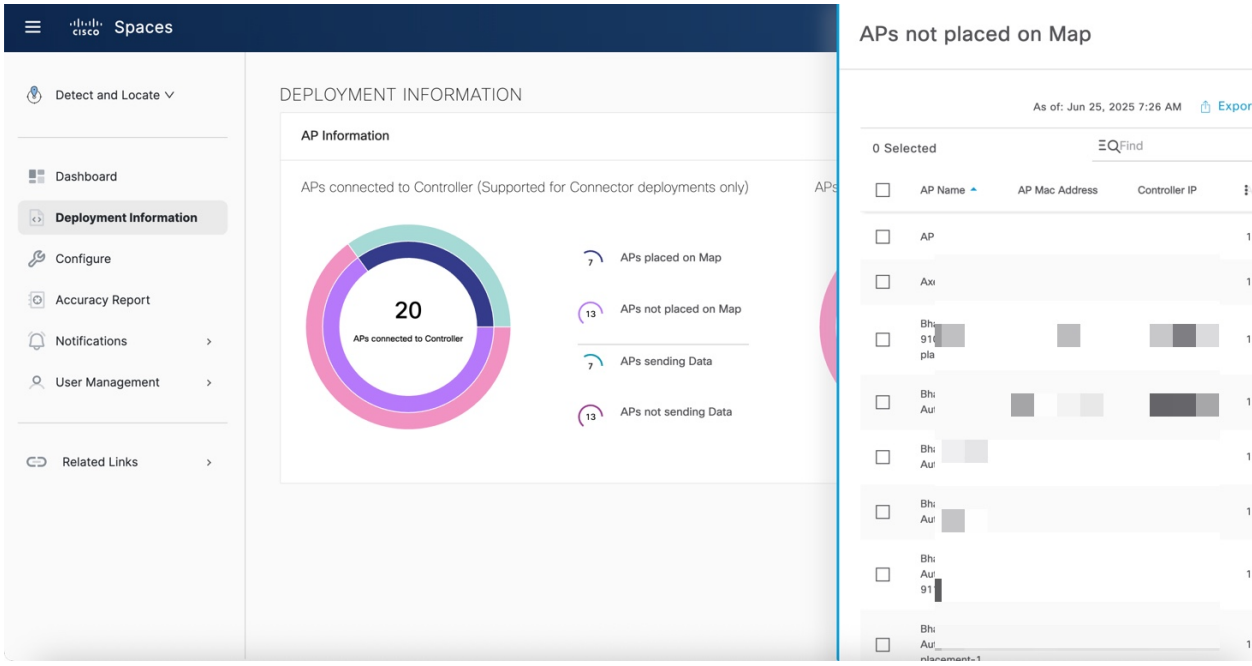


Note Each of the categories in both graphs displays detailed information when the respective buckets are clicked on.

Detailed AP information

To see a more detailed list of APs in any of the category, click each metric. A slide-in pane is displayed with AP name, MAC address and wireless controller IP.

Figure 53: AP Detailed List

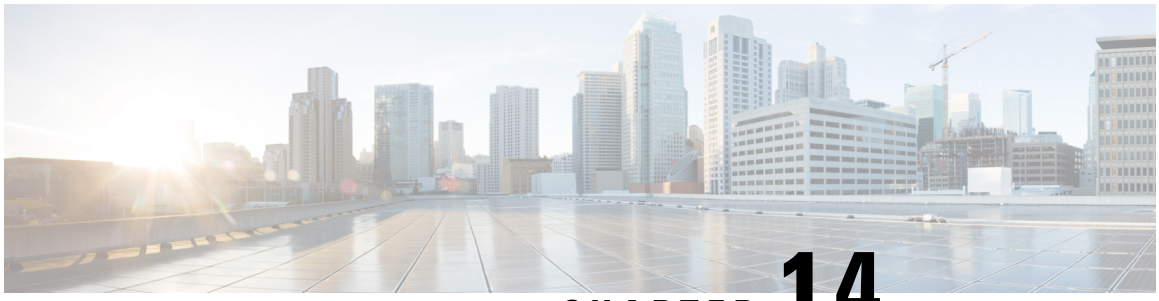




PART V

Hyperlocation and FastLocate

- Configuring Hyperlocation, on page 75
- Configure Cisco FastLocate, on page 79



CHAPTER 14

Configuring Hyperlocation

- Enabling Cisco Hyperlocation, on page 75

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.

Procedure

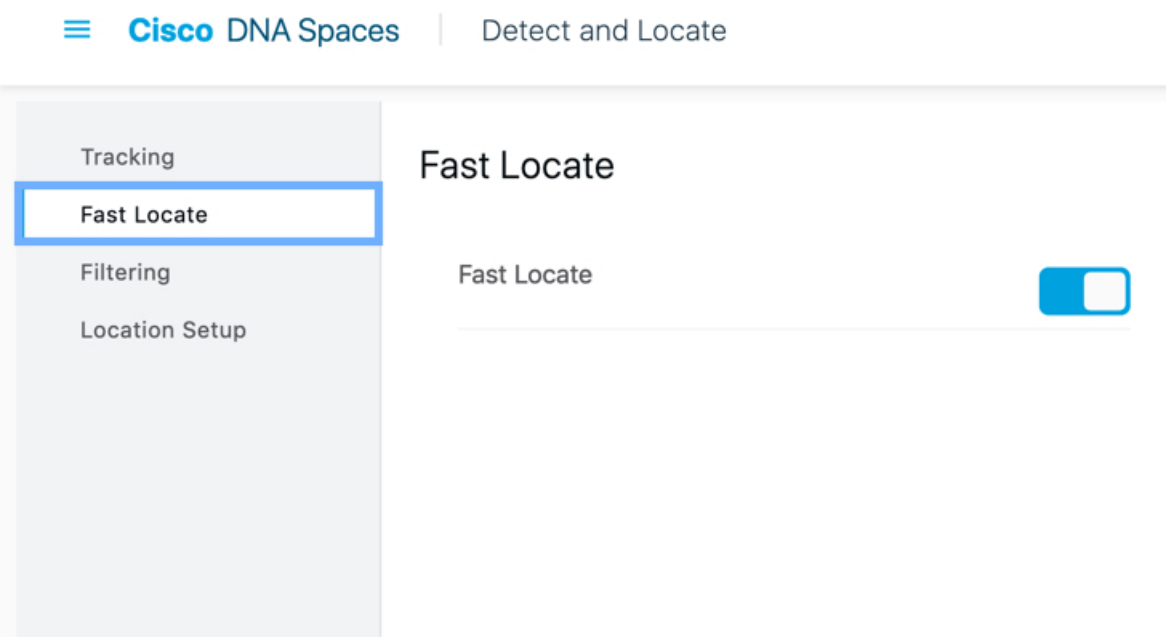
Step 1 Enable Hyperlocation on wireless controller.

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.

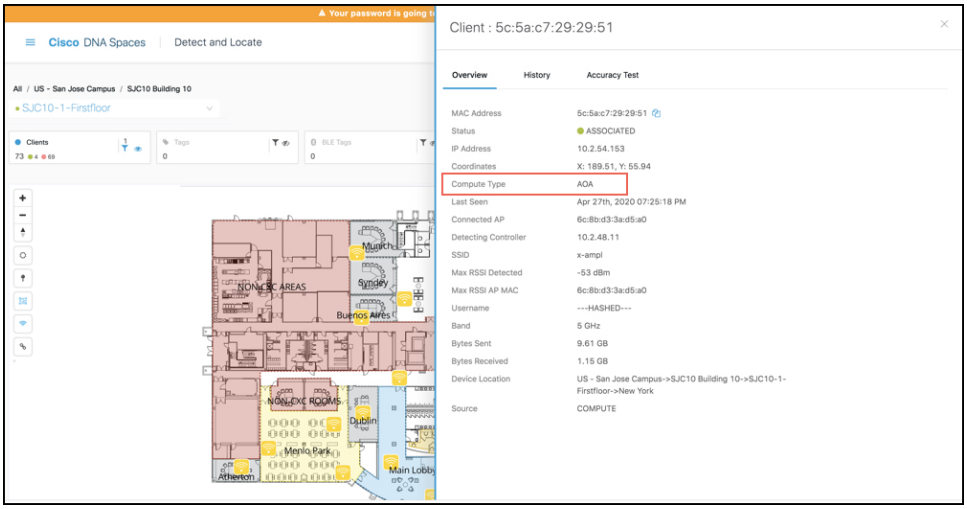
Navigate to Cisco Spaces: Detect and Locate dashboard. On the left-navigation pane, click **Configure** and enable the **Fast Locate** option.

Figure 54: Enabling Hyperlocation on Cisco Spaces: Detect and Locate



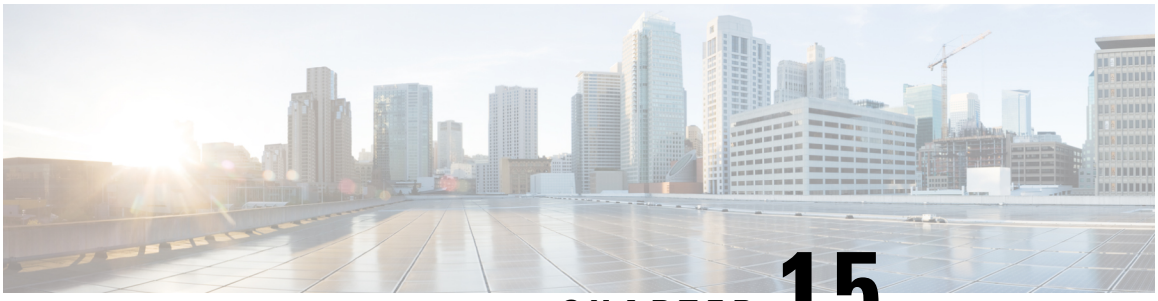
Step 3 Verify if Cisco Spaces: Detect and Locate is receiving Angle of Arrival (AoA) packets from client devices.

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



- 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 79

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.

Procedure

Step 1 Enable Hyperlocation on wireless controller.

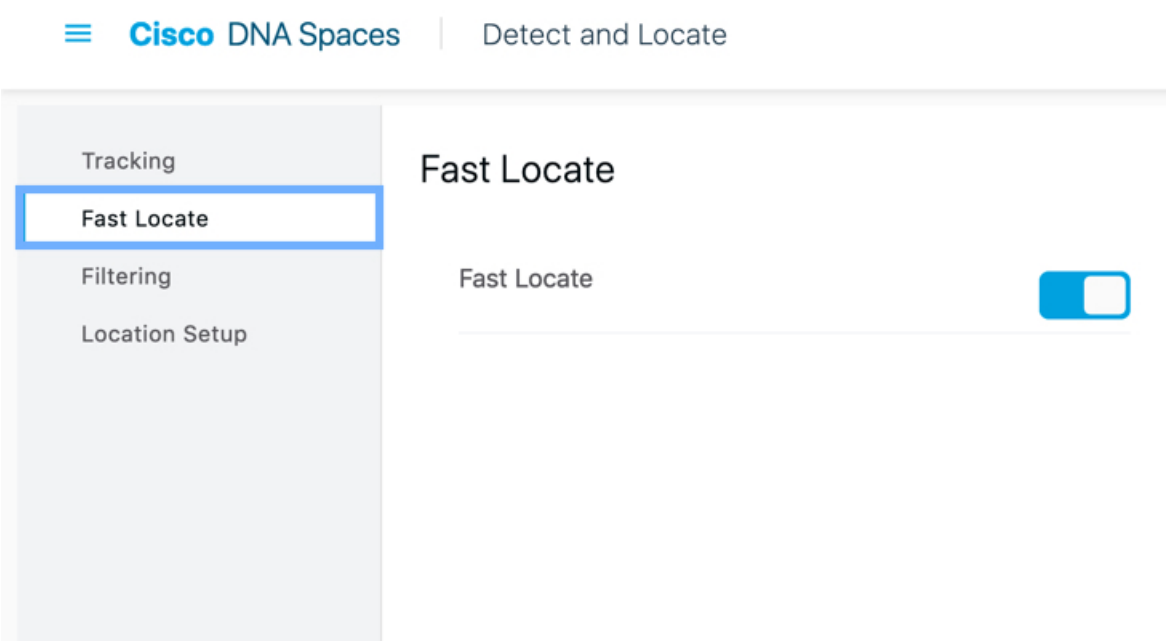
For instructions on how to enable hyperlocation on your specific wireless controller, see the respective configuration guide of your installed version.

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

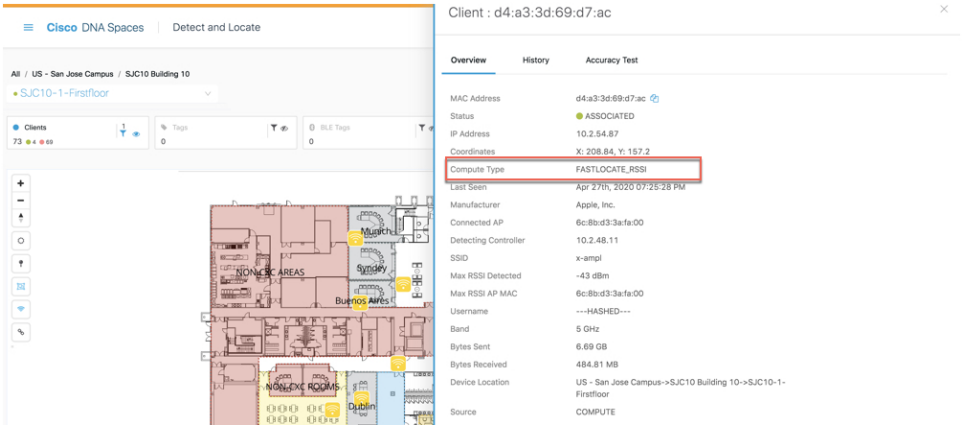


Step 3 Verify if Cisco Spaces: Detect and Locate is receiving Cisco FastLocate RSSI packets from client devices.

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.

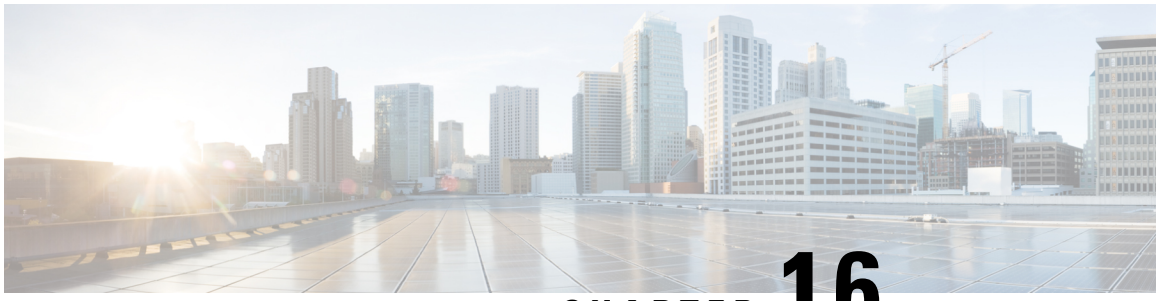




PART VI

Manage Notifications

- Using Northbound Notifications, on page 85



CHAPTER 16

Using Northbound Notifications

• Using Northbound Notifications , on page 85

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.

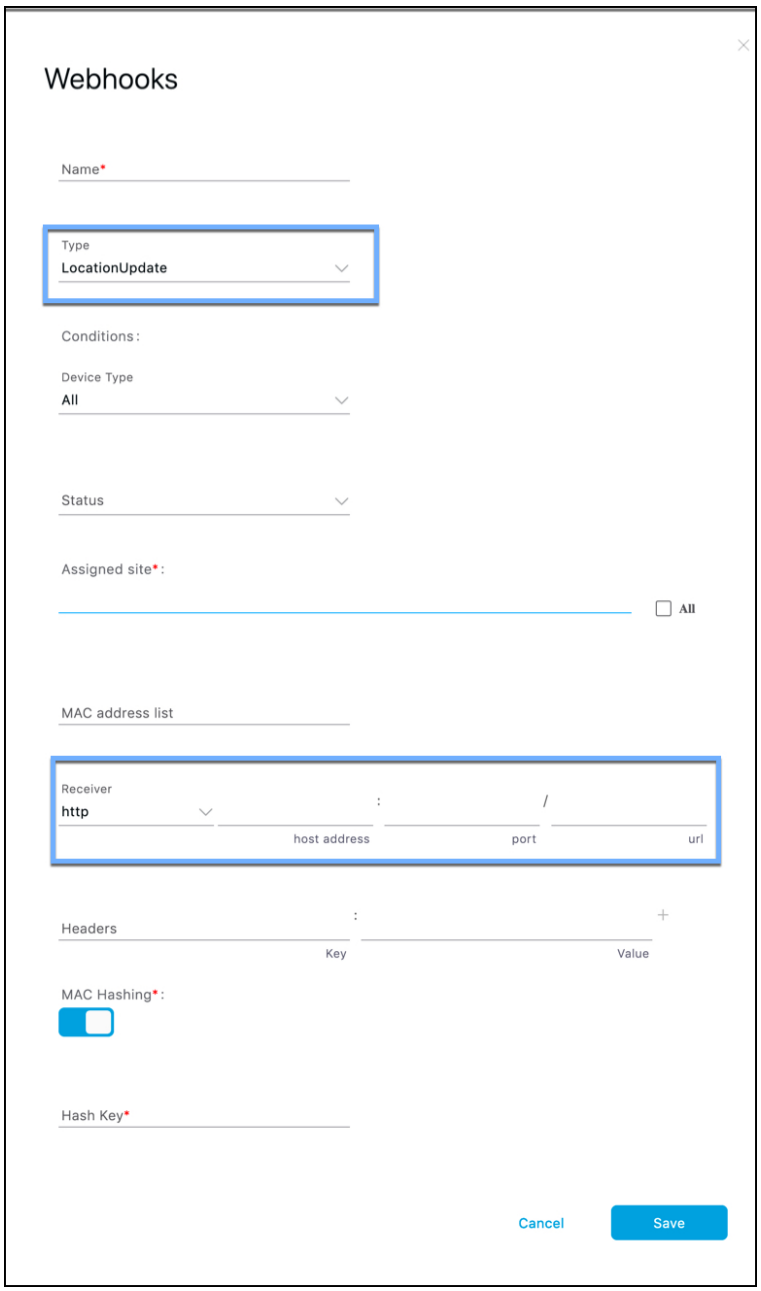
Currently, the following notification types are supported:

- **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 56: Location Update



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)

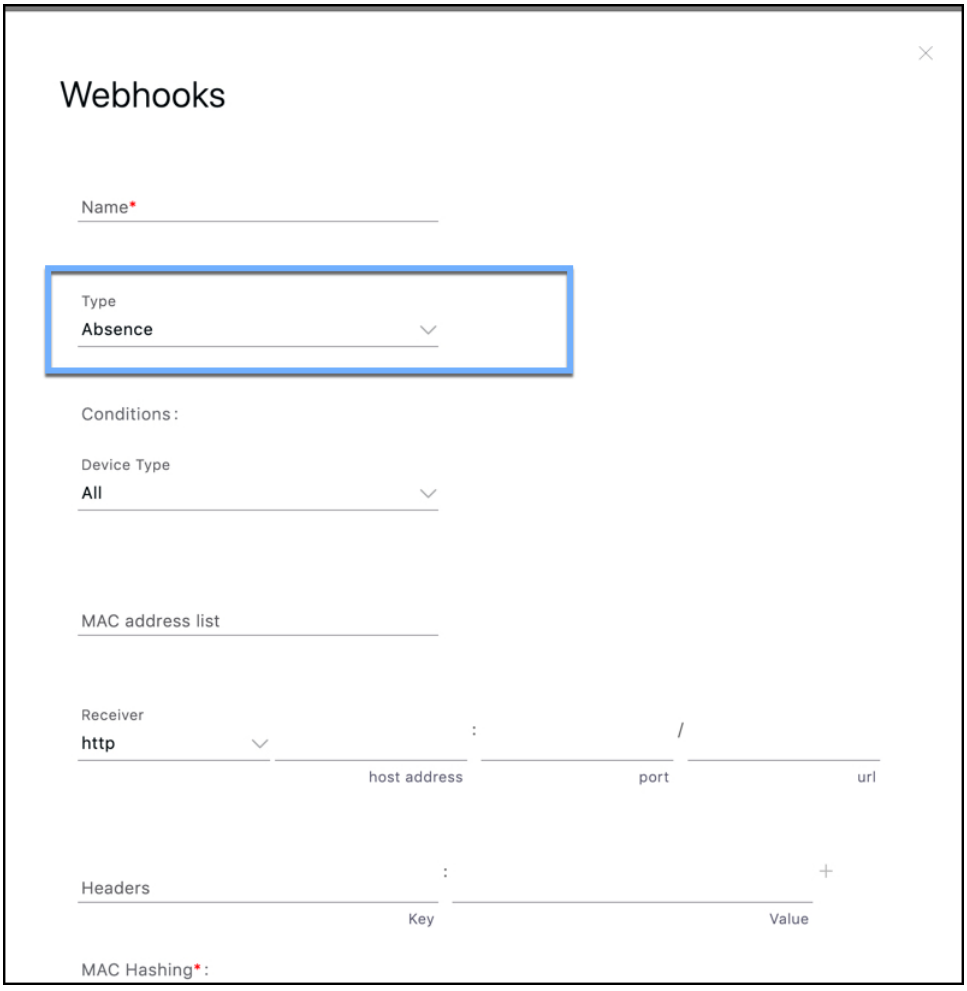
The following is a sample of the Location Update notification subscription:

```
{
    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 57: Absence



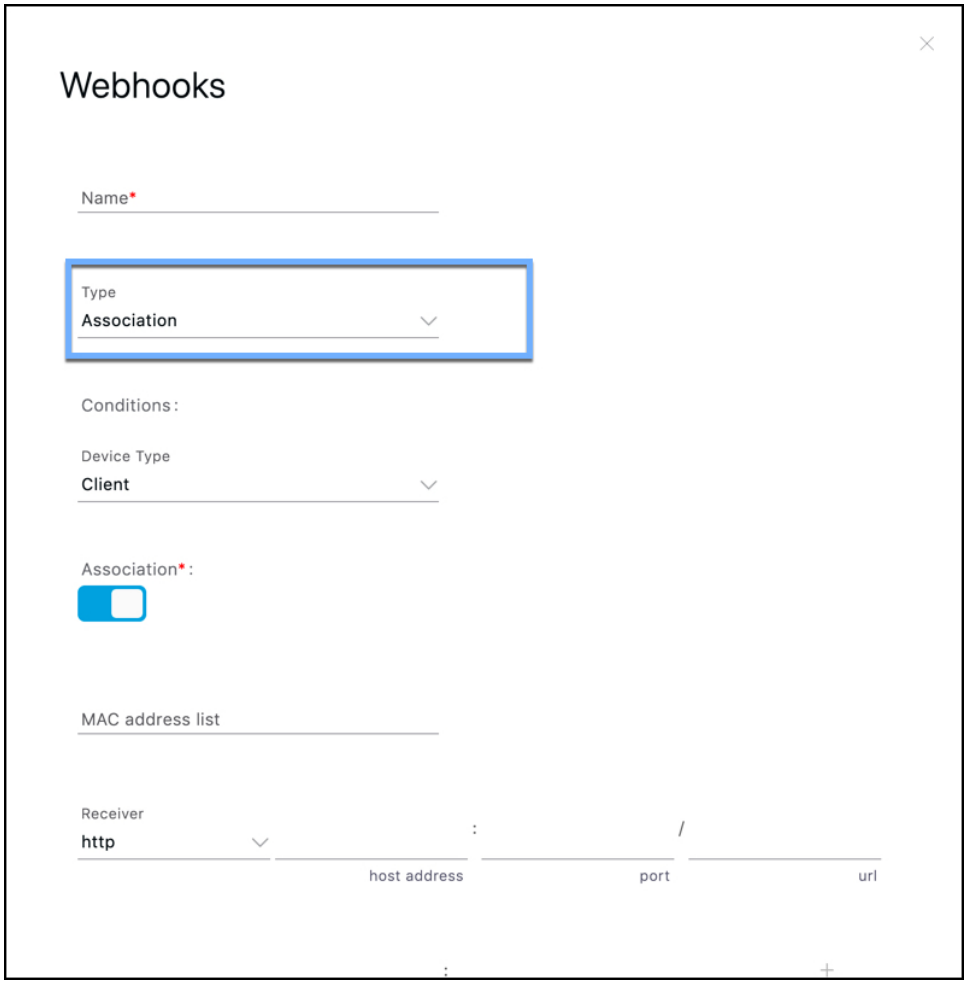
The fields of the **Absence** page are described below:

- **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 58: Association



- **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)

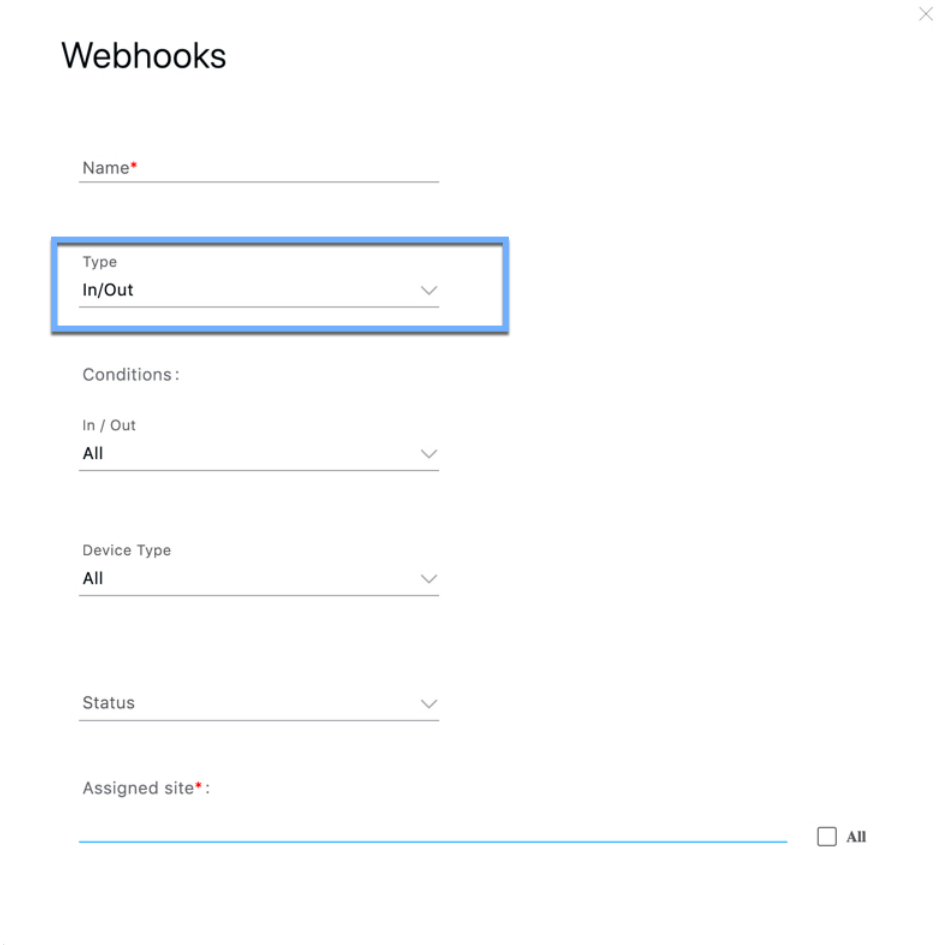
The following is a sample of the Association notification subscription:

```
{
    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 59: Absence



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:

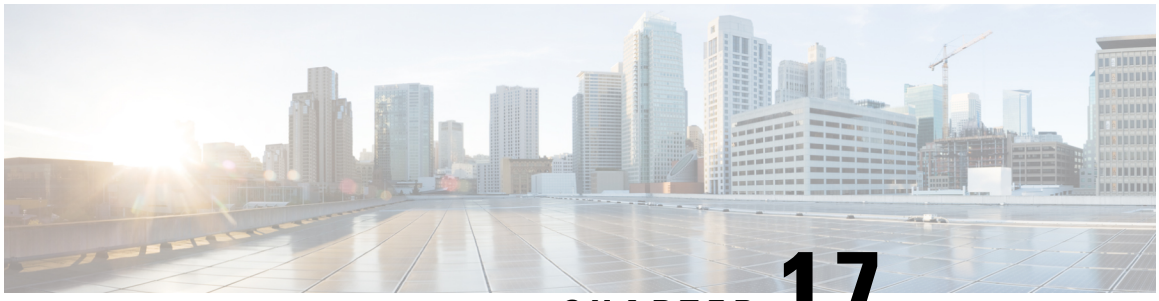
```
{
    tenantId: '2001',
    id: "552a1a14-20cb-4581-855d-f3c9f120248e",
    name: "Test InOut Notification",
    type: "InOut",
    userid: "testuser",
    enabled: true,
    intenal: false,
    conditions: {
        inout: "All",
        deviceType: "Client",
        status: "Associated",
        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 VII

Manage Users

- Manage Users, on page 95



CHAPTER 17

Manage Users

• Manage Users, on page 95

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 6: 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.

Procedure

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:

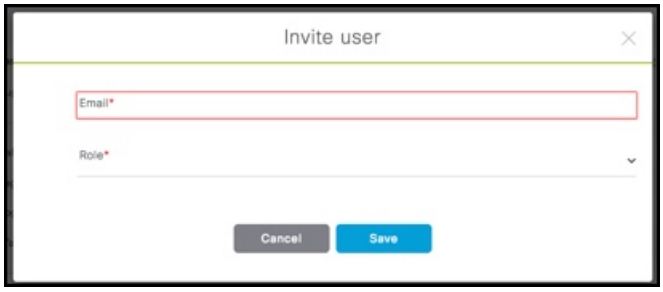
a) **Name**: Enter a name for the user role.

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.

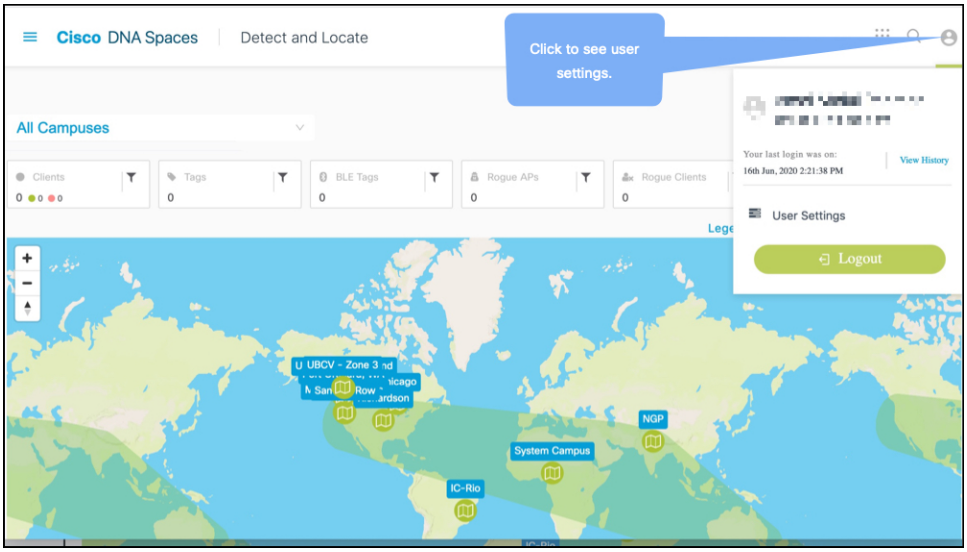
The Detect and Locate Administrator can modify User Roles only. The Detect and Locate Administrator can edit the role of a specific user by editing user details from **User Management > App Users**.

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.

Procedure

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**.

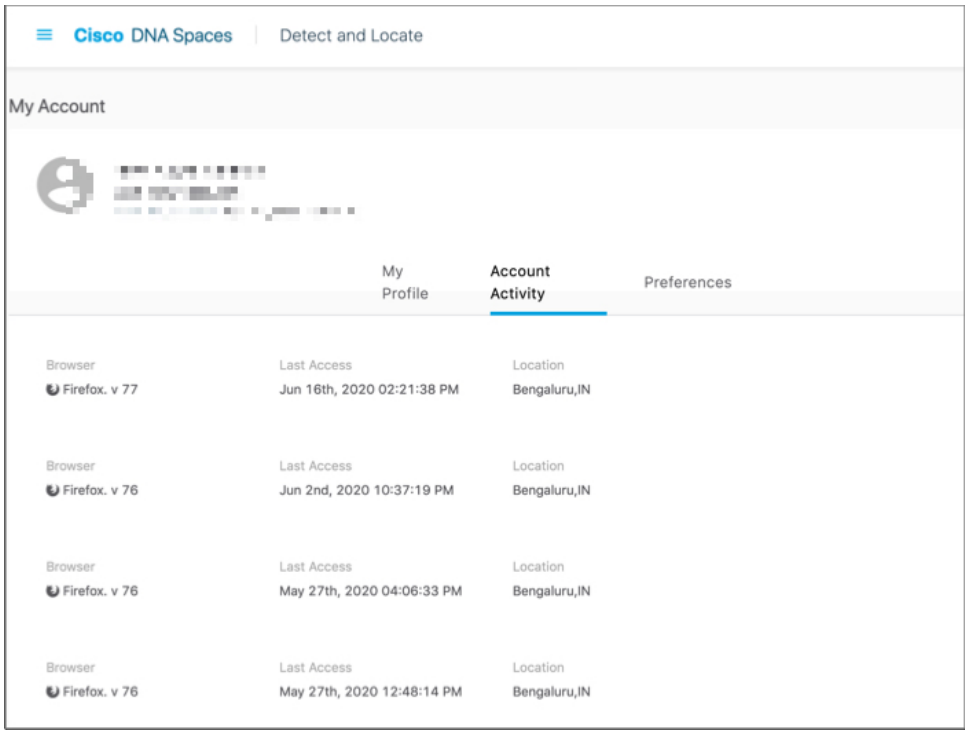
Figure 60: Modifying personal details from User Settings



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.

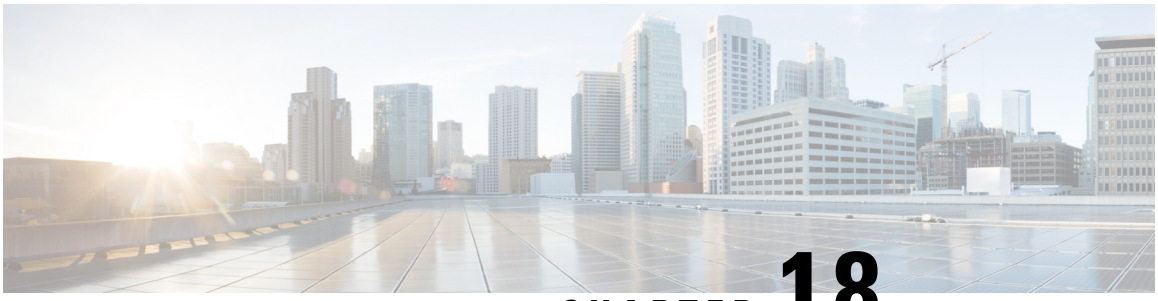

Cisco DNA Spaces
Detect and Locate
My Account
My Profile
Account Activity
Preferences
Browser
Firefox. v 77
Last Access
Jun 16th, 2020 02:21:38 PM
Location
Bengaluru,IN
Browser
Firefox. v 76
Last Access
Jun 2nd, 2020 10:37:19 PM
Location
Bengaluru,IN
Browser
Firefox. v 76
Last Access
May 27th, 2020 04:06:33 PM
Location
Bengaluru,IN
Browser
Firefox. v 76
Last Access
May 27th, 2020 12:48:14 PM
Location
Bengaluru,IN



PART VIII

FAQs

- Manage FAQs, on page 101



CHAPTER 18

Manage FAQs

- How Can I Get Support? , on page 101
- What Information is Stored in My Cisco Spaces: Detect and Locate Account and for How Long is it Stored? , on page 101

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

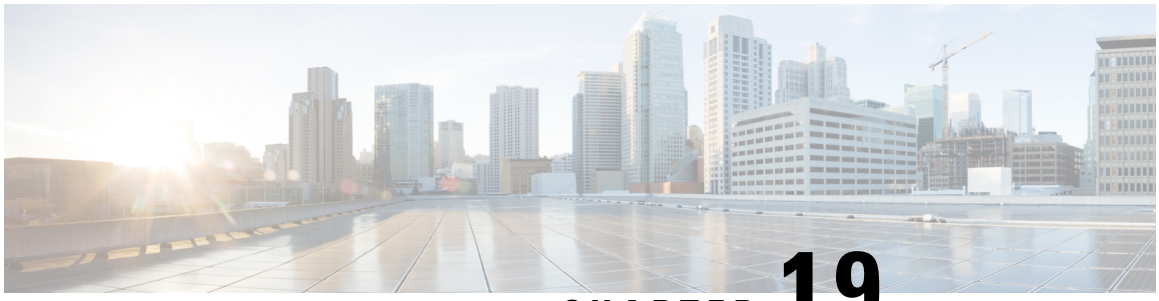
The information is retained until your Cisco Spaces: Detect and Locate account is deleted.



PART IX

API

- API, on page 105



CHAPTER 19

API

- API Key, on page 105
- API Rate Limiting, on page 107

API Key

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:

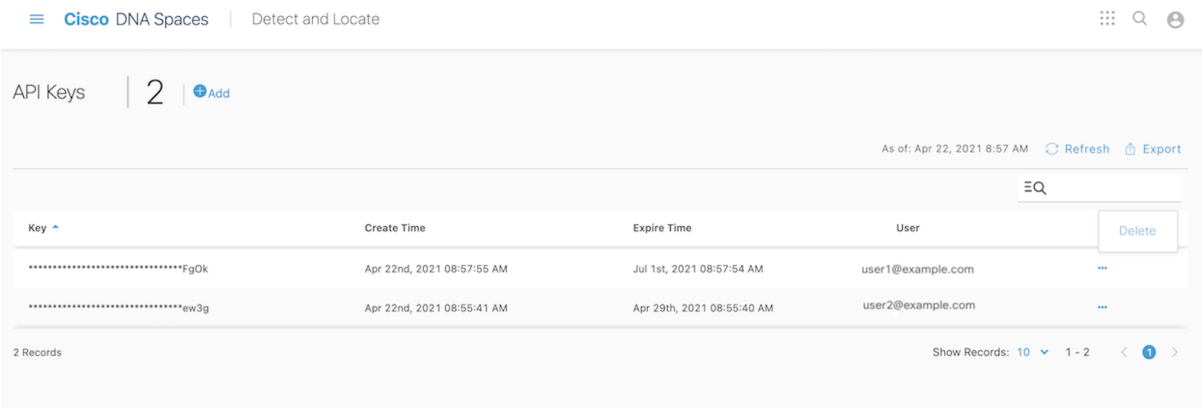
- **Active clients' location APIs**: APIs to retrieve client count and location data.
- **Clients location history APIs**: APIs to get a MAC address and the details for a given device.
- **Notifications APIs**: APIs for subscription-based notifications.
- **Map APIs**: APIs to upload, navigate the maps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

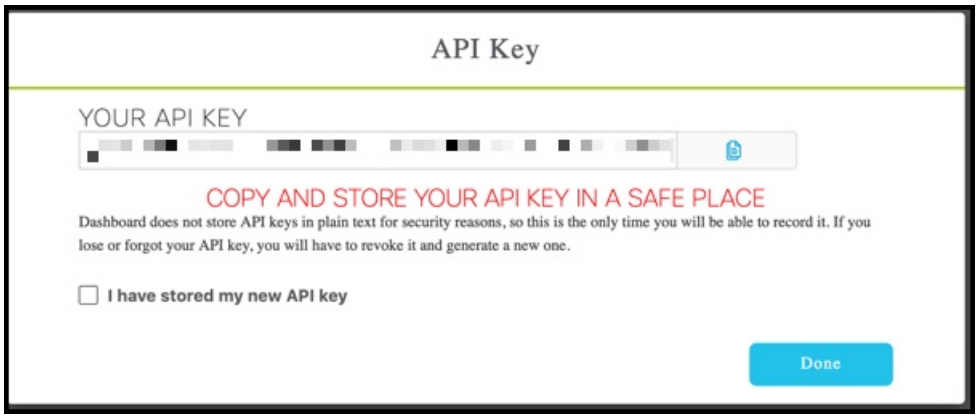
Figure 61: API Keys



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.

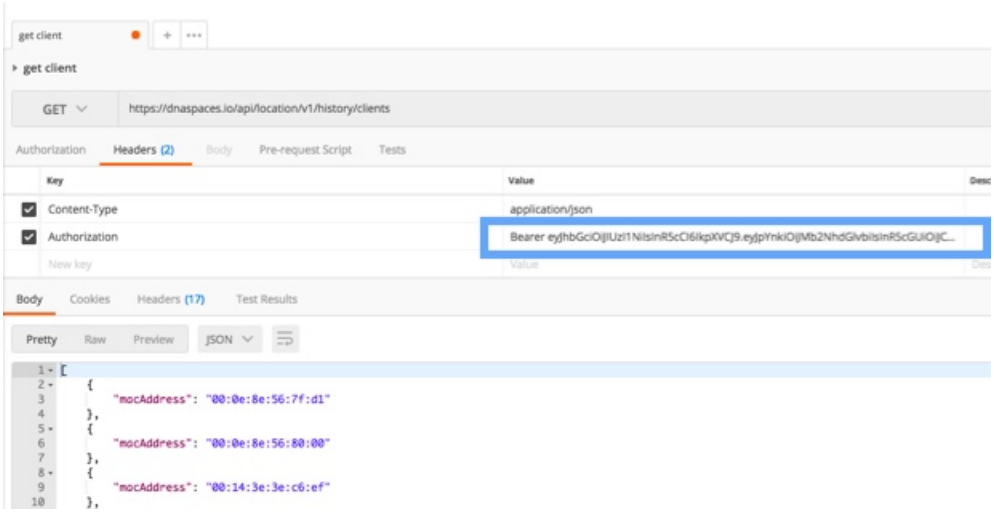
Note The API key is visible only at creation time, and hence must be stored securely. Cisco Spaces: Detect and Locate does not save the API key values. Each authenticated user can have up to 10 valid keys. This API key management feature is designed to protect keys created by administrators, ensuring that each administrator manages only their own keys and does not accidentally delete or view keys belonging to other administrators.

Figure 62: 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 63: API Keys



API Rate Limiting

Rate limiting is enforced on Location public APIs when callers authenticate with a Bearer token. This limiting is tracked per account (tenant) and applies to both v1 and v2 Location API routes.

API limit (`total`)

The maximum number of requests allowed per tenant within one rate-limit window.

Table 7: API limit

Setting	Default
Request limit per window	1250

Lockout window (`expire`)

The duration of the rate-limit window, in milliseconds. When a tenant exhausts its allowance, further requests receive HTTP 429 Too Many Requests until the current window ends.

Table 8: Lockout window

Setting	Default
Window duration	900000 ms (15 minutes)

Lockout behavior: There is no separate penalty period beyond the window. Once `X-RateLimit-Remaining` reaches `0`, the tenant is blocked until `X-RateLimit-Reset`. Clients should honor `Retry-After` on 429 responses and avoid retrying until the window resets.

Response headers (legacy format)

Successful and throttled responses include:

Table 9: Rate-limit response headers

Header	Description
`X-RateLimit-Limit`	Maximum requests allowed in the current window (for example `1250`).
`X-RateLimit-Remaining`	Requests left in the current window. When `0`, the next request will be rate limited unless the window has reset.
`X-RateLimit-Reset`	Unix epoch time (seconds) when the current window resets and the counter is restored.
`Retry-After`	Present on 429 responses only. Seconds to wait before retrying.

Example: rate limit exceeded (429)

The following example shows a tenant that has used all 1250 requests in the current 15-minute window. The client should wait `Retry-After` seconds (here, 656 seconds, about 11 minutes) before sending more requests.

```
HTTP/1.1 429 Too Many Requests
                Content-Type: text/html; charset=utf-8
                Content-Length: 42
                Connection: keep-alive
                date: Wed, 17 Jun 2026 04:26:55 GMT
                access-control-allow-origin: https://dev-dnaspaces.io
                vary: Origin, Accept-Encoding
                access-control-allow-credentials: true
                x-ratelimit-limit: 1250
                x-ratelimit-remaining: 0
                x-ratelimit-reset: 1781671071
                retry-after: 656
                strict-transport-security: max-age=31536000; includeSubDomains; preload
```

How to read this example:

- `x-ratelimit-limit: 1250` — the tenant may make up to 1250 Bearer requests per 15-minute window.
- `x-ratelimit-remaining: 0` — no requests remain in the current window.
- `x-ratelimit-reset: 1781671071` — window resets at this Unix timestamp (seconds).
- `retry-after: 656` — wait 656 seconds before retrying; aligns with time remaining until reset.